The London School of Economics and Political Science

The Social Construction of Computational Surveillance:

Reclaiming Agency in a Computed World

Daniel Frederik Knapp

A thesis submitted to the Department of Media and Communications of the London School of Economics for the degree of Doctor of Philosophy, London, October 2016

“If there is a sense of reality,
there must also be a sense of possibility.”

Robert Musil – The Man Without Qualities

Declaration

I certify that the thesis I have presented for examination for the PhD degree of the London School of Economics and Political Science is solely my own work other than where I have clearly indicated that it is the work of others (in which case the extent of any work carried out jointly by me and any other person is clearly identified in it).

I warrant that this authorisation does not, to the best of my belief, infringe the rights of any third party.

I declare that my thesis consists of 97,862 words (including footnotes but excluding bibliography and appendices).

Statement of use of third party for editorial help

I can confirm that my thesis was copy edited for conventions of language, spelling and grammar by Moritz Knapp.

Abstract

Over the last decades, surveillance has transformed into a pervasive phenomenon woven into the fabric of socio-economic life. In this process, surveillance has itself undergone a structural transformation as its principal agents such as prison guards and CCTV operators have been replaced by algorithms and data-driven technologies. Contemporary surveillance then is embedded in, and expression of, a fundamental remaking of the world, where human decision-making is increasingly supplanted by computational mechanisms, and lived experience is mediated, and even constituted, by computation.

This thesis is a sociological work with an emphasis on the role of communication at the intersection of computation and surveillance ('computational surveillance'). Current debates have predominantly focussed on the systems and mechanisms of computational surveillance. Less emphasis has been placed on the lived experience of inhabiting a computed world, and specifically how people can query and act towards computational surveillance. This thesis makes both a theoretical and empirical contribution to this question.

Through a framework rooted in the sociology of knowledge, the thesis develops a theory of agency towards computational surveillance. It outlines the changing conditions under which knowledge of social reality is constructed in a computational world and theorises modes of reclaiming these conditions for human agents. This theory informed, and its further development emerged out of the findings from a qualitative study of 40 young people in Germany and the UK about their everyday encounters with computational surveillance, which was conducted as part of the thesis. It highlights how participants obtain knowledge about invisible computational mechanisms through their everyday activities and documents practices through which they collaboratively frame computers as interlocutors that they act towards. Lastly, this thesis documents the tactics and strategies employed by participants to hide from, or manipulate computational surveillance, and how they adopt a logic akin to computers in this process.

Acknowledgements

Writing a dissertation can be a lonely task, in particular for the type of participant outsider that I found myself as, juggling a demanding day job in the media industry and academic work during a large part of this project. Needless to say, these worlds are not always compatible. I have, however, been fortunate to count on the support and encouragement of many people, and want to specifically mention a few here.

I would like to thank my supervisor Professor Nick Couldry who has been a steady guiding force throughout this thesis, from its beginnings at Goldsmiths College to its continuation at the LSE. While I could express gratitude for countless inspiration and advice, I want to particularly highlight his understanding – or *Verstehen* as a sociologist would rather say – for the particular situation I wrote this thesis in. He pushed me just when needed and, trusting in my commitment, patiently let me work to my own schedule. This fine balance has been fundamental for my ability to finally finish. I am also grateful to Dr Alison Powell at the LSE for her constructive questions and critical feedback at a crucial stage of this work, which helped me to clarify and structure my argument.

A heartfelt thank you goes to Kenzie Burchell and Sebastian Kubitschko, partners in crime for part of the way and friends beyond, for the continuous exchange of ideas. I could not have done this project without the support of my parents who always encouraged me to pursue a dissertation despite my day job, convinced me of its intrinsic value and did not change their mind when I used our calls to complain about my predicament. The same goes for my brother Moritz, who also provided editorial assistance in the final stage of this thesis. Lastly, and most importantly, I would like to thank my participants, who let me into their lives and onto their computer screens. Without their interest and openness, none of this would have been possible.

I dedicate this thesis to my wife Aleksandra, whose support I struggle to put in words. She taught me how to keep thinking freely despite the constraints and obligations of everyday life and showed me the merits of always questioning the comfortable consensus. Without her, I would have gotten lost along the way.

Table of Contents

List of Figures

Chapter One: About This Thesis

In *Computer Power and Human Reason: From Judgment To Calculation,* computer scientist Joseph Weizenbaum (1976) sketches out the contours of a debate that three decades later came to occupy a central position in the social sciences. He forecasts an algorithmisation of the human lifeworld, where processes of human decision-making are increasingly supplanted by computational judgements, risking, as the German translation of his book puts it vividly, the 'impotence of reason'[1] and changing the self-image of humankind. Weizenbaum warned that the proliferation of computers needs to coincide with human sovereignty over them and their output, already emphasising the role of ethics in computers at a time when the internet, artificial intelligence and other concepts were still in their infancy. Today, the implication of computation in the fabric of society has been adopted by and embedded in the domain of social theory (e.g. Lash 2007; Kallinikos 2009; Beer 2009). These discussions coincide with another macro-trend, the pervasive growth of surveillance in contemporary society, which is itself increasingly computational in form (Deleuze 1992; Lyon 2007) and in a feedback loop informs computational decision-making (Andrejevic 2007).

This thesis is a sociological work situated at the intersection of these societal developments of computation and surveillance ('computational surveillance') with particular emphasis on the role of human agents and their capacity to act. Its original contribution is both theoretical and empirical. As I detail below, theoretical work has so far predominantly focussed on the integration of both computation and surveillance into the large-scale conceptual thinking of the social sciences and their investigation as phenomena that make up society. Less emphasis has been placed on how to theorise the role of human agents as individuals and social beings and their lived experience within the context of such a society. With reference to Weizenbaum's original concern, this thesis applies a communications framework rooted in the sociology of knowledge to the phenomenon of computational surveillance to provide an additional perspective to the theoretical debate. It approaches the notion of agency from the perspective of how people communicate about and towards computational interlocutors, and how communicative

[1] The German translation is entitled *Die Macht der Computer und die Ohnmacht der Vernunft* (Weizenbaum 1978).

tactics and strategies themselves are manifestations of agency.[2] As agency is lived practice and escapes the confines of pure theory, this needs to be reflected empirically. The lived experience of surveillance has similarly been of marginal concern in surveillance studies, although its importance as a field of research has been underscored (Lyon 1994). This thesis, therefore, also investigates empirically through a qualitative study how people act towards computational surveillance, adding to a small body of existing empirical work on other aspects of life with surveillance, such as CCTV.

Although this thesis is sociological in nature, it draws on material and debates from various other disciplines and texts as sociology is itself being redefined through the influx of new social phenomena and concepts like computation and surveillance. Despite a growing range of theoretical material available, the topos of this thesis is both emergent and interdisciplinary. Yet it is not sociological by accident or purely by virtue of its authors' educational background. As Joas (1996) has argued, part of the value of sociology lies in the fact that it is paradigmatically unstable and therefore self-reflexive in its paradigms which makes it open to new types of problems and their interpretation. This thesis, therefore, uses sociology to go beyond sociology. The longer introduction below describes in greater detail the motivation, context and scope of this thesis to allow readers a better understanding of the both the real-life, as well as the scholarly environment in which it takes place.

1.1. A Culture of Surveillance

Sometimes people reveal too much about themselves, French magazine *Le Tigre* found. In 2009, it released a dossier on *Fred*, an regular internet user from France, soley derived from information about him that could be gleaned from social media profiles and other publically available online sources. Developed without his knowledge, the dossier features information about Fred's job, goes into detail about his family life, leisure interests, documents his past holiday destinations and explores his social outings with friends. Le Tigre also published Fred's full name, mobile phone number, mused about his

[2] I use the term 'agency' to denote a general capacity to act. I use it instead of 'action', which is often employed synonymously. 'Agency' additionally points to the wider sociological debate about the constraints and determinants to act, which is the focus of this research. For specific instances of agency, I use the term 'act', following Isin (2008).

current relationship to his former girlfriends and drilled into Fred's dating preferences (Laurent 2009). [3]

Discovering the article, Fred was shocked and sleepless for days, as he later revealed to a newspaper. It was a lesson learned: Fred claimed he had not been aware that such personal information could be extracted and set out to remove all data about himself on the internet, vying to be much more careful about what to reveal online in the future ("Magazin veröffentlicht Profil" 2010). By instrumentalising the unfortunate Fred, *Le Tigre* sought to raise wider public awareness that personal information provided on the internet runs constant risk of being gathered, rearranged and analysed. The magazine intended to place on the public agenda and make visible the hidden and increasingly pervasive mechanisms of surveillance on the internet by emulating those very practices and taking the place of the surveillors.

Only a few years later, *Le Tigre*'s story would hardly stand out. Revelations of surveillance on the internet have rapidly ceased to be a novelty and become normalised as everyday occurrences. They are *everyday* in Durkheim's sense of a regularly reoccurring feature of social life (Durkheim [1912] 1995), not routine in that attitudes and sentiments towards surveillance are numbed and muted. For instance, when *Google Street View* launched in Germany, emotions ran high, eventually leading *Google* to blur the facades of addresses where residents had issued a complaint (Lischka 2010). As part of everyday life, the topic of surveillance has become detached from a niche interest reserved to specialist publications, professional expert or academic circles. It is negotiated in the wider public sphere.

Through films, TV shows, novels and songs, surveillance has long been reflected in popular culture. It forms people's perception of how surveillance works, and this surveillant imaginary also influences surveillance itself as the media co-shape people's attitudes and actions towards surveillance (Marks 2005). Levin (2002) speaks of a rhetoric of surveillance in cinema, and Gary T. Marx highlights "the close links between surveillance and culture, and control and entertainment" (Marx 2009: 377). However, surveillance has ceased to be a theme only explored in distinct cultural works. On a nearly daily basis, surveillance is discussed in the news, from targeted advertising and *Facebook*

[3] I first referenced the anecdote about Fred in *Screen Digest* (Knapp 2009), an industry bulletin for which I worked at the time.

data leaks, over suggestions that *Your iPhone is watching you* (Lischka, Reissman & Kremp 2011), reflexive accounts postulating a *Completely Examined Life* (Albro et al. 2011), biographical narratives about the everyday experience of being observed (Roth 2011), to advice on how to trick *Facebook* algorithms into gaining higher exposure in your friends' newsfeed (Khunkham 2014). Arguing the topic is so pervasive and that it demands a newspaper rubric just like politics or sports, The *Wall Street Journal* has established a dedicated internet surveillance beat called *What They Know* that sheds light on the practices and implications of digital tracking and monitoring.[4]

Accounts that document, debate, and explain surveillance are so plentiful that they afforded Barnard-Wills (2011) to conduct a discourse analysis of how practices of surveillance are represented in UK newspapers. Such discussions coincide with public debate on how to act towards surveillance. Fred still had to figure out himself how to deal with what *Le Tigre* had uncovered. Today, popular interest books include calls to action such as *Program or Be Programmed* (Rushkoff 2011), and arguments in the news media, blogosphere and beyond more specifically discuss tactics and strategies to escape the gaze of *Facebook* and other entities that gather and calculate personal information. These range from how to prevent *LinkedIn* from using profile data for advertising purposes ("How to Stop LinkedIn" 2011), over instructions for deleting personal data from *Google* and other websites (Aschermann 2015), to software tools like *SimpleWash* which claim to clean up people's *Facebook* timeline.[5] These narratives are not merely cultural manifestations of surveillance, but emergent *Cultures of Mediatization* (Hepp 2013). Surveillance as a feature of modern societies is increasingly mediatized. It is taking place as media, as well as articulated and negotiated through media by those subjected to it.

1.2. The Rise of Computation as a Social Force

While graffiti artist Banksy famously depicted a *Nation under CCTV* ("Council orders Banksy art removal" 2008), contemporary public attention towards surveillance stands in the context of a much broader debate on the structural transformation of societies brought about by a set of computational forces denoted as artificial intelligence, robots,

[4] The Wall Street Journal's surveillance beat website indicates activity spanning 2010, 2011, and 2012. However, it is still online in September 2016 and can be found at: http://www.wsj.com/public/page/what-they-know-digital-privacy.html

[5] The *SimpleWash* website can be found at: http://simplewash.herokuapp.com (last accessed: 15 September 2016)

algorithms, and related terms. These issues have taken centre-stage in a growing range of general-interest books. They range from highlighting the socio-cultural impact of artificial intelligence (Schirrmacher 2009), over the dystopian fiction of *The Circle* which relocates the all-encompassing control of Orwell's 1984 into the age of *Apple* and *Google* (Eggers 2014), to a story of an algorithm come protagonist who reflects on its own being as it has taken over the world, written in an attempt to introduce a broader population to the technological forces that increasingly shape our world (Meckel 2011). Formerly a term confined to computer scientists and expert circles, the media now regularly highlight how algorithms shape what we see in the *Facebook* newsfeed, *Tinder* profiles and online search results (Lobe 2015). The didactics of computational surveillance are even gamified: *Data Dealer* is an online game that allows internet users to change sides from being under surveillance to taking the role of those conducting surveillance. Starting as a small dealer with a limited stock of customer data, players are supposed to invest in data collection methods, psychographic tests, gather IP addresses, acquire hospital patient data and other material via ethically dubious middlemen, link it together and sell it, to ultimately become a data tycoon (Kuechemann 2012). Such narratives of surveillance as computational in nature are reflected in academic approaches that de-emphasise surveillance per se in favour of the broader role of computation in its operation and logic (Zuboff 2015). Abstracting from the theme of surveillance, these narratives are expression of the role of computation more widely in modulating and constituting social life, which Alaimo (2014), Kallinikos and Tempini (2014) have termed ‘computed sociality’ and which Kallinikos (2009) has earlier articulated through the ‘computational rendition of reality’. Media, surveillance, and corresponding cultures of mediatisation themselves then stand in the broader context of a social world shaped by computational principles and operations.

1.3. The Janus-Faced Nature of Surveillance

Surveillance is an ambiguous concept. Lyon (1994) has highlighted the Janus-faced nature of surveillance between good and evil. Facilitating both care and control, surveillance either watches over people in the form of *Machines of Loving Grace* (Markoff 2015) or appears as a totalising power governing people with an often dehumanising gaze (Foucault 1977; Sartre [1943] 1993). Amidst prevailing critical stances towards surveillance in public debate, there is a normalisation of cultural practices that consider surveillance not as a threat, but as a feature. In 1945, Vannevar Bush

published an article in *The Atlantic* called *As We May Think*, where he took the end of World War II as an opportunity to speculate what domains research and innovation could focus on now that weapons were not needed anymore (Bush 1945). He anticipated advancements in photography, which would yield much smaller, dot-sized cameras that people wear on their foreheads. He termed them *memex* - memory extenders that archive everyday life. Bush's prediction was accurate. In 2004, *Microsoft* engineer Gordon Bell may have looked odd when he started to wear a camera device around his neck at all times, the size of a cigarette package, which regularly takes photos of his surroundings. Called *SenseCam*, his device is equipped with a sensor that detects body heat. When an interlocutor stands vis-à-vis Bell, it takes a picture. The device can also be programmed to make photos at short intervals of up to a minute, or when the light changes, signalling a chance of context. Two decades on, the practice of life-logging has become commonplace. Ambient sensors in smartphones, smartwatches, fitness trackers and other devices record their owners' every move and vital body functions through individualised surveillance as a service (Wilkinson 2007).

1.4. Understanding the Lived Experience of Surveillance

The contours of this wider public debate hint at profound social changes at the intersection between media and communication, technology and surveillance. The rapid and complex proliferation of debate in recent years suggests that surveillance has become a fixture in the world of lived experience. Notions of surveillance have entered the cultural fabric of the everyday. Debates about its digital manifestation in the form of algorithms, or other computational concepts are a matter of public attention and people as citizens and consumers navigate the perils of exposure and complicity in an increasingly complex web of surveillance. Despite such signals, there is a lack of theoretical and empirical research that systematically seeks to understand and embed into a sociological context how people live under conditions of pervasive surveillance, and in particular how far they are able to act towards forms of surveillance that are increasingly located in the realm of computers.

The urgency to facilitate such an understanding is greater than ever. In the Post-Snowden Age, the canvas on which manifestations of surveillance are narrated has changed. Previously, they stood out as deviations from a public consensus that while surveillance was rampant and colonising ever more areas of everyday life, it took place against a default of not being tracked, monitored, or analysed. *NSA* surveillance and its global web

of political and corporate complicity revealed by Edward Snowden and *Wikileaks* changed this default in the public mind, where a lack of surveillance has become the exception. In *Surveillance After Snowden*, Lyon (2015) recognises this new default. He argues that the ability for human agents to maintain their individual agency in the context of pervasive computational surveillance is a fundamental prerequisite for the future of democracy and society at large. This research seeks to contribute to addressing this urgency, with particular consideration of the current state of research.

1.5. Focus and Limitations of Existing Research

Surveillance itself is a longstanding theme in the social sciences. Over the last decade and a half, a cross-disciplinary endeavour has emerged to bring together and systematise a growing range of theoretical and empirical inquiry across various social science disciplines to form a loosely organised sub-field labelled ‘surveillance studies' (e.g. Lyon 2002; Dubrofsky & Magnet 2015). However, scholarly attention has mainly focussed on systems of surveillance and institutional aspects. While surveillance scholars highlight “the complex of surveillance practices” (Ball & Haggerty 2005: 130) as their scope of inquiry, their notion of practices tends to denote the ways in which surveillance is conducted. In fact, most research does not specifically consider practices of everyday life from ordinary people in relation to surveillance.

An emerging field of empirical studies is seeking to shift this entrenched perspective. However, despite their merits, these contributions focus on isolated empirical domains such as shopping centres or webcams, or particular types of agents such as advocacy groups, instead of a broader context of surveillance in everyday life (e.g. Albrechtslund 2008; Introna & Gibbons 2009; Koskela 2003). Such studies also tend to privilege a particular stance towards surveillance within the binary of resistance and complicity, instead of incorporating the Janus-faced nature of surveillance. Furthermore, there is a lack of empirical research on surveillance in the context of an increasingly mediated life – an area that Lyon (2007) has identified as a growth area for surveillance studies – and in particular considerations of the relationship between human agents and the computational nature of surveillance within this mediated environment. Existing studies also recognise both absence and need for a theoretical understanding of how people engage with surveillance in order to further advance empirical work (e.g. Albrechtslund 2008).

Similar limitations apply to the partly overlapping debate around online privacy and personal data. This debate, which mainly emanates from a broader legal context (e.g. Nissenbaum 2009; Solove 2004; Rule 2009) emphasises the individual under surveillance. However, accounts of privacy do not delve into the actual lived experience of surveillance. Privacy also is not synonymous with surveillance. While privacy is generally framed as an individual matter, surveillance has social aspects (Franklin 1996). Lyon (2007) cautions against the focus on privacy as a token of 'possessive individualism' (Macpherson [1962] 2011), and he is joined by other authors who argue that it downplays issues of social inequality, stereotyping, exclusion, governance and power that are constituent parts of surveillance and signal much wider social implications far beyond the conceptual limits of privacy (Lace 2005b; Mosco 1989). Understanding agency towards surveillance then requires moving beyond individual privacy to consider how people in everyday life act in the context of these much broader issues.

Accounts that highlight the role of computation in society have begun to also consider life under such conditions. For instance, Crawford (2015) highlights the need to analyse the social spaces in which computation operates, and especially those through which it is contested. Van Dijck (2013) illustrates how developers and technology executives encode assumptions and rhetorics of sociality into online social platforms, and uses this perspective from the inside of platforms to demonstrate how such computational configurations impinge on people's experiences. Similarly, Bucher (2012a) has studied how *Facebook's EdgeRank* algorithm programs visibility on the newsfeed and how sociotechnical processes on social media platforms produce affordances in which users consider the notion of friendship (ibid. 2012b). Alaimo (2014) offers a more experiential setting through an empirical case study of an e-commerce company. Documenting the company's infrastructure design in its start-up phase, she demonstrates how user choice is represented through data-mining techniques and how corresponding personalisation engines reconfigure how consumers can imagine themselves in the context of computed sociality. These are examples of a growing body of work that advances the understanding of computation in a social context and documents its complex, agential powers. However, similar to the state of the surveillance debate, particular emphasis thus far been placed on interrogating the systems of power and social moulding forces inherent in computational systems. Building on the call to pay closer attention to the perspective of human agents themselves (Couldry & Powell 2014), the centrality of agency enacted by ordinary

citizens in everyday life under these conditions is becoming more widely acknowledged (Kennedy, Poell & van Dijck 2015). Most recently, Bucher's (forthcoming 2017) empirical analysis of how Facebook users imagine its algorithms underscores the need for further systematic research under this prism.

1.6. Thesis Framework

In light of both the state of empirical work in surveillance studies and the limitations of the privacy debate, Lyon's (1994) nearly two-decade-old observation that agency in relation to surveillance demands further systematic research remains current. At the same time, the structural transformation of surveillance through computation and its growing implication in people's everyday lives have lent it unprecedented urgency (Lyon 2015) that is echoed by discussions rooted in the study of algorithms and computation more widely. This project seeks to provide an original contribution to these debates. It consists of a theoretical and empirical framework for understanding agency in the context of surveillance that is itself embedded in pervasive computation.

Chapter Two (In Search for Surveillance Theory), directly follows this first introduction. It provides a review of theoretical approaches to surveillance. Firstly, it documents the theoretical debates around surveillance, how they have changed in the context of wider transformations of modernity, and explores whether a grand theory of surveillance does justice to the complex and multi-faceted nature of surveillance. It places particular emphasis on the limitations of the panopticon as the predominant template for framing surveillance, how it has influenced the debate, and what conceptions of power and personhood it affords. Secondly, it is concerned with the ways in which theories of surveillance can inform a perspective on agency. It concludes that surveillance studies have been so focussed on systems and institutions of surveillance in their theoretical development, that they cannot facilitate a systematic account of agency. At the same time, it argues that wider transformations in the ways surveillance operates have changed the coordinates of inquiry, and that understanding agency towards surveillance demands a broader debate about computation as a social force.

Chapter Three (A Framework for Agency in Computed Sociality) expands on this groundwork. It formulates a theoretical approach of agency towards computational surveillance. This approach is delivered as a communications framework that is informed

by a sociological perspective. It discusses how algorithms, big data, software, code, artificial intelligence and related concepts as agents of surveillance are increasingly embedded in the flows of everyday life, how they transform the fabric of society and how their internal logic fundamentally alters how people can make sense of the world. Drawing on wider debates around infrastructure and visibility, the chapter outlines the perceptual, cognitive and hermeneutic obstacles that human agents face in attempting to query and act towards such surveillance, the configurations of power this implies, and how these issues define new coordinates for the sociological debate about structure and agency. The chapter then embeds these themes in a broader sociology of knowledge to theorise the possible modalities of agency, the communicative relationships between human and computational interlocutors this presupposes, as well as the wider social context in which these relationships take place. This framework provides the basis for later empirical interrogations.

A theory can only consider how agency is possible in principle, and not how it manifests itself as lived experience. The theoretical framework outlined above, therefore, is followed by a discussion on how the sense-making activities of human agents, both in relation to computation in general and surveillance specifically, can be operationalised empirically. *Chapter Four (Methodology)* addresses this. It develops a research design around in-depth interviews and think-aloud protocols. It proposes a modification of think-aloud protocols that progress from tapping into working memory to long-term memory, and from descriptive and affectual statements to those that are reflexive, contextual and participatory. Core aspect of surveillance are power relationships expressed through acts of watching. Empirical studies of surveillance, therefore, need to adhere to particular ethical standards, especially if the proposed methods contain a degree of observation themselves, and this chapter takes account of those requirements. Lastly, it outlines the sampling and interview process across 40 subjects in the UK and Germany and reflects on the experience of ‘doing' surveillance studies as a researcher.

The next four chapters contain an analysis of empirical material and how it relates to the overarching theoretical framework. These chapters are organised in a funnel structure that moves from a first chapter on general context over two chapters concerned with patterns of understanding revelations of computational surveillance, to a last chapter focussed on modes of agency. The theoretical material required to frame the empirical data is

contained in the previous chapters and will be referenced again where required. In cases where a chapter delves into the minute conceptual details of a theory, these are outlined at the beginning of each empirical discussion. In order to highlight a particular point, short references to scholarly material not part of the overall theoretical framework may occur. This is not intended to override the theoretical framework, but to provide additional nuances.

Chapter Five (The Normalisation of Surveillance in a Landscape of Risk) explores the troubled relationship between human agents and surveillance. It documents the inevitability of surveillance and how human agents consider surveillance both as a threat as well as a set of practices that they embrace – be it through voluntary self-exposure or through conducting surveillance themselves. The chapter shows the fluidity of the surveillance landscape, that surveillance is not an abstract concept but firmly embedded in everyday life, and that human agents take multiple roles between watcher and watched. It also demonstrates that theoretical concepts of surveillance do not align with definitions of surveillance in everyday life and that some acts of watching are considered as permissible while others are not, indicating a complex set of ethics of surveillance.

Chapter Six (Experiencing the Fleeting Conditions of Knowledge), shifts the focus on the relationship between human agents and computational logic. It explores how human agents encounter usually hidden computational surveillance in their daily experience on the internet, how they react to principles and assumptions of surveillance laid bare, and what tactics and strategies human agents employ in triggering surveillance to reveal itself. The chapter explores how such revelations foster a systematic knowledge about surveillance and what this means for the perceived individual powers to deal with surveillance.

While the previous chapter considered the surveillance encounters of human agents as isolated individuals, *Chapter Seven (Collaborative Inquiries and the Troubled Nature of Common Sense)* sheds light on the social practices of interrogating computational surveillance. It demonstrates how human agents work collaboratively to inform each other about the way it operates, and how they jointly attempt to deconstruct the computational logic behind surveillance. The chapter documents the range of practices across which this collaboration takes place, highlights the conflicts within common-sense knowledge about the world that emerge from the fluid nature of knowledge about

computation, and also shows how such common-sense understanding is reproduced in everyday language and folk tales about computational surveillance.

Chapter Eight (Negotiating Clashes of Reality With Unknown Interlocutors) is concerned with the tactics and strategies of interacting with computational surveillance. It proposes that computational agents are categorically unknown interlocutors and documents people's attempts at establishing a social situation with these interlocutors to negotiate interpretations of reality. On this basis, the chapter explores people's communicative practices to intervene in the ability of computers to 'see' them, and how they also adapt computational interpretations of reality through such practices. The chapter debunks the notion of human agents as hyper-rational actors and instead shows that negotiating relations of visibility involves failures, omissions and accidents. It highlights that in the process of dealing with computational interlocutors and imagining their logic, human agents themselves simulate computational principles.

Chapter Nine (Conclusion) summarises the argument advanced in this thesis and establishes additional connections between theoretical and empirical material, as well as between the individual empirical chapters, that the necessarily linear nature of argument did not previously afford. It reflects on what this thesis has achieved and highlights its limitations. Lastly, it suggests further applications of the framework developed in this study and highlights additional areas of research in both the empirical and theoretical domain to support, expand, and critically engage with its analysis.

Chapter Two: In Search for Surveillance Theory

Etymologically rooted in the French verb *surveillir* (to watch over), surveillance stands for "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction" (Lyon 2007: 14). It contains a level of ambiguity that complicates its diagnosis and at least partly puts it in the eye of the beholder. For instance, intentions and practices of caring may not be considered as surveillance by a person watching over another, but can be perceived as an intrusive act of control by the very person that is being watched over. Similarly, while some people are concerned about online surveillance, others see appeal or benefit in self-exposure and actively collaborate in their own monitoring (Andrejevic 2005; Pridmore 2013), creating contradictory subjective assessments of surveillance in a given context. Defining surveillance also is a matter of semantics. While consumer advocates may talk about 'targeted advertising', the advertising industry itself prefers the term 'addressable advertising' (e.g. Poggi 2014). Targeting implies maliciousness, vulnerability and intrusion, whereas addressability not only emphasises advertising as a service, but also hints at optionality and choice rather than determinate fact – it is not 'addressed' advertising. Prominent terms that are often used interchangeably for surveillance, and which complicate a distinctive conceptualisation, are 'tracking' and 'monitoring'. The difference to surveillance lies in the context surrounding the act of watching. Both tracking and monitoring only refer to a set of acts over time. Surveillance incorporates the motivations and consequences of those acts, which constitutes it as a political and social concept.[6]

This chapter provides a critical introduction to approaches towards surveillance and the theoretical development of surveillance studies. It organises and reviews multiple strands of surveillance theory in order to assess their merits for facilitating an understanding of agency, both bearing in mind that surveillance increasingly takes place in mediated environments on the internet, and that the principal agents of surveillance have come to

[6] While this conceptual distinction highlights the broader social and political entanglement of surveillance, it is difficult to uphold in writing about surveillance. Monitoring and tracking are terms closely associated with data-driven surveillance, or dataveillance, in a digital consumer context. Imposing the term surveillance in place of everyday language can sound contrived and artificial. In the case of the subsequent empirical part of this research, it can even be distorting. The research references people's everyday language about surveillance, and monitoring and tracking feature prominently. In this text, I then understand tracking and monitoring as expressions of surveillance itself, and not in the strict conceptual sense.

be computers in the widest sense. While the chapter considers the notion of computation to shed light on the socio-economic transformation of surveillance and to query its analytical potential, it leaves an in-depth discussion of computation as a social force and its direct relevance for understanding agency to *Chapter Three*, and merely paves the way for such an analysis. Arguably, debates around surveillance and computational issues like algorithms and big data are intertwined (e.g. Zuboff 2015; Kennedy et al. 2015). However, the conceptual history and paradigmatic focus of surveillance studies also extends beyond the social sciences' relatively novel preoccupation with computation. My interest in this chapter is to interrogate the potential of surveillance as a master concept in understanding agency under consideration of the particular role of computation from within its own theoretical repertoire and conceptual history. *Chapter Three* then shifts focus to issues of computation in wider social theory.

The chapter begins by documenting how surveillance has been discussed across classic sociological work, post-modern accounts, and approaches rooted in the tradition of reflexive modernity. It argues that while surveillance is an integral part of modernity, assessments about its nature and about its relationship with other concepts diverges across theoretical approaches. The argument follows and extends Lyon's (2007) claim that a grand theory is ill-suited to capture the complexity of contemporary surveillance, in particular from a perspective that both considers its computational nature and the role of agency, and hence calls for a situated framework that focuses on particular configurations of surveillance. The chapter suggests that surveillance studies still carry too much conceptual baggage to systematically move towards such an approach, and that any such attempt needs to emancipate surveillance studies from the panopticon, Bentham's prison design which informed Foucault's theory of disciplinary society as the archetype of surveillance. Reviewing critiques of the panopticon (e.g. Boyne 2000; Yar 2003; Haggerty 2006), this chapter identifies the 'docile bodies' paradigm (Foucault 1977) as the central obstacle for considering agency and argues that later Foucauldian approaches rooted in a governmentality paradigm cannot overcome this issue.

On the back of this diagnosis, the chapter then outlines the parameters for a situated approach via the notion of interactivity (Kiousis 2002). It proposes that interactivity is a concept which both delineates the surveillance context under study, and simultaneously offers an open framework to consider various manifestations of agency. Building on the

idea of interactivity, the chapter reviews existing, largely empirical approaches to agency, and translates them into a theoretical discussion. Concluding, the chapter considers two possible perspectives through which a theory of agency in the context of computational surveillance can be formulated despite the shortcomings of surveillance studies today. Comparing both approaches, it argues that surveillance studies ultimately are too narrow to provide an understanding of how people live with computational surveillance. As surveillance creeps into nearly all aspects of life, the chapter calls to de-centre surveillance studies and to embed the issue surveillance into the broader repertoire of social theory. This way, a more context-specific analysis of surveillance is possible, and frameworks become available in which agency plays a pivotal role, rather than standing on the periphery.

2.1. Approaches To Surveillance

In the following sections, I document how surveillance has been considered across various strands of social theory, and how conceptions of surveillance have changed as the field of social theory grappled with a transformation of society itself. I argue that a grand theory of surveillance is unable to capture the nuances and particularities of specific configurations of surveillance and needs to be replaced by a more situated approach. I reserve a separate section for a more extensive discussion of Foucault's view on surveillance expressed through the idea of the panopticon, a particular prison design, which had considerable influence on the development of surveillance studies, and outline the notions of governmentality and technologies of the self as often postulated successor concepts within a Foucauldian paradigm. I conclude that Foucauldian approaches by themselves are unable to address the issue of agency, and that a situated approach requires a different perspective.

2.1.1. Surveillance, Social Theory, and Modernity

Surveillance occurs in all cultures, societies and times (Lyon 2006). Recent archaeological work even suggests that the panopticon, which Foucault (1977) thought of as a quintessentially modern surveillance architecture, already existed in antiquity (Yekutieli 2006). But as a political and social concept, surveillance has found a structural and systematic expression in modern societies. Such considerations of surveillance are not static over time, and linked to a broader debate about the make-up and transformation of modern societies. Below, I document conceptions of surveillance in classic social

theory and newer theoretical approaches. I understand classic social theory as theoretical frameworks that have been instructive for the emergence of sociology as a discipline, and which seek to understand modernity as such. The newer theories are those which problematise modernity and document its transformation, be it under the label of post-modern or other theory. I conclude this section with remarks on the scope of theory as such, and whether changes in modernity and ergo surveillance still merit a grand theory of surveillance.

Classic Social Theory and Surveillance

Early capitalist implications of surveillance are reflected in the time-and-motion-studies of Frederick Taylor, a 19th-century factory owner who went at great length to implement and study systems of workplace surveillance in order to rationalise production (Noble 1986). Already Karl Marx[7] hence saw surveillance as part of the political economy of capitalism, creating a link between surveillance and the exploitation of labour (Fuchs 2013), and Weber considered surveillance as a constituent part of bureaucratic organisation, expressed through rationalisation and control in his 'iron cage' metaphor (Weber [1930] 2001). Giddens later argued that surveillance should not merely be considered as part of modernity by proxy of capitalism or bureaucracy, but as a feature in its own right that allows the direct supervision of social life through the state (Giddens 1985). He sees surveillance as a systemic requirement for the modern nation state in that it affords the state with the administrative power to manage populations and territories at a distance. Reviewing earlier theorists, Dandecker (1994) proposed to connect surveillance across capitalism, bureaucracy and militarism. Other classic social theories of modernity account for surveillance implicitly. Considering changing notions of social solidarity in modern societies, Durkheim's studies of crime suggested that rising inequality spurs an increase in surveillance, and Simmel's 'society of strangers' in the emerging metropolis presents itself as a world of eroding trust relationships in which people monitor each other suspiciously (Simmel 1971).

Examining the philosophical discourse around the eye and the concept of vision in France, Jay (1994) notes a transformation in attitude, a *Denigration of Vision* in the 20th century away from Enlightenment thinking to darker associations with power, perversion, and

[7] I use the full name of all authors named Marx to distinguish between Karl Marx and surveillance scholar Gary T. Marx.

ultimately surveillance. Accounts in the philosophy of history, in particular from a Foucauldian perspective, have also highlighted how a quantitative paradigm borne out the Enlightenment has facilitated and institutionalised systematic surveillance. Hacking (1990) documents the rise of statistics and measurement of people as a mode of governance. Rose speaks about the accountability through numbers emerging in the 19th century as a mode of governance for states and capitalist economies alike, which coincided with the rise of the 'calculable person' (Rose 1999). While these accounts are not directly rooted in social theory, their historical perspective provides a deeper understanding of the epistemological principles of surveillance, and how ways of making sense of the world are connected to particular expressions of power. They also serve as an analytical bridge to consider a second, newer strand of social theory that seeks to rethink surveillance in a changing social context. The critique of vision and the role of statistics and calculation are all referenced in the development of such arguments.

Surveillance and Critiques of Modernity

The classic social theories that I mentioned above are foundational for sociology as a discipline. They place surveillance in the context of the structural constitution of modern societies and its master concepts of capitalism, bureaucracy, nation state, solidarity. Aiming to order the field of surveillance studies, some observers propose that such approaches can be juxtaposed with postmodern theories of surveillance (Lyon 2007). The notion of postmodernity is itself contested, but Lyon argues that one does not need to accept the validity of the concept to consider it a useful marker for organising surveillance theory. Yet as postmodernity comes with conceptual baggage and preconceptions that would narrow the range of theories included, I propose to broaden the scope to all those theories associated with changing social, political, cultural and economic paradigms of modernity from the last quarter of the 20th century onwards. This includes theories under the label of postmodernity, but also those which instead argue for the emergence of another type of modernity, either denoted as Second Modernity, Late Modernity, Reflexive Modernity, Re-Modernity, High Modernity, or Liquid Modernity (Giddens 1990; Beck 1992; Beck & Bonß 2001; Beck, Giddens & Lash 1996; Bauman 2000). While postmodernity undertakes a *de*-structuration and *de*-conceptualisation of modernity, accounts that see another modernity emphasise a *re*-structuration and *re*-conceptualisation of modernity (Beck, Bonß & Lau 2001).

A common trait among these theoretical approaches is that they consider surveillance in light of the transformation of society itself and the critique of modernity under these conditions. In this process, surveillance becomes associated with a range of additional concepts that have come to frame social theory, such as technology, information, databases, the body, gender, culture and consumption. At the same time, such theories suggest a changing nature of surveillance itself. For instance, Staples ([2000] 2013) charts the transformation of surveillance from the informal, haphazard and unstructured supervision in pre-modernity, over formal classification and categorization in modernity expressed in bureaucracy, to postmodern surveillance, which is systematic, automated, real-time, and takes place across complex digital networks.

This echoes previous observations from Deleuze (1992), who documents a shift in how power operates through surveillance. For Deleuze, surveillance has ceased to be primarily concerned with disciplining people in enclosed and pre-defined social contexts such as the school or the prison, an idea central to Foucault's argument that I explore next, and referenced in the bureaucratic, military and Taylorist workplace supervision connotations of surveillance. Instead, Deleuze claims that surveillance has shifted towards a more subtle, but all-encompassing notion of control reproduced across and designed into all aspects of social life. At the same time, surveillance is never complete, but perpetual. A final judgement call on the subject under surveillance, as guilty or innocent, as sick or healthy, is never undertaken. Surveillance operates in an endless loop. The spatial extension of surveillance then coincides with a shift in temporal focus from the past and present to the future. Bogard (1996; 2006) has underscored this future-focus of contemporary surveillance through his idea of surveillance as simulation, where future outcomes are generated on the basis of data analysis.

Spatial and temporal reconfigurations of surveillance extend into broader considerations around the relationship between data and surveillance, and ultimately the agents and subjects of surveillance. Gary T. Marx (2002) has coined the term 'new surveillance' to highlight that alongside the changing make-up of society, surveillance relies on the use of digital data about people. Bowker & Star (1999) have emphasised the potential of social sorting facilitated through data, Poster (1996) proposed to consider databases as discourses in which surveillance becomes manifest, and other authors have underscored that the proliferation of data means that those under surveillance are not monitored as

flesh-and-bone individuals, but as representations of their data locked into code. These representations are variably termed ‘data-doubles’ (Haggerty & Ericson 2000), ‘data persona’ (Clarke 2004) or ‘data images’ (Lyon 1994). Building on Deleuze’s idea of control, Galloway (2006) suggests that code and protocol have become the primary agents of surveillance.[8]

Other authors further extend the point about changing agents of surveillance to set it apart from classic modern considerations. Giddens (1985) in particular focussed on surveillance as the exclusive domain of the state, and whereas Marx and others considered surveillance in the context of capitalism, they emphasised it in the context of the exploitation of labour. Among critiques of modernity, Staples ([2000] 2013) already hinted that the transformation of surveillance into a pervasive phenomenon needs to be considered in the context of consumer society. Bauman (2001; 2005) developed this idea more systematically and located surveillance in the broader domain of consumer seduction. The notion of seduction highlights several attributes of surveillance. Firstly, it documents the emergence of corporations as surveillance agents, secondly it argues that the aim of surveillance is neither coercion, nor necessarily control in an absolute manner, but influence. Thirdly, it incorporates the idea of the Janus-faced nature of surveillance (Lyon 1994) in that seduction can spark willing complicity in being surveilled, and that surveillance can generate at least perceived benefits to consumers.

The Fragmentation of Surveillance and the Quest for a Grand Theory

More widely, considerations of surveillance beyond classic social theory demonstrate a growing diversity of surveillance itself, coinciding with an increase in scholarship that considers different fields of surveillance. Instead of a general narrative, surveillance has become situated in a range of different discourses from crime culture over CCTV and biometric filtering to consumer targeting on the internet, which complicates a comprehensive review.

Social sciences have the tendency to elevate era-defining phenomena through labels. German sociology knows the term ‘Bindestrichgesellschaft' (Schelsky 1965), literally

[8] Galloway’s claim has considerable implications for understanding agency in the context of surveillance and intersects with broader debates about the role of algorithms, big data, software, code and other concepts in the constitution of societies. The next chapter emphasises this theme and I will hence not go into further detail here.

hyphenated society, whose name is a composite of 'society' and one dominant attribute that characterises it, such as 'knowledge society' (Drucker 1969), 'network society' (Castells 2009; van Dijk 2012), 'information society' (Webster 2006; Mansell 2009), 'post-industrial society' (Bell 1976), 'risk society' (Beck 1992) or 'consumer society' (Baudrillard 1998).[9] The proliferation of surveillance has produced similar labels. Gary T. Marx (1985) first coined the term 'surveillance society', which was soon adopted by Gandy (1989). Writing about the pervasive spread of CCTV cameras in the UK, Norris & Armstrong (1999) argued that the developed world is on its way to a 'Maximum Surveillance Society'. Although he accepts the term, Murakami Wood (2009) more carefully uses inverted commas in referring to 'surveillance society'.

These 'Bindestrichgesellschaften' require careful evaluation in the tendency of each to denote what Schelsky (1965) calls a *'pars-pro-toto'* (my emphasis) society that seeks to capture a given social system comprehensively. He stresses that contemporary society is so diverse in its inherent heterogeneity that it can accommodate a plurality of partial descriptions, but only as long as they do not take their pars-pro-toto literally and claim exclusivity of social explanation. As some authors argue, the merit of such all-encompassing labels lies in the development of hypotheses to describe and accentuate phenomena that pervade social reality at large, and provided they retain this character of a hypothesis can coexist with other perspectives on society (Schelsky 1965; Tyrell 2005).

The notion of a surveillance society has merit in that it elevates surveillance to a systemic feature of modern societies. It highlights that surveillance is not only pervasive but that a logic of surveillance is emblematic for social processes and conduct at large. This makes it possible to consider surveillance not merely as an expression of other phenomena, but as a foundational principle of society in its own right. Yet paradoxically, the pervasive spread of surveillance also undermines the usefulness of such a label. Its very rise fractures surveillance as a holistic concept. As I outlined above, surveillance exists from numerous scholarly perspectives, in multiple contexts, with multiple manifestations and is not homogenous in its intentions, distribution, and effects. This is especially pertinent

[9] These authors' use of such labels does not imply the uncritical normative acceptance of the underlying concepts. For instance, Webster (2012) is himself critical of concepts of information society and Mansell (2009) documents the dystopian connotations of an 'information society' brought forward by theorists like Jacques Ellul ([1954] 1964). Also note that while Bell is commonly associated with the term 'post-industrial society', he is considered as the originator of the term 'information society' (Mansell 2009) that has been popularised by later theorists.

in the context of the 'new surveillance' that Marx (2002) outlines, and which is at the heart of this study, where data collection and analysis pervade nearly every aspect of everyday life (Beer 2009). Any blanket theory of surveillance would ignore such nuances and trends. Thus when Lyon (2007) argues that concepts like surveillance society are potentially misleading, he instead proposes a differentiated approach that considers distinct sites of surveillance to

> "[separate] surveillance strands out into different domains of social life such as work and leisure. This gives us a sense of the variety of surveillance situations that we might encounter, a sense of how one system gave rise to or facilitated another, and at the same time a sense of how one system will overlap with another or several others." (Lyon 2007: 25)

I argue that such an approach can be extended to take into account specific agents, subjects, means and intentions of surveillance which together with sites of surveillance form distinct configurations which each require their own theoretical framework. This has implications for the theoretical framework of this particular research and its emphasis on agency in the context of digital surveillance in mediated everyday life. A grand theory of surveillance would struggle to provide the necessary detail and focus. However, the theoretical development of surveillance studies itself remains an obstacle to developing such an approach, and the influence of Foucault plays a central role in this as I argue in the following section.

2.1.2. Overcoming the Panopticon

Despite the volume and variety of scholarship, Foucault's influence and in particular his notion of the panopticon continues to dominate surveillance studies in the form of a grand theory. In fact, the panopticon has become the predominant scholarly template for analysing surveillance, invariably as a full-fledged theory or merely as a metaphor. Its continuing dominance in surveillance studies comes despite early criticism that Foucault's work was flawed (Ignatieff 1977) and arguments that understanding surveillance requires broader frameworks (Webster & Robins 1986; Baumann 1988; Zubroff 1989). In the following, I outline Foucault's central surveillance concept, how it has come to influence surveillance studies, and trace a growing discourse that seeks to overcome it.

Understanding the Panopticon from Bentham to Foucault

The panopticon is a concept for a prison design originally invented by social reformer Jeremy Bentham who envisioned it to cure social ills. Bentham contemplated the panopticon for two decades, but it was ultimately never build to his original specifications (Bentham 2010). Its architecture intended to maximise the visibility of prisoners through careful arrangement of space and light, making inmates continually exposed to an invisible observer concealed in a central tower. While this observer may not see the inmates all the time, inmates do not know when the observer might be looking at them. The gaze is unverifiable but potentially present at any given moment, causing inmates to comply due to uncertainty of exposure. Foucault powerfully describes the panoptic design as follows:

> "At the periphery, an annular building; at the centre, a tower; this tower is pierced with wide windows that open onto the inner side of the ring; the peripheric building is divided into cells, each of which extends the whole width of the building; they have two windows, one on the inside, corresponding to the windows of the tower; the other, on the outside, allows the light to cross the cell from one end to the other. All that is needed, then, is to place a supervisor in a central tower and to shut up in each cell a madman, a patient, a condemned man, a worker or a schoolboy. By the effect of backlighting, one can observe from the tower, standing out precisely against the light the small captive shadows in the cells of the periphery. They are like so many cages, so many small theaters, in which each actor is alone, perfectly individualized and constantly visible." (Foucault 1977: 200)

Foucault appropriated the idea of the panopticon and made it central to his theory of power outlined in *Discipline and Punish* (Foucault 1977). For him, the panopticon is an expression of discipline as a particular mechanism through which power operates by minutely regulating space, time, and people's behaviour. Foucault sees discipline as the dominant mode of power from the 18th century onwards with the objective to form 'docile bodies', that is bodies moulded into functioning for the specific socio-political requirements of the time, such as the military, penal institutions, classrooms and hospitals. In contrast to a previously dominant sovereign power expressed in public spectacles of torture and executions that induced compliance through fear and horror, governing bodies through discipline takes place without macabre physical force.

Exercising power in these disciplinary societies requires so-called 'total institutions', which are distinct, heavily regulated architectural entities and social environments of constant surveillance (Foucault 1977). In these enclosures, the constant awareness of

being watched by an invisible force creates an internalisation of control. As subjects of surveillance are unable to pinpoint the overseer, they adjust and normalise their behaviour even when it is not necessary (Koskela 2003). Total institutions then "manufacture conscience" (Tabor 2001: 128) through surveillance. The panopticon is the archetype of such a total institution. It enables surveillance in its purest and most radical form: a linear, top-down relationship between the watcher and those under surveillance, totalising and dominating.

The Panopticon's Changing Fortune: Appeal, Application, Critique

The panopticon's analytical appeal for understanding surveillance rests in its flexibility of application and multi-layered nature, it is "both fragmented and unified at the same time" (Whitaker 1999: 143). In surveillance theory, the panopticon can be understood as a panoptic spectrum, with Bentham's prison at one end as the panopticon in its pure form, and strewn across it other real-world phenomena that appropriate specific panoptic attributes. The example of CCTV surveillance illustrates this, where subjects of surveillance are not physically confined, the aspect of coercion is weakened, and the ability of resistance increased (Albrechtslund 2008). What remains is the notion of a spatial architecture of surveillance and a vertical relationship of visibility between known subjects of surveillance and an unknown, omniscient watcher. In contrast to Sartre's 'gaze', which offers a similarly objectifying relationship of visibility (Sartre [1943] 1993), the panopticon stands in a broader social and political context that can be selectively historicised beyond Foucault's 18th-century focus.

Beyond the literal application of the panopticon, two general strands of theory have emerged that support the longevity of the concept. Out of these, one set of theory suggests that the increase of surveillance in contemporary societies further inflates Foucault's concept into a 'superpanopticon' (Poster 1990), 'global panopticon' (Gill 1995) or 'omnicon' (Goombridge 2000). A second set of theories conceptually reworks the panopticon in order to mould it to new realities, such as changed parameters between watchers and watched and new power relations inherent in those parameters. Hence the 'synopticon' suggests that in a mass-mediated society, surveillance is expressed by the many watching the few, and not the few watching the many (Mathiesen 1997). The 'polyopticon' (Allen 1994) introduces a multiplicity of relations of visibility and the

‘cybernetic panopticon' (Bousquet 1998) and the ‘neo-panopticon’ (Mann et al. 2003) seek to bring the concept into the digital realm of computers.

Iterations of the panopticon have become so prominent that Lyon (2006) diagnoses a flourishing panopticism in surveillance studies. Haggerty (2006) laments that the inability to abandon the panopticon metaphor has effectively turned surveillance studies into panopticon studies, conflating the panopticon with surveillance itself, to worrisome implications:

> “The sheer number of works that invoke the panopticon is overwhelming. More problematically, the panoptic model has become reified, directing scholarly attention to a select subset of attributes about surveillance. In doing so, analysts have excluded or neglected a host of other key qualities and processes of surveillance that fall outside of the panoptic framework. The result has been that the panoptic model has been over-extended to domains where it seems ill-suited, and important attributes of surveillance that cannot neatly be subsumed under the ‘panoptic’ rubric have been neglected.” (Haggerty 2006: 23)

Yar (2003) finds three types of critical responses to the panopticon. There are those like Norris & Armstrong (1999) who see a problem of degree rather than kind. Such approaches accept the concept of panoptic power in principle but caution against blindly reproducing it across all surveillance settings. Another type of criticism focuses on the temporal and geographical applicability of the panopticon. It argues that the socio-historical context of the panopticon was limited to 18th century Europe, failing to capture surveillance in globalised contemporary societies. So-called ‘post-disciplinary’ accounts like Bogard (1996), Bauman (1988) and Rose (1999) propose alternative frameworks for surveillance which, as their common label suggests, seek to realign socio-historical reality and theoretical approach. Lastly, Yar considers approaches that revise or extend the panopticon as a form of criticism. This is different from my own framing of these accounts which follows Haggerty (2006) and Lyon (2006). I share their interpretation that such revisions of panopticism are expressions of endorsement that hinder more relevant engagements with surveillance.

In his critique, Yar subsumes Boyne (2000) in the category of those who reformulate the panopticon and grant it staying power. However, I argue that Boyne’s argument is more complex than Yar’s analysis suggests, and of particular merit to this particular research project. In his ‘post-panopticism’, Boyne advances a critique that joins up existing characterisations of surveillance in the context of changes in modernity into an explicit

argument against the panopticon and combines this with an interrogation of Foucault's underlying assumptions. His account is instructive for the theoretical framework of this research project because it references both the mediatisation of surveillance, its computerisation as well as offering a perspective on agency.

Boyne proposes a categorical transformation of surveillance in five arguments. Drawing on Bauman, he firstly highlights that discipline as a principle of social order has been replaced with the idea of seduction. Secondly, he argues that post-panoptic subjects watch over themselves instead of being watched over by "central executive functions" (Boyne 2000: 300). Thirdly, he concurs with Bogard (1996) that as surveillance has become computerised, it has become future-directed and that such diagnostic surveillance is incompatible with the panoptic model. Fourthly, he sees a "reversal of the Panoptical polarity" (Boyne 2000: 299) through models like the 'synopticon', which changes the uni-directional and totalising notion of watching. Lastly, Boyne suggests that the idea of discipline itself is a historically specific manifestation of the self in Christianity which is under pressure today as concepts of self have changed towards a liberatory and self-expressive paradigm. He argues that the contemporary self is not amenable to Foucault's idea of 18th-century discipline and would rebel to such an extent that physical force would be needed to sustain order. Instead of producing 'docile bodies', the panopticon would dismantle itself. Boyne concludes that the panopticon should be dismantled, but also that it should remain as a reference point against which contemporary theory of surveillance positions itself.

'Docile Bodies' and the Limits of the Panoptic Paradigm

For the central question of this research, agency towards surveillance, the 'docile bodies' hypothesis stands out as an aspect of critique. While Boyne (2000) principally considers this idea in the context of a socio-historical transformation of the self, its limitations are much more poignant when it comes to agency and thus requires further exploration. Accepting the 'docile bodies' paradigm means acknowledging that individuals are passively exposed to power (McNay 1994). This *a priori* negates the very possibility of agency and renders any such inquiry impossible. The ongoing prominence of the panopticon in surveillance studies then helps explain why debates have mainly focussed on the perspective of watchers over those under surveillance. However, such a focus is

insufficient, and Lyon has underscored that beyond well-acknowledged issues of power, surveillance also is about personhood:

> "Persons, by which I mean social, embodied subjects, are often aware of surveillance and they interact with it in an imaginatively complex range of ways. At the end of the day, it is also flesh-and-blood humans who are affected by surveillance, for better or for worse, and thus whose life-chances and whose choices are at stake when any surveillance system is in place that touches their lives. Several debates about both power and personhood must be explored […]." (Lyon 2007: 24).

The presumption that bodies are docile does not allow to consider personhood. Even total institutions themselves do not produce docile bodies and afford at least some agency, as Goffman (1961) has shown in his study of mental asylums, where the inmates subvert the guards' orders. Similarly, studies of resistance indicate how agency can be considered in surveillance research once researchers rid themselves of the docile bodies paradigm (e.g. Albrechtslund 2008). In a nod to Goffman, Yar then proposes that a theoretical reconsideration of surveillance requires a change of method as well:

> "Sociologically, it is suggested that the precise relation between surveillance and self-discipline requires us to attend, in ethnomethodological fashion, to the situated sense-making activities of subjects as the go about everyday practical activities […]." (Yar 2003: 254)

Critiques of the panopticon, and in particular the dismantling of 'docile bodies', provide justification for abandoning a grand theory of surveillance. However, as Boyne (2000) indicated, despite the fact that the panopticon is dead, it remains analytically productive: Yar's argument to emphasise the sense-making of subjects in everyday life itself is a consequence of the shortcomings of the panopticon. Paradoxically, in the debate for or against the panopticon, Foucault himself might have joined the side of critics and dismissed extensions and reinterpretations of the panopticon:

> "[…] to use Foucault's concepts in the manner of universals […] goes against the grain of his own insistence on using concepts as *a posteriori* 'principles of intelligibility' rather than as *a priori* universals, even when they are historicized to fit current practices […]." (Voruz 2013: 127, original emphasis)

Yet Foucault offers other principles of intelligibility beyond the panopticon, which means that his influence on surveillance theory remains notable. I illustrate this in the next section.

Foucault After the Panopticon

In light of the pervasive criticism of the panopticon, surveillance scholars have turned towards Foucault's later idea of governmentality as an alternative paradigm for theorizing surveillance (Haggerty 2006). Unlike the panopticon that regards power as totalising, governmentality proposes that power is at once totalising and individualising (Foucault 1991). On the one hand, the state aims to rule the individual continuously. On the other hand, it can best do so by involving non-state authorities in governance and by encouraging freedom, provided freedom is exercised in a well-regulated and responsible manner. This way, the state can avoid using force and outsource responsibility (Barry et al. 1996). In such a configuration, individuals participate in their own governance through 'technologies of the self' (Rose 1999) which stand for techniques to watch over, and take care of themselves. While surveillance is the price paid for such freedom (Rose 1999), recent scholarship also shows that surveillance is itself a mode through which freedoms are enacted. For instance, Ouellette & Hay (2008) argue that amidst the retreat of the state in neoliberal societies and the privatization of welfare, the public gaze of often disenfranchised people on reality TV provides blueprints for self-help and self-responsibilisation. Governmentality hence sees individuals not merely as subjected to power, but affords them an active role and thereby grants them the possibility for agency that the panopticon denied. At the same time, governmentality is not embedded in a grand theory of surveillance, which makes it more flexible in its application. Governmentality acknowledges that surveillance is designed into many aspects of everyday life and enables situated, meso-level approaches that recognise the particular rationale of each surveillance configuration. This is particularly useful for perspectives on types of surveillance that rely on data collection and processing across very different contexts and objectives, from urban policing to consumer monitoring (Lyon 2007; Haggerty & Ericson 2000). Taken together, these attributes would suggest governmentality as a suitable candidate for understanding agency towards contemporary surveillance. However, governmentality falls short of its promises.

Firstly, governmentality merely permits responses to surveillance that do not critique or undermine it. This becomes apparent through the technologies of the self that inform governmentality. Technologies of the self present themselves as a range of options which are provided by a governmental culture (McNay 1994). They only allow individuals to take care of themselves within a certain range of practices, as long as individual acts are

not detrimental to the ambitions of top-down power. Agency is thus constrained and pre-engineered. Moreover, any such agency, however limited, depends on accepting surveillance in the first place, as surveillance enables the very freedoms that people are granted.

Secondly, governmentality is concerned with issues of power and how they sustain a system and logic of governance. It is not preoccupied with the subjective, lived experience of such regimes and lacks the conceptual catalogue to develop such a perspective. The notion of agency, and human actors themselves, remain untheorised. Haggerty (2006) has therefore stressed that surveillance studies need to look beyond governmentality if they want to take serious the perspective of human agents. The idea of the self, and with that agency, becomes more prominent in Foucault's later work on the history of sexuality (Foucault 1976). Foucault develops an ethics of the self which establishes an account of human subjectivity. However, this ethics stands removed from a wider theory of power and has received criticism for its opaque notion of a Baudelarian aesthetic, hampering its use (McNay 1994).

As the applicability of the panopticon to surveillance wanes, surveillance scholars remain interested in Foucault, mainly due to his detailed work on power and governance, which are core aspects of surveillance. While governmentality overcomes many of the limitations of the panopticon, it still does not permit to look at relations among actors, and in particular subjects of surveillance. Doing so requires considering alternative frameworks outside of a Foucauldian tradition.

2.2. A New Framework for Surveillance

So far, I have documented the complexity of surveillance in contemporary society and have highlighted the proliferation of multiple theoretical approaches from classic social theory over approaches located in a critique of modernity, to Foucault's panopticon as the predominant template for understanding surveillance. I have concluded that overcoming the legacy of the panopticon is a prerequisite for considering agency towards surveillance and that newer paradigms in the Foucauldian tradition by themselves fall short of this task. In this analysis, I have stressed that a grand theory of surveillance needs to be replaced by a situated approach specific to the surveillance problem at hand. Lyon offers a sense of orientation. To formulate a situated approach, he proposes a taxonomy

of surveillance sites that range from "military discipline and intelligence", "state administration and the census", "work monitoring and supervision", "policing and crime control", to "consumption and making up consumers". (Lyon 2007: 27, 30, 33, 36, 40). Yet a focus on surveillance sites alone neglects the importance of choosing a particular perspective on such sites. Given the problems of surveillance studies with the notion of agency, my interpretation of a situated approach expands on Lyon's original proposal. Instead of focussing on sites of surveillance per se, below, I outline a site-specific approach through the prism of agency. Specifically, I describe the parameters for such a situated approach, in how far the conceptual repertoire of surveillance studies is capable of addressing them, and whether a broader analytical framework outside of surveillance studies is required, in particular as surveillance now takes place within a wider computational transformation. What I outline below is not a theory of agency towards computational surveillance as such, which will follow in the next chapter. Instead, I delineate the factors that it needs to consider and propose a way forward. I begin by proposing the notion of interactivity as a concept that helps define the particular issue of surveillance in question. I then argue that interactivity provides a template on which numerous expressions of agency can be considered. Outlining these possible expressions of agency, I embed them in a broader framework of the self in contemporary society. I conclude by discussing two possible ways forward in translating such a situated approach to surveillance into a theory of agency.

2.2.1. Information, Surveillance, and Interactivity

More than two decades ago Lyon (1988) projected that the politically and socially most significant aspects of digital information technologies would be their data-processing capacities. However, surveillance is not merely a consequence of information. Rather, the two concepts are mutually constitutive and inextricably intertwined. Using interactivity as a binding concept helps to explain this relationship. Whilst there is a lack of clarity among scholars how to exactly define interactivity (Kiousis 2002), a key characteristic is the two-way flow of information it enables. Interactive space is a realm in which every action generates information about itself (Andrejevic 2007) through a feedback channel. Interactive space can thus be considered as both an information and a surveillance space. This mutuality of information and surveillance is documented by Andrejevic in the context of digital television platform *TiVo*. By the act of watching, audiences generate real-time information about their viewing habits which through a digital interactive

channel is delivered back in a continuous stream to the sender. The analysis of this information facilitates for instance targeted advertising and informs the kind of content which will be aired in future on the principles of the ratings industry (Andrejevic 2007). On the internet, the feedback opportunities far extend this example and are in principle endless.

Whilst Andrejevic paints a grim picture, the interactivity afforded by the internet has been heralded as a liberatory promise by others. Pool ([1983] 1984) articulates a deep optimism, seeing electronic media as harbingers of freedom through their ease of access, low cost and distributed nature, that only wrong political choices could undermine. De Kerckhove recognises in interactivity on the internet a shift in power from the producer to the consumer. He considers interactivity as a genuinely democratic concept which holds a liberatory potential that an analogue politics has failed to put to practice (de Kerckhove 1997). More recently, Deuze (2012) explicitly turned against critical perspectives:

> "[…] we have to let go of seeing media as influence machines that will eventually make us disappear, instead considering media as part of our lives to the extent that they will make us visible (again)." Deuze 2012: 264)

Against the stance these authors take, an etymological approach to interactivity reveals more troublesome implications. The concept of interactivity was originally coined in a military-technological discourse on computer sciences, known as cybernetics. Long before the proliferation of the internet, in the 1940s, a founding figure of this discipline, Norbert Wiener, developed the concept of cybernetics as referring to a mechanism of command and control, enhanced through feedback capacity. However, Wiener already pointed to potential social implications of this technical feedback mechanism and cautioned about misuse for purposes of social control (Wiener [1948] 2013). Before the concept became prominent, its technical developer already became its first critic.

Andrejevic goes even further back in time and traces a use of the term cybernetics before it became a scientific concept associated with technology or even 'the media'. While Wiener's take on the term reveals that interactivity is much more ambivalent than Deuze and de Kerckhove frame it, Andrejevic highlights an outright anti-liberatory origin of cybernetics. He traces a first use of the term in an article by Clerk Maxwell in 1868 on governors. Maxwell borrowed the term cybernetics as a pseudo-latinism from the Greek

term *kubernetes*, which can be translated as ‘steersman’. This evidence leads Andrejevic to conclude that cyberspace from its very inception is a steered, a directed space which clashes with liberatory promises articulated by de Kerckhove and others (Andrejevic 2007). Such assessments of interactivity offer two perspectives on the way towards a theory of agency.

Firstly, the notion of interactivity helps specify the surveillance environment this study seeks to address. The role of interactivity has recently been recognised by a range of inquiries that combine the context of media and communications with a perspective on surveillance, such as in Turow’s (2006; 2011) work on digital advertising and personalisation, Halavais’ (2009) analysis of search engines and surveillance, debates around surveillance as a force in digital labour (Scholz 2013) and Zuboff’s (2015) diagnosis of surveillance capitalism that underpins *Google* and other online companies. These studies help specify the site of surveillance that this study seeks to address and fills a gap in the portfolio of surveillance studies. While Gandy (1993) put the issue of dataveillance - the collection, structuring and storing of information about individuals for surveillance purposes - on the agenda of surveillance studies, it had been principally applied to issues such as the merging of government and commercial databases or the multi-source tracking of individuals using credit card information, health records, and similar sources in a post 9/11 environment of political risk management (Gandy 2003). When it comes to the focus on media, surveying the past issues of the journal *Surveillance and Society* reveals that surveillance studies have predominantly emphasised representations of surveillance in the media over the media as a context in which surveillance (Surveillance and Society 2002-2015) takes place. Lyon (2007) posits that the intersection between media and surveillance remains under-researched, and an area in which surveillance studies should develop. The notion of interactivity allows this by neither prioritising surveillance nor the mediated environment that people find themselves in. Instead, it regards them as mutually constitutive. This perspective is particularly useful for this study because it connects the theme of dataveillance to the broader trend of ‘datafication’ (Kennedy et al. 2015), or the rendering of the social world as such through data and its computation, that will be discussed in *Chapter Three*.

The competing utopian and dystopian narratives of interactivity secondly suggest that agency towards surveillance is a complex matter. They evoke the Janus-faced nature of

surveillance (Lyon 1994) and hint at contesting ideas of how agency should manifest itself – as a futile endeavour due to the notion of control inherent in cybernetics, as expression of resistance against those powers, or indeed as a liberational force. In the next section, I further specify these configurations of agency and how they inform a path for studying surveillance.

2.2.2. Configurations of Agency

Accounts of agency towards surveillance are scarce and come with a range of limitations. They generally focus on isolated empirical domains such as shopping centres or webcams, or particular types of agents such as advocacy groups (e.g. Albrechtslund 2008; Introna and Gibbons 2009; Koskela 2003) and are not supported by a theoretical framework. In one of the rare broader accounts, Gary T. Marx outlines eleven tactics to "subvert the collection of personal information" (Marx 2003: 369). His taxonomy transcends particular settings and is geared at forms of data-driven surveillance more widely. However, it is not generated from an empirical analysis and more programmatic than analytical. He also sees these techniques as exceptions and thereby relegates agency to a niche phenomenon. Inherent in all such accounts is an *a priori* focus on particular modes of agency as either resistance or complicity, with resistance as the dominating theme. This excludes more complex configurations of surveillance such as those implied in the notion of interactivity.

Below, I propose that firstly, increases in depth and scale of commercial surveillance on the internet affect individuals throughout everyday life, and not just in limited encounters. However, the ways in which this happens are not transparent to individual agents. Secondly, I argue that the internet is not merely more interactive than previous media, but that there are new kinds of interactivity at play. Supplementing the concept of interactivity with the notion of generativity (Zittrain 2008) helps to better understand complex relationships between online surveillance and individual agents in a world where the general relation of humans to computers has been transformed: "Generativity is a system's capacity to produce unanticipated change through unfiltered contributions from broad and varied audiences" (Zittrain 2008: 70). This implies that a generative system is open and mouldable, which both invites participation as well as new and flexible forms of surveillance. The manifold implications of generativity provide a framework which can accommodate contradictory views on interactivity as liberating or dominating, and

which sees people as both subjects of surveillance and active agents in the surveillance process. This requires a more complex understanding of agency beyond straightforward resistance or complicity. I illustrate this through the awareness of consumer surveillance, user-generated surveillance, and the broader socio-biographical context in which surveillance on the internet takes place. On this basis, I evaluate two possible ways forward in arriving at a theory of agency.

2.2.3. Consumer Surveillance and Individual Awareness

In a review of consumer attitude surveys, Turow demonstrates that while most Americans are aware of the fact that websites gather information about them and are familiar with the concept of a web cookie, this knowledge does not translate into a deeper understanding of data flows and techniques by which online organisations derive, filter, manipulate and exchange information about them. Nor are websites' privacy policies comprehensible to consumers:

> "[t]he reactions of most online-at-home adults to a common way websites handle visitors' information indicate that they do not understand the collection, interrelation, and use of identifiable and anonymous data." (Turow 2006)

Such knowledge becomes more vital as the surveillance activities and capacities of the commercial sector are superseding those of the nation state, as Whitaker already observed nearly a decade ago (Whitaker: 1999). Even earlier, Oscar Gandy hinted towards the economic significance of personal data for targeting the right consumers. This economy of personal information has, Gandy claims, implications far beyond issues of privacy protection as it uses technology to enact a discriminatory logic which discards of less attractive potential customers while 'skimming-off' others as "high quality targets of opportunity" (Gandy 1996: 152). An increasingly sophisticated and interlinked process of data collection and analysis allows the institutionalisation of these processes through the categorisation of consumers based on social sorting techniques (Lyon 2007) and thus the variable creation of social divisions of which consumers may not even be aware.

This emerging process marks a fundamental turning point in the relation between individuals and categories. For decades, marketing companies have been analysing social groups based on gender, income and other variables and tried to target people which they believed belonged to this group. However, with the rise of data-mining, this process is being reversed as marketers gather vast amounts of data on individuals to separate them

into desirable customers (‘targets’) and unnecessary expenses (‘waste’) to be avoided (Turow 2011). Together with the automation of advertising planning, buying, selling and delivery through algorithmic processes, this results in consumers being grouped in categories that are being built from the ground up, or individually tailored advertising messages (Turow 2006). Industry research suggests that this so-called ‘programmatic advertising’ is becoming the dominant mode of advertising on the internet (Knapp & Marouli 2015). As advertising-funded content on the internet comes under increasing pressure despite these advances in targeting, mainly due to low advertising margins and fragmenting consumption, these targeting principles are starting to be applied to editorial content itself, performatively modulating websites and the presentation of content to individual users based on their data signals to drive audience loyalty (Couldry & Turow 2014).

According to Turow, consumers become at least diffusely aware of the fact that they are treated according to certain data-driven assumptions. Trying to evade questions about privacy intrusion, marketers are increasingly shifting towards an invitation-based business model where they ask desired customers for personal information in return for special discounts on their products. This enables consumers to partly influence whether they are being elevated to a preferred customer category or not. However, the rationale behind such measures is difficult to comprehend for consumers and there is a great degree of uncertainty which actions will trigger desirable responses (Turow 2006).

This has implications for the way in which consumers think tactically or strategically about their actions online. Whilst most surveillance writers focus on the categorisation aspect of data mining which acts upon consumers, (see Lyon 2007), Turow opens up a way to think of how consumers themselves deal with and act in the face of online marketing:

> “[consumers] will find it difficult to decipher what marketers and media think of their social status. The envy and suspicion that result from that insecurity will generate new worries about how to reveal oneself in public when doing so may reveal information that may be inserted into databases and may then have unknown consequences for one’s own social choices.” (Turow 2006: 187)

What Turow describes is a two-way process of how consumers deal with information about themselves – either holding it back to be used for certain purposes or to actively use the display and exchange of such information for their own benefit. Whilst

acknowledging limitations which consumer action towards commercial top-down surveillance has, this approach goes beyond a linear model which suggests that consumers are merely exposed to data-mining surveillance and passive subjects in the process of category creation (such as Gandy 1993).

The metaphor of the 'glass consumer' developed by Lace supports Turow's argument. While a straightforward interpretation of the term would indeed merely suggest that data collectors "can almost see through us" (Lace 2005a: 1), she extends the metaphor to a more nuanced analysis about consumers themselves, likening their role in societies saturated by surveillance to "properties and capacities of glass - fragility, transparency, the ability to distort the gaze of the viewer" (Lace 2005a: 7). Apart from underscoring the vulnerability that people experience when being exposed to surveillance, Lace's metaphor acknowledges 'capacity' expressed through 'distortion', and thereby highlights the possible active role of those under surveillance. The proliferation of data-mining and social sorting techniques demonstrates that people's skills in dealing with such surveillance for instance through distortion to generate personal benefit or to avoid negative consequences, is increasingly relevant for the management of individual life-chances.

2.2.4. Generativity and User-Generated Surveillance

Online surveillance does not end with surveillance based on a hierarchical and fixed relationship between watchers and those being watched. Turow already implied this when he attributed to consumers a degree of choice about what information they intend to hold back and what they want to communicate. This presupposes awareness about one's owns potential to be surveilled and can go beyond making marketing choices to wider issues of self-surveillance, such as checking which information about oneself can be retrieved on the web through ordinary tools like search engines. In fact, a survey by the *Pew Research Center* noted an increase in American adult internet users who regularly search for themselves online by 22% to 64% between 2003 and 2007 (Pew Internet: 2007). This not only suggests an increasing user awareness about the role of search engines in the portrayal of personal information, but also the need to monitor and keep up to date with the flow of information about the individual self on the internet.

In addition to self-surveillance, internet users may be surveilled by fellow users or engage in such practices themselves. Andrejevic (2005) uses two terms to frame this

phenomenon; ‘peer-to-peer surveillance’ and ‘lateral surveillance’. The term ‘peer-to-peer surveillance’ grasps a new constellation of actors in the surveillance process. Both the watchers and those being watched are ordinary internet users, suggesting that no party with different structural properties (such as a company, or the state) needs to be involved in the surveillance process. The term ‘lateral surveillance’ underlines the power relationship between those parties. Lateral surveillance is not a top-down hierarchical process, but a more or less horizontal one. Although some users may be more internet-literate than others, they do not have fundamentally different tools or infrastructures at their disposal. In contrast to Andrejevic, Albrechtslund (2008) uses the term ‘participatory surveillance’ in order to highlight the active role of the individual in the surveillance process.

The differences between Andrejevic and Albrechtslund are not merely terminological. Albrechtslund mainly regards participative surveillance as a form of entertainment, fuelled by the curiosity to find out what peers are doing, without seriously dominating or controlling implications (Albrechtslund 2008). However, although peer-to-peer surveillance involves actors with similar structural properties, it may have controlling aspects, such as the desire to conduct background checks on potential dating partners in the online dating culture, as Andrejevic (2005) highlights.

I suggest a further distinction. Practices of peer-to-peer or self-surveillance are not merely forms of naïve surveillance which draw on information available in the public domain, such as using *Google* or browsing someone’s photos on *Facebook*. Consider the life-tracking websites which employ sophisticated opportunities to chart and analyse information using algorithms. These websites represent a ‘function creep’ (Winner 1977), a spill-over of the logic used in commercial data-mining surveillance technologies to the consumer realm.

User-generated surveillance practices, despite happening without clear-cut top-down implications which are characteristic of commercial data-mining, are far from straightforward phenomena, both in terms of their motives and technological characteristics. This is something which the concept of interactivity fails to grasp. Instead, understanding the internet as a generative system capable of accommodating unfiltered contributions from a variety of parties (Zittrain 2008) opens a way to understand that users can – at least partly – design and mould their own tools and environments of

surveillance. Not only can they adopt new practices towards existing technologies, such as turning *Google* into a tool for self-surveillance. More profoundly, they can also design and contribute to entire surveillance-based internet communities, such as life-tracking sites which create new surveillance environments. This implies that not only are individuals in their everyday actions online exposed to an existing surveillance infrastructure which they have to come to terms with. They are also involved in the creation and proliferation of new surveillance contexts and the voluntary submission to such contexts.

2.2.5. Surveillance and Concepts of the Self

Just as concepts of surveillance need to be understood in the context of macro-social transformations, so does agency towards surveillance need to be embedded in a broader framework of the self in society. As Giddens (1990) points out, in the break-up of the traditional world order the rule of God was replaced by the faith in rational progress. However, in contrast to the rule of God, the concept of rational progress was ill-equipped to be an ontological safe-haven for the subject. As Touraine points out:

> "Modern society was born of the break-up of the sacred world order and saw the divorce between rational instrumental action and the personal subject." (Touraine 1995: 215)

What he means is that there is a dualism inherent in modernity: The detachment from the rule of God on the one hand features the advance of reason and on the other the disembedding of the subject. Giddens puts it more clearly when he states that

> "[m]odernity is a post-traditional order, but not one in which the sureties of tradition and habit have been replaced by the certitude of rational knowledge. Doubt, a pervasive feature of modern critical reason, permeates into everyday life […] and forms a general existential dimension of the contemporary world." (Giddens 1991: 3)

This existential dimension fostered through doubt can be mapped as a threat to the ontological security of the self. Giddens understands ontological security as possessing answers to existential and fundamental questions of human life which are under siege in a late-modern order that cannot replace the certainties of tradition. Instead, self-identity has become a reflexive project in an environment of uncertainty and multiple choice. In contrast to the deterministic order of a traditional society, it is up to the individual self to sustain a coherent biographical narrative which has to be revised continuously in a context

of multiple choice (Giddens 1991). Surveillance is an aid to a biographical narrative as Ouellette and Hay's (2008) work on reality TV has shown through a Foucauldian framework. However, it can also be a threat to ontological security as it robs agents of their ability to craft their own narratives and, for instance through data mining, creates alternative narratives which are obscure and opaque to individual agents. In the words of Ulrich Beck (1992), surveillance is both an expression of risk society in that it produces unanticipated consequences for the very acts and people that it monitors, but acts as a way to mitigate risk as well by rationalising and ordering oneself.

2.3. A Way Forward: De-Centring Surveillance Theory

The question of agency is situated in a complex set of relationships between human agents and surveillance. These relationships reference several conceptions of surveillance summarised by Boyne (2000) in his critique of the panopticon. They contain the element of consumer seduction that Bauman (2001; 2005) has advanced, the distributed and networked nature of surveillance (Gandy 1993; 2003) that is aimed at control, management and foresight instead of discipline (Deleuze 1992, Bogard 1996), as well as the transformation of roles and distribution of power which concepts like the synopticon (Mathiesen 1997) propose. While surveillance itself may be driven by general (power) and specific motivations (e.g. marketing, terrorism), so are human agents' engagements with surveillance expression of broader social forces. In order to take account of this complexity, two possible approaches to agency emerge. One is rooted within the paradigm of surveillance studies and merely extends it. Another argues that surveillance is too narrow as an analytical framework to capture the issues at play, and that consequently surveillance itself needs to be embedded in a broader framework. In this section, I outline and extend the first option based on existing surveillance scholarship. I then develop a second approach and offer an argument to pursue the latter.

A first approach to develop a theory of agency towards surveillance from this scenario would be to follow in the footsteps of theoretical assemblages as propagated by Hacking (2004) that combine disciplinary or post-disciplinary surveillance theory with a micro-sociological approach. While one has to be careful in merging such distinctly different perspectives, Hacking (2004) suggests that it is possible to combine a Foucauldian view with Goffman's bottom-up approach by drawing on Foucault's work on discipline (Foucault 1977) and Goffman's work on total institutions (Goffman 1961). Goffman

throughout his work developed a theory of rules which govern the way people interact with each other from the points of view of how they are performed. He was interested in how everyday situations are defined by actors aiming at a social consensus, being co-operative and egalitarian, as well as in situations in which the definitions of a situation by one actor or team of actors could be used to control others and thus become a form of power. He studied this in the context of mental hospitals where his main interest was not in studying how supervisory staff exerts power on inmates, but rather in the ways in which patients were able to circumvent and avoid fulfilling the intentions of supervisory staff. While patients were watched over, they could not all be changed or 'cured' in the desired way, due to their purposeful actions as subjects. This does not mean, however, that they remind entirely unchanged. As Goffman observes:

> "[the self] is not a property of the person whom it is attributed, but dwells rather in the pattern of social control that is exerted *in connection with the person himself and those around him.*" (Goffman 1961: 168, my emphasis)

Hacking draws on this observation and summarises that:

> "The changes are not deliberately brought about by the system of control, but instead take place in the presence of another person, and by virtue of this presence […] Each person learns to behave whether by concealing one's feelings, by affirming one's central role or by a tactical effacement." (Hacking 2004: 194)

As a Foucauldian scholar, Hacking thereby erodes firm distinctions between surveillance power and subjects of surveillance and re-introduces the subject into Foucauldian theory in a way in which it can both comply with or resist modes of governance.

Such an approach gains additional value if complemented by drawing on de Certeau who engages with Foucault and sketches out commonalities and differences. De Certeau criticises that Foucault "privileges the productive apparatus [of power]" (de Certeau 1984: xiv), whereas he intends to look at not how order is reinforced through productive technologies, but "to bring to light the clandestine forms taken by the dispersed, tactical, and makeshift creativity groups or individuals already caught in the nets of 'discipline'" (de Certeau 1984: xiv-xv). Goffman (1961) puts an emphasis on the performance element of social action and his concepts like 'front' or 'backstage behaviour' can provide valuable insights into how people try to negotiate their appearances in an online world where front and backstage cannot be easily maintained. Introducing de Certeau's concepts of tactics and strategies emphasises a stronger element of power struggle and

allows the analysis of specific acts which emerge out of the surveillance situation and are not rooted in pre-existing role conceptions.

Yet there are major drawbacks to formulating a theory of agency towards surveillance on this basis. It assumes that surveillance itself is the implied interlocutor that people relate and act towards. Post-disciplinary surveillance theory, in particular, has highlighted the role of data in concepts like ‘dataveillance' (Clarke 1988). But such reformulations of surveillance theory away from the panopticon have nevertheless assumed that surveillance has remained a standalone concept. They have not reconsidered how data and the proliferation of computation alongside it change the relationship between surveillance and its environment. In fact, the pervasive nature of surveillance today also means that it is embedded within other social processes. The notion of interactivity and the intersection between surveillance and information indicate this. Similarly, the informationalisation of surveillance coincides with a change of surveillance agents, from the guard in the watchtower to data, code, algorithms and software. A theory of agency towards surveillance, therefore, needs to be seen in the context of broader social changes. It needs to take into account the complicit, or even constitutive role of computation in shaping the social world, what Kallinikos (2009) has called the ‘computational rendition of reality’ and how such processes and operations bring about new configurations of agential forces (Van Dijck 2013). It also needs to explore the modalities of interaction which human agents can engage in and which emerge in such a world.

Based on these shortcomings and requirements, a second perspective then emerges. I propose to de-centre surveillance studies and instead embed the question of agency towards surveillance in a broader framework of social theory that considers the role of computation in making up the social world. This also addresses another drawback of surveillance studies. Their historical focus on systems and institutions of surveillance has foreclosed a systematic debate around agency. If agency is being discussed, this mainly happens in an empirical environment (Albrechtslund 2008; Koskela 2003), and not through a theory of agency. As surveillance is about power and personhood (Lyon 2007), it requires a theory that considers the structural forces of surveillance and agency in combination. But theoretical approaches from within surveillance studies are not set up to provide such a perspective. Hacking’s suggestion to pair Foucauldian theory with Goffman points in this direction. Yet it appears disjointed because it forcefully merges

two distinct theoretical strands, one of which is concerned with power, and the other with agency. It also does not theoretically enrich the specific socio-historical context of computation and mediated communication in which surveillance takes place. In contrast, social theory itself offers a rich portfolio of approaches that allow an integrated perspective on both structure and agency. In the next chapter, I will develop such a de-centred view on surveillance with the help of the broader range of social theory under special consideration of Kallinikos' (2009) notion of the computational rendition of reality and Berger and Luckmann's social construction of reality ([1966] 1991).

2.4. Chapter Conclusion

This chapter has discussed approaches to surveillance, how they have changed over time alongside the make-up of society itself and manifestations of surveillance, and explored the suitability of those approaches to facilitate an understanding of agency towards surveillance. It has shown that approaches rooted in a critique of modernity and the panopticon develop a set of attributes characteristic to the surveillance which people on the internet encounter: distributed rather than concentrated in nature, residing in computers rather than in panoptic watchtowers, with the intent of control, foresight and consumer seduction rather than discipline. Yet the chapter has also argued that the pervasive spread of surveillance in contemporary society coincides with particular expressions of surveillance that vary by context, which a grand theory of surveillance is unable to address. Ultimately, it has highlighted that as surveillance becomes a pervasive part of everyday life, a surveillance-centric theory is unable to grasp the issue of agency. To address this, the notion of surveillance needs to be de-centred and embedded in a broader context of social theory that recognises computation as a social force, and which possesses the conceptual repertoire to query the tensions between human agency and the social systems that people live in. This chapter has provided a foundation and justification for this approach, which is developed in the next chapter.

Chapter Three: A Framework for Agency in Computed Sociality

This chapter aims to overcome the limits of earlier surveillance literature by integrating it within a broader theory of agency in a world where not just surveillance but sociality itself is transformed by computational processes. Contemporary surveillance manifests itself in a particular logic of accumulation and extraction of information that is expression of a much deeper transformation at the foundation of modern societies brought about by computation (Zuboff 2015). Silicon Valley venture capitalist Marc Andreessen (2009) proclaimed that *Software Is Eating The World*, diagnosing a comprehensive rearchitecting of commerce and consumption through programs, apps and digital platforms. The notion of big data is reconfiguring how data are produced, managed, stored, interpreted and applied, leading to "the worlds we inhabit to be captured as data and mediated through data-driven technologies" (Kitchin 2014: xv). These are not just epistemological developments that affect the modalities of mediation. They have acquired ontological status:

> "[…] the 'stuff' that makes up the social and urban fabric has changed – it is no longer just about emergent properties that derive from a complex of social associations and interactions. These associations and interactions are now not only *mediated* by software and code they are becoming *constituted* by it." (Burrows 2009: 451)

This changes the coordinates in which an inquiry into the modes and possibilities of agency needs to take place, converting it from a question of surveillance into a broader investigation around the computational forces that underpin it. Against the background of a world constituted by software and code, Kallinikos has coined the term 'computational rendition of reality' to denote the computational factors that "[remake] key principles upon which social agents frame and act on the world" (Kallinikos 2009: 184). An important next step therefore is to investigate the implications for individual agency and the lived experience of actually inhabiting the world under these premises. Alaimo (2014) provides a precursor to such a discussion by expanding on Kallinikos' concept to show how data-driven interpretations of acts of consumption by online companies disaggregate individual practices, reaggregate them according to their own logic and recast them to consumers as representation of reality that in turn shapes consumers' experience. Bucher (forthcoming 2017) offers a perspective on how ordinary

people relate to computation on Facebook through the notion of ‘algorithmic imaginaries’.

My aim in this chapter is to contribute to the broader debate around computation by emphasising the angle of human agents themselves, who live within the reified outcomes of computation. I intend to help develop a language and conceptual catalogue that can accommodate everyday life under such conditions. Although my approach transcends surveillance, it is also relevant to surveillance in that I draw on people’s experience of computational surveillance as a context in which the problem of agency towards computation manifests itself. Indeed, Kallinikos' idea of the computational rendition of reality underpins Zuboff's (2015) analysis of surveillance capitalism, highlighting the close relation between computation and the original theme of surveillance.

Specifically, I propose a wider sociological contextualisation of the computational rendition of reality through Berger and Luckmann’s ([1966] 1991) social construction of reality. While Kallinikos is primarily concerned with the computational attributes that change the parameters in which human agents act, Berger and Luckmann provide a general theory about how people make sense of and legitimise the social world they inhabit as reality. At their time of writing, Berger and Luckmann could not anticipate the rise of computation as a constituent part of society. The computational rendition of reality offers an avenue to explore the modes and possibilities of constructing reality that Berger and Luckmann describe change through the introduction of computational forces. A reinterpretation of Berger and Luckmann in this vein ultimately allows considering the perspective of human agents under the conditions that Kallinikos outlines.

I select Kallinikos' concept as an entry point to discussions about agency over other diagnoses of computational forces because it connects the principles and processes of computation with a realm of experience - reality itself. It underscores that people live in a world that is already computed, and that is being perpetually recalculated at the same time. This implies both that people cannot act outside of computation and that the ongoing computational modulation of reality produces a context for agency. Such a perspective echoes Berger and Luckmann’s assertion that people create and reproduce reality within the parameters of a social world that they already inhabit, and not in a void, underscoring the compatibility of both approaches. However, to augment the analytical potential of such a joint perspective, I add one complication. I incorporate the computational rendition

of reality by proxy of an associated concept. The notion of computed sociality specifies the computational rendition of reality through a more explicit social dimension. It stands for:

> "[the] complex technological arrangements that recast sociality in a network of social affinities that are shaped by computational operations." (Kallinikos & Tempini 2014: 830)

Computed sociality underscores that computational mechanisms structure interaction between people (Tempini 2014). The focus on interaction makes the ideas implied in the computational rendition of reality more amenable to analysis under the prism of social construction. Berger and Luckmann emphasise that people create and reproduce reality through intersubjectively shared knowledge about the social world. Constructing and legitimising reality is a product of interaction. This specifies the particular problem of agency that comes to the fore in a computed world. If computation modulates interaction, the notion of computed sociality brings with it problems of the conditions of knowledge, or on what basis people can make sense of the world they live in. Computed sociality lends new urgency to investigating the production of knowledge, specifically how people can understand, intervene in and shape sociality that is recast in such ways. Ultimately, this poses questions how people can query and interact with the computational operations they are embedded in, and in how far the modes, affordances and limitations inherent in their interactions with computational operations themselves are expressions of computed sociality. Agency[10] becomes a problem of scrutinising and reclaiming the conditions under which knowledge of the social world is produced.

This chapter is composed of two parts. I begin by problematising the conditions of the production of knowledge in a computed world. To do so, I reframe the notion of computed sociality as a communication problem for human agents. Drawing on debates around algorithms, big data and related terms, I isolate particular characteristics of computation that jointly form a computational logic that defines computation as an interlocutor for human agents. I then document how this logic is embedded in everyday experience and

[10] In a critical review of the sociological literature on agency, Emirbayer & Mische (1998) highlight that "the term *agency* itself has maintained an elusive, albeit resonant, vagueness" (ibid. 962, original emphasis). They disentangle the various conceptualisations across theoretical strands and offer a generalised understanding of agency that tackles the concept's historic elusiveness. Acknowledging their argument, I outline my specific understanding of agency as associated with the conditions of knowledge in section '3.1. The Communication Problem of Computed Sociality' and reiterate it again with the aid of empirical material in *Chapter 9: Conclusion*.

juxtapose it with human agents' ability to make sense of the world. I propose a dichotomy of interface and infrastructure as a template to locate a communication problem. I argue that a computational logic operates through infrastructure, but that human agents' acts of constructing knowledge take place on the level of the interface, rendering the computational logic conceptually invisible. Finally, I argue that reclaiming agency requires a reconstruction of visibility as a mode of perception and expression of power to overcome the communication problem between human agents and computational logic.

In the second part of this chapter, I apply the communication problem of computed sociality to Berger and Luckmann's social construction of reality. I begin by outlining the authors' core concepts and probe their applicability in a world where computational forces structure reality. I then propose a reinterpretation towards the social construction of computed sociality. This reinterpretation is informed by various concepts within and outside of sociology, encompassing Lash's media ontology, Goffman's interaction rituals and glitch theory. Through such a revised account of social construction, I show how different social practices become possible through which human agents can interrogate and reclaim the conditions under which knowledge is produced.

3.1. The Communication Problem of Computed Sociality

A theory of agency ultimately asks how people can act in, and towards a computational world. Yet it needs to take seriously the nature of computation itself, how it affects the possibility of agency and how it structures the conditions under which agency takes place. Such a theory then requires a framework that explores the relationship between computational modes of shaping the world, and human agents' abilities to make sense of it. The underlying complexity of technological configurations that Kallinikos and Tempini (2014) ascribe to computed sociality already suggest that interaction between human agents and a computational order is fraught with difficulties. In this section, I will develop such a perspective by recontextualising the computational rendition of reality (Kallinikos 2009) - the computational, generative processes that underpin computed sociality - as a communication problem for human agents. Below, I outline this communication problem in two steps.

Firstly, I unravel the computational principles and processes that underpin computational reality with the aim for formulate a 'computational logic', which I understand as a

particular way of decision-making and acting on the world by computers in the widest sense. By describing such a logic, the constituent parts of computers as structural forces and new types of agents that shape the social world become tangible. A theoretical framework that places the lived experience at its centre, therefore, cannot start with agency itself, but requires a detour that systematically identifies those constituent factors that make up the computed world.

Secondly, I explore how a computational logic is embedded in lived experience. I propose that such a logic differs categorically from how human agents make sense of the world. This problematises how people can relate to the computational rendition of reality, and outlines the conditions in which people's construction of knowledge takes place.

3.1.1. Towards a Computational Logic

In recent years, several terms have gained prominence that seek to capture the computational principles and processes affecting socio-economic life, from 'algorithms' to 'big data', 'code' and 'software'. The discussions and conflicts surrounding these terms help outline a computational logic. For instance, in their critique of big data, boyd and Crawford (2012) problematise the promise of objectivity and the quality of insight associated with it, and point to the mythological rhetoric surrounding the term. Barocas, Hood and Ziewitz diagnose a systematic confusion in the use and definition of algorithms and seek "to trouble the coherence of the algorithm as an analytic category" (2013: 1). Such confusion and critique is productive because it isolates specific attributes of computation without having to appropriate the conceptual baggage and preconceived meaning that comes with each term. My interest does not lie in a comprehensive theoretical review exploring the capillaries of these debates. Rather, I seek to identify conceptual attributes emerging through them that allow for framing a computational logic as a communication problem. The notion of algorithms, in particular, has received recent scholarly attention. As terms are overlapping, for reasons of clarity, I select this concept as my point of departure. On this basis, I develop four characteristics that make up a computational logic: (1) performativity of algorithms, (2) physicality of algorithms, (3) epistemology of big data, and (4) human-machine complicity. By describing such a

'logic', the constituent parts of computers as structural forces and new types of agents that shape the social world become tangible.[11]

The Performativity of Algorithms

Despite assertions that algorithms are pervasive (Lash 2007), that they have crept into the fabric of everyday life (Burrows 2009), and the diagnosis of an 'algorithmic culture' (Galloway 2006), algorithms remain an elusive phenomenon. Even computer sciences struggle to formalise a universally accepted definition (Berlinski 2000), which Blaas and Gurewitch (2003) recognise as a foundational problem. Efforts to translate the notion of algorithms into the conceptual catalogue of the social sciences have sparked an array of competing interpretations that hamper a systematic understanding.[12] Approaches to algorithms ultimately are fraught with unclear and conflicting definitions that coincide with often bold assertions about how they operate and speculations about their effects, converting them into "somewhat of a modern myth" (Barocas et al. 2013: 1), or rendering them intangible and inconceivable (Röhle 2010).

However, from the perspective of theorising agency, the conceptual confusion is analytically productive. It hints at possible difficulties of grasping algorithms in lived experience, which in turn affects the ability to act towards them. The narrative of myth, and claims that algorithms cannot be studied, are connected to the idea that algorithms are performative; that they change in shape, form and intention. While performativity is just one among many characterisations of algorithms, it is a central computational characteristic for a theory of agency. Thrift has labelled algorithms 'performative infrastructures' (Thrift 2005) in the sense that they modulate outcomes for those who are subjected to them. Algorithms then have a capability for decision-making, which is at least partly autonomous and which generates flexible outcomes. Algorithms 'sort things out' (Bowker & Starr 2000), and they do so according to their own inherent, flexible, unstable rationales. This is particularly evident in the notion of machine-learning

[11] I understand the notion of 'computational logic' not as a monolithic logic that is the same across all contexts and manifestations. Acknowledging the multiplicity of configurations that a computational logic can take on the basis of its four constituent principles and their specific design and implementation, I use it as an ideal type and short-hand that always recognises its fluid nature.

[12] A detailed review of these lines of interpretation exceeds the scope of this thesis, but for an authoritative discussion of current debates, their shortcomings and proposals for new directions, see Barocas et al. 2013. Through 39 'provocations', the authors provide a catalogue of critical questions and theses about algorithms. They also offer a useful ordering of approaches, distinguishing between those who see algorithms merely as a "technology", as "form of decision-making", "epistemology onto itself", "form of rationality", "general mode of social ordering", and as "sociotechnical process" (ibid. 2013: 2).

algorithms, which self-improve and change over time, emancipating themselves from the original code that conceived them (Lewis 2014; Ailon et al. 2011). The spread of algorithms then stands for a new type of reasoning at odds with conventional forms of knowledge that people are familiar with, where "the algorithmic rules of rationality replaced the self-critical judgments of reason" (Daston 2013: para. 1).

The Physicality of Algorithms

Algorithms, in all their possible definitions, depend on a vast range of physical factors to be in place, orchestrated and optimised. Server rooms provide storage, computing power and electricity. Depending on its purpose, a server also needs to be connected to other servers within and across different data centres, as well to further networked components such as the trading desk at a bank, or data management platforms used by advertising agencies. Speed is a foundational logic of technologically advanced societies (Virilo 1986; 2005). In a growing number of industries, the speed with which signals are transferred and processed across these networks is paramount to outwit competitors. Competitive advantages to buying a stock or securing a winning bid for an advertising impression are articulated in milliseconds (Aldridge 2013). Under these circumstances, data centres have coined the concept of 'co-location'. As Lewis (2014) highlights, this denotes a mechanism of ordering where frequently interacting algorithms are placed in the same data centre, and even in a particular order within a data centre to further cut transaction time. Algorithms, therefore, are embedded in a spatial configuration expressed in new forms of centrality and periphery that emerge through telecommunication networks (Sassen 2005). Decisions about which routes on these networks algorithms chose to interact with each other are themselves influenced by algorithmic calculations. For instance, the succession in which a financial trading algorithm contacts stock market exchanges for pricing information is itself determined by a specialised algorithm (Lewis 2014). Algorithms then are networked and interact with each other (e.g. Hayles 2006). Physical factors affect this process. The particular configuration of these physical factors co-determine how self-improving algorithms evolve, which algorithm succeeds over another, which algorithms interact with each other, and ultimately what outcomes are generated.

The Epistemology of Big Data

Algorithms depend on data as a raw material that fuels their performative decisions, influencing how they evolve, act and which inferences they make. Only a decade ago, when the volume of data feeding into algorithms was comparably scarce, the complexity of an algorithm was its main competitive advantage. Today, data is available in abundance. *Google*'s chief economist, Hal Varian, estimates that "[b]etween the dawn of civilisation and 2003, we only created five exabytes of information; now we're creating that amount in two days" (as cited in Kitchin 2014: xv), and a range of studies observe a rapid growth in the volume of data generated and analysed (e.g. Hilbert & López 2011; Gantz & Reinsel 2011). Amidst this data deluge, simpler algorithms paired with a higher volume of source data are making more accurate inferences than complex algorithms that have to rely on relatively poor data material (Mayer-Schönberger & Cukier 2013). For instance, as Morozov (2015) argues, the contemporary market power of *Google* depends less on the sophistication of its algorithms, as it does on having access to, and hedging large sources of proprietary data that its algorithms can draw on.

The notion of data itself has witnessed surging attention recent years, as epitomised by the term 'big data'. Originally coined in the 1990s to denote management and analysis of large-scale datasets (Diebold 2012), by the late 2000s, it had become a buzzword across academia, industry, government and the media, often associated with hyperbolic claims of revolutionary changes and regarded as a fix-all for world problems from health to traffic congestion (e.g. Anderson 2008). A common framework to describe big data has come to be known as the 3Vs: data is at once large in *volume*, high in *velocity* as it is being created and analysed near real-time, and diverse in *variety*, containing various sources of data and types of data from structured to unstructured (e.g. Zikopoulos et al. 2012). As Kitchin (2013) demonstrates in a wider overview, further attempts have been made to refine these characteristics. These attempts include the idea that datasets are exhaustive (n=all), that big data dispenses of the sample altogether, or that it relies on unprecedented sample sizes.

Data have always involved categorisation. Suicide, a sociological interest since Durkheim, offers a perspective to illustrate this. In his analysis on the rise of modern statistics, Hacking (1990) posits that suicide was among the first human behaviours regularly counted. Alongside crime and other acts considered wrongdoings, or amoral,

these data started to fill up official tables of deviancy in the nineteenth century. Out of such tables, distributions and averages informed what was considered normal. Moral statistics were later extended by other variables to sort people more widely. However, these categories did not just depict people to those who sought to analyse them, but also described people to themselves:

> "One can ask: who had more effect on class consciousness, Marx or the authors of the official reports which created the classifications in which people came to recognise themselves?" (Hacking 1990: 3)

Data and classification thus are a modern way of generating reality, or as Hacking calls it elsewhere with a nod to Foucault, a 'historical ontology', that is a historically specific way of constituting people as "objects of knowledge, [as] subjects acting on others [and as] moral agents" (Foucault 1984, as cited in Hacking 2002: 2).

Beyond the 3Vs, big data stands for a new rationale of classification. Big data weaves together data as a raw material with a particular logic of inference that is governed by algorithms (Mayer-Schönberger & Cukier 2013). *Knowledge Discovery in Data* (KDD) is a common approach to handling large datasets. Here, algorithms sift through data sets to discover "emergent relationships among attributes" (Nissenbaum 2009: 44). Cheap storage and processing power in abundance have removed economic barriers that have previously required to structure and limit data set exploration. These limitations coincided with epistemological principles suited to draw inferences from such data, most notably the formulation of hypotheses and the principle of causality. Big data changes this by shifting focus from the cause of phenomena to the mere evidence of their occurrence. This causes a historical rupture in the epistemological foundation of societies. Furthering Daston's claim about algorithmic rules of rationality, this means that:

> "[…] society will need to shed some of its obsession for causality in exchange for simple correlations: not knowing why but only what. This overturns centuries of established practices and challenges our most basic understanding of how to make decisions and comprehend reality." (Mayer-Schönberger & Cukier 2013: 18)

While classifications through data have always shaped lived reality in modern societies, the process of arriving at these classifications could be queried and understood in principle by human agents. Established modern categories like class, or those in the media business denominating audience segments from 'housewife' to 'millennial', are accessible to those who fall into them. People know about these classifications, their

names and the socio-economic characteristics they signify. People can also anticipate which category they would fall in and shape their self-perception in either agreement or disagreement. They can position themselves towards those data and categories that seek to describe them. The logic of inference that underlies big data renders this impossible. Categories are emergent, unstable, classifications are buried within the computational calculations, do not have a name, and may not be intelligible by an outsider. As boyd and Crawford (2012) remind us, the volume of data also does not make it infallible and instead carries inherent biases and limitations rooted in unreliable source data and its misinterpretation. Gitelman (2013) stresses that the notion of 'raw data' in itself does not exist, and that the construction of any data corpus already entails values and judgements, which are themselves increasingly informed by computation. In light of such issues, Lash argues that power "enters into us and constitutes us from the inside" (2007: 61), instead of being imposed on us through an external label. Lash uses a uni-directional expression of power that does not accommodate the possibility of agency. However, stripping aside these dystopian tendencies, his statement nevertheless underscores the fundamental shift of the dynamics in self-understanding brought about by the mechanisms of generating and enacting social classifications in the context of big data.

Human-Machine Complicity

Considering the range of data sources implied in the processes of calculation and inference further widens the scope to consider another computational characteristic. In a surveillance context, Lyon (2001) has highlighted the porosity of distinct data sources as 'leaky containers' and the notion of 'surveillant assemblage' (Haggerty & Ericson 2000) underscores a connective imperative of data for surveillance purposes. Amidst these data sources are those people under surveillance themselves, whose demographic, location, behavioural, attitudinal or other data are considered as raw material through which outcomes are generated. This does not just include automatic tracking data and dataveillance, but also social data that consumers intentionally produce themselves through tagging, liking and sharing of media content in particular on social platforms, which in turn influence selection, curation and personalisation mechanisms on which these platforms modulate further interactions between users (Alaimo & Kallinikos 2016). In these ways, through their everyday practices, the subjects of surveillance are – often unwillingly – complicit in the computational principles that govern them.

In contrast to claims that algorithms are "totally isolated from all social and cultural factors whatever" (Slezak 1989: 563), this means that people are constituent parts of computational practices. These social and cultural factors also extend to the production side of coders, programmers and other software architects in the widest sense. Algorithms are not neutral (Halavais 2009), and similar to the modern ways of classifying and standardising that Bowker & Starr (2000) have described, algorithms prefer and emphasise some attributes over others. Preference selections are part of the performative nature of algorithms, and in particular machine-learning algorithms may generate the underlying criteria autonomously. Yet those who write algorithms themselves also encode moral judgements, lay-sociological and lay-psychological assumptions, behavioural research and many other factors. For instance, the proverb 'opposites attract' has been translated into the matchmaking criteria of dating websites (Ayres 2008), and Alaimo (2014) has shown empirically how online companies select particular design infrastructures and assumptions of personal relevance for consumers that are encoded into their platforms. A fourth computational characteristic then is about the willing or unwilling complicity of consumers and professional experts with machines to create and sustain powers of computation.

3.1.2. The Lived Experience of Computation

I have now characterised a computational logic through four characteristics. While my broader aim is to understand the lived experience of a computed world, this emphasis on computation per se was a necessary precondition. It illustrates the particular rationale through which computation acts on the world and thereby delineates it as an interlocutor for human agents. This establishes a basis for developing the communication problem of computed sociality.

Although a computational logic emerges as a distinct set of characteristics, there is no Manichean dualism between computers and human agents. As the notion of complicity has illustrated, people's acts themselves feed into the computational logic. In light of both the complexity as well as the modularity of the characteristics above, people are not addressing a monolithic interlocutor when they seek to act towards a computational logic. They encounter a configuration composed both of machine and human elements. As this research is principally concerned with the lived experience of surveillance, it must remain open to how ordinary people recognise a computational logic. People's perceptions of

what and whom they act towards may differ from the theoretical notion of a computational logic that I have proposed. This neither diminishes the concept, nor the value of people's experience. Rather, the overlaps and discrepancies between the characteristics that make up a computational logic and how it is represented in the domain of lived experience is a productive field of empirical analysis later in this study that helps to understand opportunities and limitations of agency in practice.

A theory of agency cannot pre-empt an empirical analysis, but it must provide a suitable framework. To do this, in a next step, I embed the idea of a computational logic into the domain of lived experience. It is here that people encounter computation and need to reconcile their own ways of making sense of the world with its logic. At this intersection, the communication problem inherent in computed sociality becomes apparent. I develop such a perspective in three arguments below. Taking stock of current debates, I diagnose (1) the absence of a suitable analytical language that can accommodate the lived experience of a computed world. I then proceed to highlight (2) the role of interface and infrastructure as sites of constructing meaning, and conclude with (3) the role of visibility in structuring the communication problem.

Obstacles to an Analytical Language

Despite their prominence in documenting the changes brought onto the world by computation, emerging accounts about big data, algorithms, code or other concepts provide little guidance for a framework that connects the computational logic to lived experience as they are largely preoccupied with defining and delineating these phenomena. I illustrate this through the example of algorithms. Notable exceptions to the conventional focus are those accounts which seek to order existing debates, such as the proposition to compartmentalise the study of algorithms between disciplines, including "a sociological approach that studies algorithms as the product of interactions among programmers and designers" (Barocas et al. 2013: 3). Yet this implies that a sociology of interaction should look at the production end of algorithms, facilitating a conceptual understanding of algorithms themselves, and not of their lived experience. In a related effort, Gillespie proposes criteria to narrow attention from algorithms at large to 'public relevance algorithms', which he understands as those algorithms that affect human discourse and knowledge in mediated interactions (Gillespie 2014). One dimension of public relevance algorithms is 'entanglement with practice', or

> "how users reshape their practices to suit the algorithms they depend on, and how they can turn algorithms into terrains for political contest, sometimes even to interrogate the politics of the algorithm itself" (Gillespie 2014: 168).

Gillespie's interest lies in how such practices can help characterise algorithms and the internet platforms on which they operate, or, referencing his terminology, how algorithms are entangled with practice rather than how practice is entangled with algorithms. Considerations of the situated experience are left undeveloped here, even in those accounts which pledge for a concerted, structured curriculum for embedding algorithms in a social science context.

Computed Sociality as Interface and Infrastructure

A more productive perspective can be found in concepts that by its very nature stand for a connection. For instance, the notion of 'fabric' reflects observations that computation is pervasive and suggests that it is interwoven with lived experience. Amin and Thrift (2002) claim that software is now part of the material fabric of everyday life, and Burrows sees code and software as making up the 'social and urban fabric' (Burrows 2009). Yet neither of these authors specify what they mean by fabric, and the term is not embedded in a wider theoretical discourse. A related term is 'infrastructure'. Previously, I have referenced Thrift's (2005) statement that algorithms are performative, but he more specifically speaks of a performative infrastructure. Containing the word 'structure', the notion of infrastructure[13] provides a first link between computational principles and the notion of agency. Structure and agency form a conceptual dualism in social theory where agency manifests itself directed towards, and taking place within structure.[14] Debates around information and communication technologies (ICT) as infrastructure support the idea of performativity by considering them to be malleable (Furlong 2010), in contrast to conventional infrastructures like wires or cables which do not change what they provide through their very operation (Parks 2012). Like the notion of fabric, the idea of infrastructure extends the computational logic into socio-economic life. However, in contrast to the idea of fabric, infrastructure already connects to the notion of performativity, and is embedded in a richer theoretical history which allows us to link it to the relationship between structure and agency in a wider sense.

---

[13] For a discussion of 'infrastructure' and its various connotations in a social science context, see e.g. Bowker et al. 2010; Graham & Marvin 2001; Edwards et al. 2007.

[14] For a survey of the structure-agency debate, see for instance Ritzer 2010.

At first glance, infrastructure prioritises the computational logic over lived experience. However, infrastructure is not a standalone concept. Software studies and computer sciences distinguish between the front-end and the back-end of software (Manovich 2013). The front-end is available for users to see and to make inputs. The back-end is where those operations take place that are removed from user access, but from which outcomes are relayed to the front-end. Infrastructure is part of a similar dichotomy, with the notion of interface as its opposite. Infrastructure stands for the back-end, where reality is mediated and constructed, before it enters the lived experience. Conversely, representing the front-end, the interface is emblematic for the realm in which most media-related practices take place. Galloway (2012) even frames the interface as the most emblematic manifestation of digital culture per se. The interface is the screen of a digital device that serves as a window into mediated experience. At the same time, the interface is a means of translation which connects a computational logic with a human way of experiencing the world. This division is echoed in how media and technology companies consider themselves as engineers of consumer experience. For instance, in an article about *Facebook*, German newspaper *Frankfurter Allgemeine Sonntagszeitung* used the photo of a wallpaper in the company's office, demonstrating that at least implicitly, the logic of interface and infrastructure is part of *Facebook*'s self-perception. This wallpaper symbolically depicts the user interface of *Facebook*. But on one end, the interface is lifted like the corner of a curtain to reveal an intricate arrangement of cogwheels surrounded by depictions of people going about various activities – a view into the underlying infrastructure.

Figure 1: Facebook Office Wallpaper

Source: Glassdoor[15]

The combination of interface and infrastructure enables an extended reading of computed sociality. Under this perspective, computed sociality encompasses the processes of computation, its calculated outcomes, and the human experience of these outcomes. This specifies the domain of agency in a computed world. The interface through which human agents experience computation constitutes a site at which they are able to construct meaning. Agency can then be understood as situated acts around the interface against an underlying infrastructure. Those acts themselves fall into the empirical domain. However, a theory of agency needs to explore the possibilities, modalities and constraints of agency within the setting of interface and infrastructure. This requires an understanding of how acts on the interface can relate to the computational logic that is enacted from within the infrastructure. I argue that conflicts in relating the experience on the interface to the infrastructure and vice versa ultimately constitute the communication problem of computed sociality. In the next section, I show this through the concept of visibility.

The Invisibility of Computational Logic

The notion of visibility is an integral part of infrastructure debates: "[i]nfrastructure typically exists in the background, it is invisible and it is frequently taken for granted"

[15] I have received permission from Glassdoor to publish this material, sourced at: https://media.glassdoor.com/l/0f/a7/13/ef/3.jpg

(Bowker et al. 2010: 98), as these authors emphasise in reference to Star & Ruhleder (1996). The notion of visibility also has direct implications for agency. Brighenti (2007) proposes that visibility is composed of the overlapping domains of "aesthetics [as] relations of perception [and] politics [as] relations of power" (ibid. 2007: 324). He continues to suggest that such power is intertwined with agency: "Everything *I see* is, at least potentially, within the reach of the *I can*. What is not seen is not thematised as an object in the domain of action" (ibid. 2007: 328, original emphasis). Agency then depends on perceiving the object or subject towards which it is directed, before specific acts can be performed.

Applying the notion of visibility in the context of infrastructure to include modes of perception outside the human senses, and to make explicit the relations of power that emerge through them, offers a framework for theorising agency in the context of computation. In the following, I understand visibility as a metaphor for power and perception more widely, that extends beyond human sight to include all possible means of understanding the world through the human senses, and conversely through a computational logic. Visibility then is about sensors, whether biological, cultural, or technological, paired with modes of understanding and acting. In this section, I relate the notion of visibility to the dichotomy of interface and infrastructure and sketch out how this structures the possibilities and modalities of agency in a computed world.

At its *I/O* developer conference in 2013, *Google* elevated the notion of invisibility to a precept that should guide the development of new projects. The company proposed to "get computers out of the way" ("Hello Larry!" 2013: no pagination; Page 2013: no pagination), in other words removing the awareness that mediation occurs from the mediated experience itself. Invisibility then emerges as a desirable state for a system's end-users: "[g]ood, usable systems disappear almost by definition. The easier they are to use, the harder they are to see" (Bowker & Star 1999: 33). Parks suggests that each "infrastructure can be differentially positioned on a continuum of visibility and invisibility depending on its material composition, scale, design, location and purpose" (Parks 2012: 66), ranging from television towers conceived as architectural icons and landmarks, to satellite stations or data centres that are barred from access and often located in remote areas or protected by high security measures. Yet most infrastructures are visible in principle - they can be dug out, uncovered, and queried. Similarly,

algorithms are embedded in a language of perception, having been described as 'unseen', 'concealed', or 'unnoticed' (Beer 2009), or as sinking into the uncontested background of everyday life (Thrift & French 2005). However, such descriptions do not reveal just in what way a computational logic is invisible, and in how far this invisibility differs from other infrastructures. Understanding the specific factors that constitute the invisibility of a computational logic informs how, if at all, this invisibility can be overcome, and ultimately how agency is possible. The concept of visibility then provides a framework for understanding how (media) infrastructures that are sunk into the background may come to the centre of people's lived experience.

In contrast to other infrastructures, a computational logic cannot simply be revealed. While physical objects like server rooms remain part of the computational logic, they have ceased to be signifiers for its operation. Visibility has become disconnected from ways of knowing the world.[16] Already more than two decades ago, Michel Serres observed that

> "[t]he informational world takes the place of the observed world [where] things known because they are seen cede their place to an exchange of codes [with the consequence that] sight looks blankly upon a world from which information has already fled." (Serres 1989: 45-47)

A computational logic stands at odds with the cultural specifics and biophysical universals of perception and understanding. Hayles has implicitly alluded to this in her concept of a 'cognisphere', where she argues that while cognitive flows take place in a complex web between humans and machines, most of these flows are outside human grasp:

> "[m]ost of the communication will be automated between intelligent devices. Humans will intervene only in a tiny fraction of that flow of communication. Most of it will go on unsensed and really unknown by humans." (Hayles interviewed in Gane et al. 2007: 350)

[16] I argue that the metaphor of a 'black box' (e.g. Pasquale 2015) is not able to advance the debate in this regard. In order to frame invisibility, it paradoxically uses a visible container, the box itself. As a side effect, the computational logic is treated as if it indeed resided within a contained entity. The 'black box' then does not problematise the notion of visibility. It instead falls back on an object that is within the sensory realms of human experience to explain that which escapes this experience. The confinement, or boxing, also stands at odds with the pervasiveness of computational principles in socio-economic life, which Hayles describes as "the movement of computation out of the box and into the environment" (Hayles in Gane et al. 2007: 349).

These characteristics foreclose the ability of human agents to intervene in the computational rendition of reality - they live in a world where there are perpetually being looked at by computers which count, analyse, infer and categorise, but they cannot look back. These radical changes in the conditions under which knowledge about the world is produced constitute the communication problem of computed sociality. This problem manifests itself not in the sense of misunderstandings, or issues of translation, but in the categorical inability for human agents to relate to the computational logic as an interlocutor. Computers monopolise the means of perception that make reality, and thereby its interpretation. This radical shift in control over knowledge of the world and its production presents a historically unprecedented obstacle to human agency[17] and underscores its urgency and political nature. Brighenti states that if visibility exerts power, this converts places which manufacture visibility into sites of political struggle:

> "Visibility curdles into representations. In the absence of dissonant messages, representations tend to settle down and stabilise themselves. That is why the issue of access to the places of visibility is a central political question. To access these places is the precondition for having a voice in the production of representations." (Brighenti 2007: 333)

When places of visibility are monopolised by a computational logic, the struggle for representation gains a new quality. Querying representations is obstructed by the incompatibility of human modes of perception and understanding with the logic of computation. As a precondition, agency then needs to embark on a restoration of visibility to overcome the communication problem inherent in computed sociality. It needs to find a modus operandi that renders visible the principles behind the production of representation and the monopoly of interpretation.

3.2. Theorising Agency in Computed Sociality

Some writers have started to see a problem of agency posed by a computed world. Mayer-Schönberger & Cukier (2013) propose specialist auditors that mediate between public interest and corporate algorithms. Hayles (2005) argues for a critical code literacy to restore agency, and others diagnose a dichotomy of *Program or Be Programmed* (Rushkoff 2011), urging human agents to "break through the glass ceiling of the smooth

[17] I use the term 'unprecedented' to denote the historically new type of obstacle and make no judgement about the difficulty of acting towards a dominant structure. Particular socio-historical configurations, such as racial exclusion, have rendered people powerless in much more immediate and material ways. See for instance Gilroy 1993.

interfaces and start programming" (Lovink in Lynn 2010: para. 'What role can an artist have'). But such programmatic calls to action do not consider the lived experience of computation, and how agency emerges through it. I will now explore how social theory has already dealt with agency, and how it offers a more comprehensive framework. As my argument so far proceeded, as concepts and problems solidified, the traditional contours of social theory re-emerged. The discussion of interface and infrastructure, as well as the tension between human agents and a computational logic, recall the debate in social theory over the primacy of social structure versus individual autonomy in shaping human behaviour.

While most social theory, largely a twentieth-century undertaking, could not anticipate the rise of computation as a constituent part of social structure,[18] this does not hamper its relevance. Computed sociality may be a contemporary phenomenon, but the broader underlying questions it addresses – structure, agency, power, participation – remain relevant. Nevertheless, the changing coordinates of the social world brought about by computation foreclose a straightforward application, and we must consider concepts specific to today's computed world beyond established social theory to revisit and update existing frameworks. Sociology provides a more suitable canvas for this undertaking than other disciplines because it remains conceptually open and theoretically flexible to accommodate these new realities in a non-prescriptive way. It enables researchers to go beyond disciplinary boundaries and redraw its scope without causing a paradigmatic crisis. Hans Joas succinctly stated:

> "[…] that the original wealth of problems has persisted in this discipline to a greater extent than in others, where they have been lost from the outset owing to a greater degree of abstraction. Commentators often bemoan sociology's lack of a firm paradigm. Yet the positive side to this absence is that it allows certain losses of abstraction to remain visible which, for example, are simply ignored by the model of a rational economic subject adopted in economic theory or by psychology's notion that the organism merely reacts to outside stimuli." (Joas 1996: 4)

[18] Despite its central role in the social sciences, 'structure' is an elusive term without a consensual definition. For an overview and critique, see Sewell (1992; 2005). I follow Sewell's suggestion that in contrast to mainstream structural functionalism, 'structure' does not only constrain (e.g. Cheal 2005), but also enable, and that it is a process, not static. Sewell is influenced by Giddens's theory of structuration and Bourdieu's habitus. While I chose a different theoretical framework, it shares Sewell's dialectical ideas of structure and his criticism of structural functionalism.

To ensure this strength unfolds, delineating a theoretical understanding of agency in the context of pervasive computation also demands to narrow the choice of social theory itself. It requires a framework that does not radically prioritise either structure or agency and instead incorporates their potential tension as a productive theoretical feature. This is particularly important for this research because it seeks to explore the very possibility of agency, and not deny or advocate it *a priori*.

3.2.1. Computed Sociality and the Social Construction of Reality

Berger and Luckmann offer such an approach. When their book *The Social Construction of Reality* appeared in 1966, it was the first publication to feature 'social construction' in its title, inaugurating the term into mainstream sociological parlance. It was released at a time when the extreme ends of the structure and agency antagonism were being laid out. A decade and a half earlier, Parsons had for the first time fully outlined his theory of structural functionalism in *The Social System* ([1951] 2012) and Blumer ([1969] 1992) was formulating his anti-structural approach to sociology. Between those two poles, Berger and Luckmann offer a theoretical framework that seeks to reconcile structure and agency through a dialectical relationship. In the context of computed sociality, its particular merit lies in its ability to bridge macro and micro sociology, as I demonstrate below.

The structuralist ideas which Berger and Luckmann draw on can accommodate the pervasiveness of computation and the invisibility of infrastructure as external to human grasp, yet also as constitutive of social life. Structuralist ideas also provide a connection to the traditional discourse of surveillance theory. At the same time, Berger and Luckmann incorporate the interactionist ideas of Mead – and by proxy reflect those of Goffman. Berger and Luckmann see society as a consequence of interactions and emphasise the idea of communication for social order. This provides an analytical framework for how human agents are co-constitutive of social order, and how they can relate to, and query the structure they are embedded in through the sensory, cognitive and epistemological means they possess. An interactionist perspective also allows us to consider the idea of 'interface' as the site of both human-to-human and human-to-machine interaction. Lastly, although Berger and Luckmann could not foresee the future relevance of computation for social theory, their choice of concepts echoes the language I have used so far. Social order for Berger and Luckmann is a reality of lived experience,

and the notion of reality provides a terminological link to the discourse on computed sociality. It is echoed by Kallinikos' phrase of 'the computational rendition of reality' and also reflected in Crary's claim that technologies create

> "[p]roducts" are hardly just devices or physical apparatuses, but various services and interconnections that quickly become the dominant or exclusive ontological templates of one's social reality." (Crary 2014: 40)

For Berger and Luckmann, the primary means through which this reality is generated and maintained is intersubjective knowledge. The question of knowledge then provides a conceptual link to the tension between visibility and invisibility, which is defined as a struggle for knowledge about the world.

Berger and Luckmann's language and concepts at times are bulky and not self-evident, such as their particular interpretation of 'institutions' and especially their idea of 'objective reality'. But through these concepts, they offer a distinct approach to sociological analysis. I will outline their core concepts in greater detail below.

3.2.2. Berger and Luckmann: Main Concepts

The fundamental premise in Berger and Luckmann's theory is that human agents are the authors of society:

> "[…] social order is a human product. Or, more precisely, an ongoing human production. […] Both in its genesis (social order is the result of past human activity) and its existence in any instant of time (social order exists only and insofar as human activity continues to produce it) it is a human product." (Berger & Luckmann [1966] 1991: 52)

Yet this ongoing production takes place in ordered world of experience, or reality, that already exists before a specific human agent enters the world. Indeed, in answering how society is possible, Berger and Luckmann revert to a structural argument, drawing on Karl Marx's dictum that social existence determines individual consciousness. In contrast to Marx, they do not mean this in an economic sense, but simply in the sense that human agents exist under objective circumstances which determine how they make sense of the world and which provide the backbone for the production of social order.

Society is a human product in the sense that human agents express themselves through their activities in a process called 'externalisation'. The products of their activities, if repeated and habitualised, eventually attain an independent character from those who

created them and stand for themselves in a process labelled ‘objectification’. Berger and Luckmann use a broad definition of ‘objective', encompassing any product of human activity. Yet human agents are also a social product in that these objects reflect back on them in a process called ‘internalization’: “[t]he objectified relations that human beings have created constitute frames of human activity, which in turn affect the human beings who created them” (Repstad & Furseth 2013: 58). Externalisation, objectification and internalisation constitute a dialectical, ongoing process.

Berger and Luckmann’s book carries the subtitle *A Treatise in the Sociology of Knowledge* and they are particularly concerned with the role of knowledge in creating and maintaining social order. This knowledge is the intersubjectively shared knowledge about society that everyone possesses. Far from the expert knowledge for instance associated with specific professions, it is a common-sense knowledge that guides everyday conduct (‘knowledge of everyday life’):

> “I live in the common-sense world of everyday life equipped with specific bodies of knowledge. What is more, I know that others share at least part of this knowledge, and they know that I know this. My interaction with others in everyday life is, therefore, constantly affected by our common participation in the available social stock of knowledge.” (Berger & Luckmann [1966] 1991: 56)

The knowledge of everyday life is considered as self-evident until further notice. It is not challenged or queried “until a problem arises that cannot be solved in terms of it” (Berger & Luckmann [1966] 1991: 58). Such shared, consensual knowledge forms the structure of meaning without which human society would not be possible. Berger and Luckmann ask how this socially developed, distributed and preserved knowledge congeals into an unchallenged, taken-for-granted reality – in other words how knowledge becomes institutionalised. Their answer appears straightforward: the perpetual acceptance and reproduction of knowledge through the acts of human agents creates lasting social order. This is expression of the dialectics of externalisation, objectification and internalisation. Yet the underlying process is more complex.

When human agents express themselves through their activities, repeated acts solidify into a model which can be reproduced with less effort in the future. Acts and corresponding situations become habitualised and are converted into a type. Institutionalisation takes place when habitualised activities are reciprocally typified by different agents. This way they become abstracted from specific human agents into

generalised roles and expectations. Acts and situations can now be anticipated by different members of society. The process of institutionalisation concludes when emerging institutions are handed over to third parties (e.g. a new generation) which have not participated in their initial construction. Knowledge about the right conduct in everyday life congeals into what Berger and Luckmann call ‘objective reality’, a social world that appears set in stone, unsurmountable and partly inexplicable. The man-made origin of institutions wanes and they become reified as a non-human facticity as if they were a natural phenomenon. Objective reality serves as the unscrutinised canvas on which social life is acted out.

In contrast to Durkheim, who explains order via the concept of institutions, Berger and Luckmann stress the dynamic notion of institutionalisation, which are acts of perpetual confirmations of objective reality. So while the concept of objective reality hampers the autonomy of human agency, the need for reconfirmation adds this agency back in. Objective reality needs to be maintained. The most important medium through which this process takes place is language, which supplies human agents with knowledge about society and is the medium through which this knowledge is applied. Continuous interaction with others through language creates a sediment of knowledge that cements the taken-for-granted-ness of society. What emerges is a ‘recipe knowledge’ that serves as a guide or script that human agents rely on and which they know others also do.

Alongside the continuous production of social order, its legitimacy must be further ensured through mechanisms of ‘universe maintenance'. These range from folk-wisdoms to more elaborate theories of legitimation expressed for instance in legal directives and religious prescriptions. Together, they form symbolic universes of meaning. When these symbolic universes of meaning fail, the taken-for-granted character of society erodes, and objective reality loses its status as a self-evident order. For Berger and Luckmann, the term ‘dissonances' denotes the tension between objective reality and the world of individual experience, or subjective reality. Dissonances occur when there is a rupture between objectification and its internalisation. For social order to be maintained, limiting those dissonances is essential. Dissonances also permit a critical perspective on objective reality, its reform or replacement.

Problems of social order then emerge when common-sense knowledge is under siege. This happens when not all members of society share the same experiences, a threat that

society always faces with new generations coming along, or when counter-realities, produced for instance in subcultures or expert circles, stand in conflict with objective reality and leap into the common-sense experience of everyday life:

> "[R]ebellions on part of laymen (as form of social organization) may lead to emergence of rival definitions of reality and, eventually, to the appearance of new experts in charge of the new definitions. […] Incipient counter-definitions of reality and identity are present as soon as any such individuals congregate in socially durable groups. This triggers a process of change that will introduce a more complex distribution of knowledge. A counter-reality may now begin to be objectivated in the marginal group of the unsuccessfully socialized." (Berger & Luckmann [1966] 1991: 136, 185)

As societies get more complex and functionally differentiated, this threat grows. In the later twentieth century, Berger and Luckmann see the emergence of a society "in which discrepant worlds are generally available on a market basis" (Berger & Luckmann [1966] 1991: 192). Writing in the 1960s, the authors treat this scenario as an outlook and do not further investigate such discrepant worlds. Recognising the transformative potential stemming from a conflict between subjective experiences and objective reality as reified common-sense knowledge, they call for further research:

> "The historical and empirical application of sociology of knowledge must take special note of social circumstances that favor de-reification [DK: of objective reality]." (Berger & Luckmann [1966] 1991: 109)

I argue that the implication of pervasive computation in social structure has created a situation which further consolidates objective reality as inexplicable, yet also provides distinct opportunities for de-reification, and claiming back agency this way. This situation provides the basis for applying Berger and Luckmann's framework to understanding agency in the context of computation, and I will outline it below.

3.2.3. Revisiting Berger and Luckmann in the Context of Computed Sociality

Despite the theoretical and conceptual fit of Berger and Luckmann's approach with key themes that I have explored thus far, applying their framework requires some modifications. Berger and Luckmann's main case study was religion, and they did not take into account the role of technology in modern societies, let alone the notion of computation. Below I outline the limitations of a literal use of their framework and propose a reinterpretation of core concepts. I will mainly draw on ideas from Lash's new

media ontology, glitch theory and Goffman's notion of interaction. I draw on Lash despite differences in approach. Lash focusses on hegemonic and post-hegemonic notions of power. He pursues an understanding of power as largely uni-directional, that is dominant and all-encompassing (Lash 2007). Such an emphasis on this particular understanding of power leaves little room for the systematic contemplation of agency. Yet his analysis of algorithmic forms of power contains a commentary on how (impossible) human agency should look like vis-à-vis computation, which I turn on its head by incorporating it into an actual framework of agency.

The fact that computers do not just mediate, but constitute social life (Burrows 2009) challenges Berger and Luckmann's assumption of society as an exclusively human product. Pervasive computation does not negate the man-made character of society. But it adds another type of agent that is involved in the creation and maintenance of social order. Just like human agents, today, a computational logic is involved across the entire dialectical process of externalisation, objectification, and internalisation. While I will explore this empirically later throughout this work, the example of online purchase recommendations illustrates this in a simplified way.

Human agents externalise their activity (e.g. *Amazon* movie purchases) in the form of mediated interaction with a computer database. A computational logic then aggregates similar activities across different human agents and develops a comprehensive model of product preferences. This is the stage of objectification in which the computational logic manufactures how members of society relate to each other and perceive themselves by means of their consumption patterns. The engineered outcome is then relayed back to human agents and internalised in the form of suggestions such as 'other people who liked this product also liked that one', or 'you may also be interested in this offering'. By proxy of a computational logic, human agents now have an intersubjective understanding of preferences that has been constructed by computers. The criteria by which this happens are removed from human scrutiny, yet the outputs are relayed as a given reality on the computer screen. Computers have created a reality that appears as set in stone, given and trusted, yet somehow inexplicable. Unlike in Berger and Luckmann's original theory, it, therefore, does not take a new generation, or the factor time more generally, for reality to obtain an objective character. Rather, the willing or unwilling handover of institutions

from human agents to computers creates a new form of facticity that lets reality appear as objective.

Computational processes are also complicit in a latent takeover of an existing objective reality that is already set in stone. As computers have become pervasive, they seep into existing institutions that already make up objective reality and alter its premises without human agents recognising this transformation. Although Lash's (2007) understanding of power as dominant and all-encompassing itself may not be helpful for conceptualising agency, the shift in the nature of power that he outlines opens a new perspective on the struggle that human agents encounter. Lash speaks of a power binary that distinguishes between hegemonic and post-hegemonic forms of power. Hegemonic power is expressed in a concerted ideology and imposed as a coherent narrative from outside onto the modalities of everyday life. In contrast, a computational logic[19] constitutes post-hegemonic power that spreads from within everyday life and is not discernible as a coherent force (Lash 2007). What human agents believe to be reality and what actually constitutes the reality they participate in becomes increasingly discrepant. Human agents may possess a sedimented everyday knowledge and act according to this knowledge. But as Berger and Luckmann have highlighted, objective reality is dynamic and needs to be maintained. When computers mediate the application of this knowledge in interaction between human agents, the performative nature of these computers alters reality in the process. This computational intervention is not necessarily recognised by human agents and instead perceived as a regular adjustment of common-sense knowledge, making it an expression of computational power.

In this new constellation, the nature of social interaction changes. Berger and Luckmann based their model on the ideal type of face-to-face communication derived from Goffman's concept of interaction ritual ([1967] 2003) and did not consider mediated communication. Drawing on Berger and Luckmann, Hepp (2013) emphasises that mediated communication also underpins the production and maintenance of common-sense knowledge. He highlights that changes in media and their everyday appropriation through human practices affect how reality is constructed.[20] Today, computation modulates mediated interaction and co-shapes the social consensus reached between

[19] Lash (2007) uses the term 'algorithms'.
[20] See in particular pages 38, 46, 58 and 59 in Hepp (2013).

human agents. In this context, as computers become engaged in the construction of reality, they also emerge as a new type of social interlocutor for human agents. Arguably, computers are not members of society.[21] But because they co-shape society, Berger and Luckmann's framework suggests that from an interactionist perspective, they have to be treated as social interlocutors in the process of producing social order alongside, and in conjunction with human agents.

In this new framework of interaction, human agents are robbed of the primary means to develop and maintain common-sense knowledge – human language does not reach the language of a computational logic. In Berger and Luckmann's theory, this scenario would put objective reality under siege because at least in part it could not be maintained. Yet paradoxically, a computational logic is backed by a human-made mechanism of universe maintenance which at least today prevents this. This mechanism is the utopian promise of salvation attached to technology by a Silicon Valley narrative as technology as a silver bullet and fix-all for social problems, epitomised by the proverb 'there is an app for that'. Morozov (2013a; 2013b) has called this narrative 'solutionism'. The term denotes:

> "[...] an intellectual pathology that recognizes problems as problems based on just one criterion: whether they are "solvable" with a nice and clean technological solution at our disposal. [...] The ideology of solutionism is thus essential to helping Silicon Valley maintain its image. The technology press — along with the meme-hustlers at the TED conference — are only happy to play up any solutionist undertakings. 'Africa? There's an app for that,' reads a real (!) headline on the Web site of the British edition of Wired." (Morozov 2013a)

Under this reading, the lack of available language for human agents to compete on equal terms with computers for the production and maintenance of knowledge leads to a transformation of the nature of common-sense knowledge itself. The conventional modalities of common-sense knowledge that Berger and Luckmann describe are complemented by a consensus that 'technology knows best', an idea that echoes Turkle's (2011) observation in a different context about people's heightened expectations towards technology. Common-sense knowledge becomes detached from specific issues of social order and transforms into the meta-knowledge that other members of society also buy into the accuracy and superiority of computational solutions.

[21] However, the film *Her* provides a compelling utopia in which an artificial intelligence that was purchased as a software product develops a personality and is seen as part of the social world by the protagonist.

Reformulating the social construction of reality in this way would paint a bleak picture for the potential of agency. However, I argue that two concepts in Berger and Luckmann's theory, (1) dissonances and (2) mechanisms of universe maintenance, open a new perspective once they are revised.

Glitches as Dissonances

Berger and Luckmann maintain a vague understanding of the term dissonances. They do not dwell on the term and rather focus on the social groups that may spark dissonances. I argue that computed sociality comes with a specific type of dissonance – the glitch - that helps understand the possibility of agency. Glitches are unanticipated and unpredictable irregularities in how a computational system behaves. They can arise from the normal working conditions of a software, such as pixelated images during a situation of low bandwidth, but usually are "perceivable malfunctions of a system" (Goriunova & Shulgin 2008: 111) resulting from error in software syntax, logic or incomputable exceptions when unsuitable data is decoded in the way a computational logic deems proper. Yet glitches are not failures in the sense of a full computational shutdown: "Stated differently, it is a given program's *failure to fully fail* upon encountering bad data […]" (Manon & Temkin 2011: para. 3, original emphasis). In that the computational system does not fail but embody the glitch, it momentarily becomes representational in an unintended way, reconfiguring the relationship between a digital interface and its underlying processes:

> "A glitch is a mess that is a moment, a possibility to glance at software's inner structure, whether it is a mechanism of data compression or HTML code. Although a glitch does not reveal the true functionality of the computer, it shows the ghostly conventionality of the forms by which digital spaces are organized." (Goriunova & Shulgin 2008:114)

A glitch thus means that the categorical invisibility of infrastructure collapses, at least partially. A glitch does not reveal the entirety of a computational logic but discloses fragments of its character at a moment in time. The computational logic, or a tangible reference towards it, is spilt out onto the interface and into the realm of human experience. Glitches then are artefacts of mediation. Mediating between interface and infrastructure, they produce a site through which meaning can be created. Through glitches, the otherwise invisible computational logic enters the domain of people's experience, helping them to articulate the world they live in. Couldry and Hepp (2013) have proposed a

definitional difference between mediation and mediatisation that sheds further light on such glitches:

> "While 'mediation' refers to the process of communication in general - that is, how communication has to be understood as involving the ongoing mediation of meaning construction, 'mediatization' is a category designed to describe change. It then becomes possible to link both concepts in the following way: mediatization reflects how the overall consequences of multiple processes of mediation have changed with the emergence of different kinds of media." (Couldry & Hepp 2013: 198)

In this sense, glitches more specifically are a form of mediatisation because they alter the communicative landscape of mediation. They convert the computational logic into media and transform the means by which the construction of reality takes place. However, due to their temporal and unstable nature, glitches do not transform a computational logic in a binary model from 'unmediated' to perpetually 'mediated'. Instead, they are 'pop-up' mediatisations that occur and vanish interchangeably and unexpectedly. People's acknowledgement of their existence, and past experiences of glitches, however, induce a wider socio-cultural change in the construction of reality, irrespective of whether a glitch is present or absent at a given moment in time. Such modes of mediatisation in glitches may not be fully registered in broader *Cultures of Mediatization* (Hepp 2013), but they reflect deeper processes of mediatisation nonetheless.

Glitch theory is a discourse mainly located in new media and computer art which focuses on the aesthetics of glitches as digital artefacts (Barker 2011). A sociological reading of the term provides a connection between the sociology of knowledge and the interactionist tradition of agency. In Berger and Luckmann's language, when the underlying logic of infrastructure suddenly becomes visible on the computer screen, human agents encounter a situation in which their own, subjective reality encounters the principles of computed, objective reality. Such encounters can either verify common-sense knowledge or reveal a clash of counter-realities. A glitch represents a potential instance of de-reification that Berger and Luckmann stress as theoretically and empirically important for understanding social order. Usually, human agents are removed from a computational logic as a category of agent that is involved in the production of social order. A computational logic is an unknown, invisible interlocutor with whom human agents struggle to establish a social situation in Goffman's ([1959] 1990) sense. A glitch creates a social situation in which a computational logic enters the sphere of human sensory and cognitive experience. As a

glitch occurs, the computational logic declares itself and becomes an available interlocutor. Language, human agents' primary means of developing, maintaining and challenging everyday knowledge is temporarily restored, and human agents encounter a face of their interlocutor which helps them establish a situation that creates the basis for a range of different acts.

Reflexivity as Universe Maintenance

As types of societies change, so does the relationship between objective and subjective reality. Berger and Luckmann acknowledge this in their statement that I referenced earlier about contemporary societies which offer an abundant choice of discrepant realities, requiring constant readjustment between what is objective, and individual, subjective experience. A few decades later, in a different debate, the notion of discrepant realities surfaced again. Perpetual discrepancies of what is real convert the paradigm of certitude, a characteristic of rational, modern bureaucratic societies, into a question mark. Beck (1992) has expressed this in the concept of 'risk society', where all truths are temporary (Giddens 1990), that is until their unanticipated consequences nullify them.[22] Modernity has become reflexive: it problematises itself and its own rational logic; criticism and adaptability to changing certainties become features of society (Beck et al. 2001; Beck 1992). Lash (2005; 2007) has embedded the notion of reflexivity into a discussion of algorithms through the concept of 'rules'. He identifies three types of rules – constitutive, regulative and generative. Both constitutive and regulative rules are institutionalised, codified and policed by human agents (e.g. religion, law). The rise of computation stands for a new set of generative rules that are formed by and expressed through software and algorithms without human agents encountering them, or being able to rewrite them. While generative rules themselves are virtual, they generate actuals in the domain of lived experience (Lash 2007). Generative rules are the ultimate expressions of reflexivity as they perpetually adapt to changing constellations, reinventing themselves in the process. The association of generative rules with the idea of reflexivity makes Lash's perspective

[22] For a more detailed discussion of 'risk', its use in theories of modernity and its relationship with surveillance, see *chapter two*. For participants' empirical experience of risk, see *Chapter Five.*

on agency relevant to my argument.[23] For Lash, human agency needs to mirror the modalities of generative rules:

> "As social norms, i.e. regulative rules, weaken, we must increasingly become, in Ulrich Beck's sense, reflexive. We must become as if algorithmic. We must find our own rules and use them generatively. That is we must give the rule to ourselves. We are less rule followers than rule finders. Kant gave us two types of judgement: determinate judgement in which the rule is given to us, and reflective (reflexive) judgement in which we must find the rule." (Lash 2005: last para.)

Clearly, human agents cannot become computers in the way they think and act, and Lash's is careful enough to add an 'as if' to his statement, suggesting approximation rather than convergence. As pro-active rule finders, the task of agency then is to perpetually query and unearth the hidden logic of computers. This is echoed by Goffman's interaction theory. Goffman has proposed that each interaction takes place in a social situation which must be defined before such interaction can take place. This entails a clear conception of one's interlocutor (Goffman [1959] 1990). Generative reflexivity then is a means for human agents to frame their computational interlocutor. Within Berger and Luckmann's framework, there are two ways in which this can be enacted.

Firstly, reflexivity expands the possibility of agency through glitches. The concept of glitches suggests that they are evoked through internal processes within a computational logic and thus reveal themselves haphazardly, in an unplanned manner. While glitches may enable agency, in a conventional reading of the concept, human agents would need to wait for glitches to occur. Glitches then stand for a reactive conception of agency which can only take place once the computational logic affords it. Yet the idea of reflexivity offers a way to imagine glitches as tactically provoked. If human agents act reflexively in the sense of perpetually updating the relationship to their environment, acts that can trigger glitches become an expression of Lash's idea of human agents as rule finders. Acts on an interface usually have a specific, often utilitarian purpose (e.g. purchasing a book at *Amazon*, arranging a bank transfer). If human agents combine those acts with rogue entries, or monitor their own acts and compare them against return visits to a given interface, human agents can themselves provoke glitches. Acting in a computed world

[23] Based on Lash's preoccupation with power, I read his statement below as intended as an unattainable imperative in the abstract, rather than a hands-on instruction. However, I see practical applicability through connecting it to Goffman's and Berger and Luckmann's frameworks.

then implies combining everyday acts on the interface with querying the computational logic at the same time in a reflexive manner. These queries are contemporary expressions of establishing a social situation in Goffman's sense and framing a computational interlocutor.

Secondly, the idea of reflexivity allows us to reimagine Berger and Luckmann's concept of universe maintenance. Acts of universe maintenance are social acts that take place in interaction with others. Shared myths, legends and stories about reality and its institutions are principal mechanisms of universe maintenance. In the societies that Berger and Luckmann describe, especially in the context of religion as their major case study, such narratives remain relatively stable over time. I argue that in contemporary reflexive modernity, mechanisms of universe maintenance become themselves generative. Social stability is not generated by the permanence of these narratives, but through the knowledge that they will continue to constantly change and adapt in order to offer new perspectives on how a computational logic operates. Universe maintenance then is less about perpetuating a specific set of institutions, but about maintaining a stream of information about the modulations of a computational logic, which in turn allows human agents to adjust their behaviour (e.g. privacy settings on social networking sites, opt-out from online advertising). Glitches can form the basis for such universe maintenance in that they are shared and distributed by human agents as folk tales across society, only to be expanded by or supplanted by narratives about other glitches. They are joined by interventions from artists, algorithmists, or other translators, whose folk tales enter the repertoire of everyday knowledge of the world.

A theoretical understanding of agency in light of the communication problem of computed sociality, which I have outlined above, can only determine how agency is possible in principle. It cannot capture the actual modalities and acts performed on this canvas of possibility. As Jonathan Crary highlights "[…] agency itself is a mutable and historically determined notion" (Crary 2014: 82). The manifestations of agency in the context of computed sociality, therefore, differs from sociological conceptions of agency in context of the classical struggles the discipline has long documented, such as class, race, or gender. How exactly human agents navigate the social situations that glitches and modes of universe maintenance create, and whether human agents need to wait for a glitch to happen *ipso facto*, or can actually produce it, remains an empirical question which I

will document in the following chapters. At the same time, the framework of agency that I have offered remains confined to the communication problem of computed sociality, and is not a general theory of agency, or a critical meta-review of the concept of agency as such (e.g. Emirbayer & Mische 1998).

3.3. Chapter Conclusion

In this chapter, I have proposed an approach to understanding agency in the context of the computational rendition of reality (Kallinikos 2009). I have set out by arguing that existing terms to frame the computational mechanisms that undergird society today do not take into account the lived experience of computation and by themselves do not offer a perspective on agency. Drawing on the notion of computed sociality and the social construction of reality, I have specified the focus of a theory of agency as interrogating the conditions of knowledge in a computed world. I have developed my argument in two sections.

A first section framed agency as a communication problem for human agents vis-à-vis computational interlocutors. Reviewing a range of terms, from algorithms, big data to code and software, I have isolated four characteristics which jointly form a computational logic. I have then embedded this computational logic in a framework of lived experience, which allowed to juxtapose computational and human modes of making sense of the world. I have argued that the problem of agency in a computed sociality needs to be framed through the tension between interface and infrastructure. Human activity takes place on the level of the interface, whereas computational principles act on the level of infrastructure. The dualism of interface and infrastructure is itself expression of a further dichotomy expressed through visibility and invisibility. I have suggested that the infrastructure of computation is categorically invisible for human agents. My interpretation of visibility is not contingent on the human eye and sensory perception but applies more widely to the cultural specifics and biophysical universals of making sense of the world. A communication problem then arises through a categorical incompatibility between computational and human modes of constructing reality. Agency requires a restoration of visibility to reclaim the conditions under which knowledge of the social world is produced.

In a second step, I have applied the communication problem of computed sociality to a broader framework of social theory. I have argued that the paradigmatic flexibility of sociology permits updating and going beyond existing social theory to incorporate computation as a social force while retaining its analytical potential. Berger and Luckmann's *Social Construction of Reality* has provided a theoretical scaffold for this task. While the authors could not anticipate the rise of computation as a central feature of society, their basic framework overlaps with central themes in the conceptual language of computation that I had previously outlined. I have updated Berger and Luckmann's framework by introducing a computational logic as an additional type of agent that co-produces reality alongside human agents. I have then documented in how far this changes the idea of intersubjective common-sense knowledge and the structure of objective reality. The basis for my reinterpretation was Berger and Luckmann's outlook on the theoretical and empirical need to take into account ruptures between objective and subjective reality as modernity evolves. This required moving the concept of dissonances from the margin of their theory to centre stage, and specifying the term through the concept of glitches. I have proposed that computational glitches lead to a collapse of the hitherto insurmountable barriers between interface and infrastructure. Glitches permit human agents to approach a computational logic through their own sensory and cognitive means, creating a site for the production of meaning. While this brings computation into the realms of human experience, additionally, the internalisation of generative rules and reflexivity provides a basis for agency which brings human agents closer to computation by emulating its principles.

I have concluded that a theory of agency can only be a theory of the conditions of knowledge under which agency is possible. It cannot identify the actual modalities of agency in lived experience. This would be prescriptive and defy the idea of agency as such. The manifestations of agency remain an empirical question, which I will analyse in the remainder of this work. More widely, this chapter has provided evidence that the diagnosis of computed sociality does not relegate the understanding of society to the explanatory frameworks of computer sciences, related disciplines and to practitioners who read and write computer code. Instead, the paradigmatic flexibility of sociology and its conceptual repertoire enables social scientists to analyse present and future societies in the context of computation.

Chapter Four: Methodology

This chapter outlines the research approach adopted in this thesis, the underlying rationale for selecting it and the steps taken to assemble it. I follow Josselson and Lieblich (2003) in understanding this approach as a 'plan of inquiry' instead of a 'method' in order to reflexively develop an approach specific to the research problem at hand, rather than to overemphasise procedural conventions. As this chapter documents through a discussion of 'digital methods', this research takes place in a changing epistemological environment and lacks precedents that allow reliance on a fixed, consensual set of procedures. Through a plan of inquiry, I discuss how the reflexive application and modification of existing research tools, including those outside sociological conventions, can be combined to facilitate an empirical understanding of everyday life in the context of surveillance and computation. Aimed at the in-depth understanding of everyday life from the perspective of research subjects themselves, the empirical approach is rooted in a qualitative paradigm. The research strives to understand how people make sense of surveillance in computed sociality, how they perceive themselves as active agents vis-à-vis a computational logic, how they act towards this logic, how their interaction with computational agents unfolds, and what this means for their relationship with computational surveillance. These concerns reflect the theoretical framework at the intersection between a sociology of knowledge and a sociology of agency developed earlier in this thesis and place the empirical analysis in the tradition of ethnomethodology and interpretative sociology, which focus on the meaning-making of subjects in and of their worlds. This translates into the following research questions:

- *What is the role of online surveillance in everyday life?*
- *How do people develop knowledge about the computational mechanisms behind online surveillance?*
- *What practices do people employ to act towards such forms of surveillance, and what are their intentions?*

The research design operationalises these questions in a multi-step process. It sets out with a content analysis of news reports on surveillance, followed by active interviews and in the last step a combination of think-aloud protocols, participant observations and live interviews. Forty participants were recruited through a combination of snowball, quota, and maximum-variation sampling. After a broader discussion of methodology and research precedents that define the coordinates for the plan of inquiry, the chapter

explains the specific research design, sampling and generalisability of findings, before looking at research ethics and concluding with a reflection on the researcher's experiences during fieldwork.

4.1. Doing Sociology in a Digital Age

Everyday life is increasingly mediated through, taking place in, and constituted by digital technologies (Burrows 2009). This is a core premise for the theoretical framework of this thesis and motivates its empirical questions. It also has implications for the choice of method. If the purpose of method is access to 'the social' (Savage & Burrows 2007), or knowledge of the lives of people and their relations through a "social science apparatus" (Ruppert et al. 2013: 23), a systematic transformation of how life is experienced requires scrutinising existing sociological practice. Warning of a *Coming Crisis of Empirical Sociology*, Savage and Burrows (2007) see the portfolio of established sociological research methods as dated. Elsewhere, they argue that

> "[s]ociologists [...] are losing whatever jurisdiction we once had over the study of the 'social' as the generation, mobilization and analysis of social data become ubiquitous. [C]onfronted with these circumstances, sociologists needed to rethink their methodological practices in radically innovative ways, unfettered by some of the deeply rooted domain assumptions in our discipline that were so central to our methodological success in the 1960s and 1970s but which no longer pertain in the early years of the 21st century." (ibid. 2009: 763-4)

The authors' concerns are particularly pertinent for this research because they are informed by Thrift's (2005) notion of 'knowing capitalism', a macro-social diagnosis that knowledge about people increasingly is derived from the pervasive monitoring and surveillance fuelled by commercial interests. The struggle to make sense of a world governed by computation and surveillance, which the main theoretical and empirical theme of this thesis, then also affects sociologists in their work. Data about people is increasingly located in proprietary platforms such as *Facebook*, where mediated life takes place,[24] and the company has set up its own team of social scientists (Zhou 2014). Lupton (2015) highlights that as sociologists compete with an increasing range of commercial researchers and organisations as experts on the social, they face growing lag in the analysis of the digital domain, lacking tools, computational skills and access to digital

[24] As of November 2015, Facebook had 1.5 billion monthly active users (Facebook 2015).

data.[25] Also, they are confronted with an epistemological challenge as research from such competing domains frequently draws on big data as a logic of inquiry that stands at odds with established sociological ways of investigating the world (Mayer-Schönberger & Cukier 2013). Even if social scientists take advantage of a growing array of free digital analytics tools to counter the proliferation of new authorities on the social world, these are usually not designed for social analysis and limited in their applicability (Manovich 2012). Taken together, these issues affect sociologists' ability of "developing, funding and conducting sociological research" (McKie & Ryan 2012: 2), as well as to lend authority to their findings. While Savage and Burrows focus on surveys and in-depth interviews and predominantly provide examples from the domain of quantitative research (ibid. 2007; ibid. 2009; Savage 2013), these challenges also apply to other modes of inquiry. Such modes include ethnography, where the complex relationships between online and offline worlds, and the distribution of internet use across devices, platforms and tools, challenges the classic notion of the field site (Miller 2011).

4.1.1. Averting the Crisis: Digital Methods

Under the label of 'virtual methods', early attempts to update social research methods for digitally mediated environments mostly seek to migrate existing methods into the digital domain (Hine 2005). In contrast, the paradigm of 'digital methods' argues for digitally native approaches that "consider the Internet as a source of data, method, and technique" (Rogers 2013: 27). A growing range of such approaches is proliferating.[26] Rogers (2013) himself emphasises the study of hyperlinks, date stamps, algorithms, geo-IP location technology, historical website archives, search results and other digital artefacts. Latour et al. (2012) suggest to take advantage of the data generated through human interactions with digital technologies. Arguing that conventional methods represent a 'dead sociology' (Back 2012) that in its entrenched research practices fails to appreciate the rapid change in the constitution of contemporary society brought about by digital technologies, Back and Puwar (2012) articulate a manifesto for a 'live sociology'. The term has multiple connotations and is more a composite of directions than an instructive toolset. Abstracting from the eleven points in which the authors develop the concept, it firstly can be understood in juxtaposition with dead sociology as a set of methods that is

[25] However, as Manovich (2012) demonstrates through the example of telecommunications firm *Sprint*, commercial organisations do not possess a monolithic power of interpretation as datasets and rules of access are fragmented across the organisation, creating hierarchies within and between companies.
[26] For a comprehensive overview, see Lupton 2015.

contemporary and hence ‘alive’. It secondly recognises the fluidity of data and includes approaches to capture them in real-time, including web scraping. Yet most profoundly, live sociology stands for the liveliness of methods expressed through curiosity and flexibility, as the authors demonstrate through an analogy with Baudelaire’s figure of the flâneur:

> “[w]e need to take our research tools and devices for a walk, [prompting] unexpected relationalities with the environment, the body and the senses. Presented with strange encounters, alternative ways of categorizing and knowing the world emerge. [W]e as researchers become exposed to openness and the liveliness of the events we try to get close to.” (Back and Puwar 2012: 10)

Such fluidity is also a theme in Pink’s (2009) digital anthropology. Instead of changing the tools for data-gathering and modes of analysis, she reconsiders the field site. Her concept of ‘ethnographic place’ flexibly combines places, objects and people both online and offline. It acknowledges that sites are neither static in time, nor that they can be defined exclusively through material or other criteria. The ethnographic place then becomes a dynamic collection of sites and signals that stand in flexible relations and multiple constellations with each other. Debates on rethinking method in a digital context more broadly extend to the humanities (Berry 2011; Gardiner 2015). For instance, Moretti (2013) proposes ‘distant reading’, a way of studying literature that does not involve the close reading of texts by scholars, but big data analysis of content to uncover grammatical structures, vocabulary, thematic and dramaturgical patterns.

These examples suggest a diverse set of efforts to rethink the methodological toolbox not just of sociology, but of the wider social sciences and humanities. They also portray an emerging landscape of inquiry that is based on exploration rather than consensus around a fixed canonical portfolio of methods. There is evidence that this new landscape by its very nature will remain unstable in order to accommodate the fluidity and complexity of the phenomena under study. In a deliberately provocative book, Beer (2014) argues for a ‘punk sociology’ that permanently challenges the status quo. It includes “relativism, openness, and eclecticism” (ibid. 2014: 34) in the development of knowledge, embraces new and unconventional approaches of narration that include unpolished outputs beyond academic texts, and applies a do-it-yourself ethos to finding sociological problems and approaches that draw on inspiration from outside disciplines. A common trait in rethinking methods then is the idea of an ‘assemblage’ (Savage 2013), a notion that

already informed surveillance theory to develop situated approaches that combine often seemingly incompatible perspectives (Haggerty & Ericson 2000). While the choice of method should always be contingent on the research questions at hand (Silverman 2006), digital methods stand for the combination of data from different sources, disciplines and epistemologies to create new approaches to understanding social life, such as assemblages between conventional ethnography and data from digital sensors (MacKenzie & McNally 2013; Lupton 2015).

Some aspects of digital methods are not new and instead evolutions of earlier observations. Pre-dating this debate by more than 20 years, Williams, Rice, and Rogers already emphasised that

> "although we consider possible research methods for new media as mainly extensions of existing methods, we propose that the new media researcher should consider alternative methods, or even multiple methods, and to attempt a triangulation of methods." (Williams, Rice & Rogers 1988: 15)

Generally, the rise of digital methods can be understood as a critical response to entrenched ways through which sociologists have sought to understand the world. Yet digital methods are not a silver bullet and themselves must remain open to critique. In particular, the use of big data in social analysis creates new concerns and limitations. Large volumes of data do not mean that data is representative, and their inherent bias can be difficult to spot (boyd & Crawford 2012), troubling established processes of asserting validity in particular if previously untested approaches are used:

> "[…] researchers should be aware that the most easily available measure may not be the most valid one, and they should discuss to what degree its validity converges with that of established instruments." (Mahrt & Scharkow 2013: 27)

Problems of access then can also distort results in that easily accessible datasets are prioritised over those which are more difficult to obtain. Even without such constraints, interactions between people and technology create vast amounts of data. Researchers need to make decisions about inclusion and exclusion of data that reliably represents an issue under study, creating a new form of sampling bias under a "veneer of scientificity" (Bruns 2013: section 2, para. 1). Furthermore, applying a 'technological fix' to a sociological crisis can alter the sociological agenda, inadvertently favouring a quantitative paradigm over interpretative understanding (Gooding 2013). Despite the explanatory power ascribed to its volume and logic of inference, critics consider big data

inward-looking as it neglects the socio-cultural, economic, historical and political context it is embedded in, leading to a reductionist perspective devoid of wider sociological imagination (Uprichard 2012; 2013). If sociology seeks to draw on technological systems for the collection of data, or considers those systems themselves as data objects, it therefore needs to incorporate wider theoretical debates such as the politics of algorithms (Barocas et al. 2013) in its thinking on method. Such reflection extends to ethical considerations about access to and ownership of data, privacy intrusions and consent, where sociologists are held to other standards of accountability than commercial actors (Mahrt & Scharkow 2013; Boase 2013; Lupton 2015).

The ideas of punk sociology and assemblage of methods can mitigate some of these critical issues due to their openness to both big data and qualitative approaches. Yet the fluidity of the empirical landscape, the dynamic nature of digital objects and the need for creative combinations of tools also entails a lack of conventions through which to legitimise a particular choice of method, placing greater emphasis on the documentation and justification of a selected approach. Some argue that the term 'method' itself can be misleading because it focuses on procedure, rather than on how to consider the underlying questions. Josselson and Lieblich (2003) prefer to speak of a 'plan of inquiry', a phrase that reflects the 'punk', unstandardised and problem-centric nature of approach. I adopt their suggestion in my empirical approach.

4.1.2. Applying the Digital Methods Paradigm

For this thesis, the emergence of digital methods begs the question whether researching phenomena in the digital domain prescribes 'digitally native' methods as outlined above, and whether the demarcation between digital methods and apparently 'dead' sociology is actually clear-cut. My objective is to provide an understanding of everyday life under conditions of computational surveillance. While I take into account issues of algorithms, big data and related concepts, they are not instructive for my approach. I focus on the lived experience of human agents from their own perspective(s), and their subjective sense-making of and in such a society. My emphasis reflects the longstanding remit of qualitative sociology "to document the world from the point of view of the people studied" (Hammersley 1992: 165), allowing me to draw on its established set of tools. This study therefore does not need to consider big data approaches to sociology or attempts to decode or reverse-engineer computational artefacts directly. Yet other aspects

of the digital methods debate provide valuable guidance. Firstly, mapping the field of human experience in a networked, messy and fluid environment requires an approach analogous to reworking the ethnographic place and cannot rely on established conventions of field site. A static approach to field sites would privilege the site over the lived experience and force manifestations of agency in a too narrow context. Secondly, an assemblage of methods that incorporates approaches outside of sociology in order to establish deeper access to people's experience in a digital environment can supplement conventional qualitative research methods. This includes using the internet as a source of data itself through aspects of a live sociology, provided that such data not only reflects people's experience but is itself part of their experience. Lastly, ethical considerations brought forward in the context of digital methods are particularly relevant to this thesis because they ask whether research on surveillance can legitimate methods based on monitoring and surveillance themselves, and whether such methods can be replaced by less controversial approaches that yield a comparable depth and breadth of insight.

My plan of inquiry is focussed on people's experience, rather than technology as such. This makes my research less exposed to the limitations of current empirical sociology discussed in the context of digital methods. Yet I incorporate numerous intersections between human experience and technological artefacts and translate them into tools of inquiry in order to supplement existing methods.

4.2. Research Precedents

The lack of systematic empirical research into the lived experience of surveillance means that research precedents which this study can draw on are scarce (Ball & Haggerty 2005). These limitations are exacerbated by the fact that while surveillance studies themselves are a multidisciplinary field of study, empirical work on surveillance tends to draw on the mono-disciplinary methodological paradigms of its constituting disciplines, such as human geography or the sociology of crime. Such studies often are too narrow to inform this research, which draws on a multitude of debates and disciplines in its theoretical constitution. Nevertheless, supplementing the broader meta-discussion around digital methods, a review of existing studies in the domain of surveillance helps to develop the coordinates for my plan of inquiry, both by incorporating ideas, and by circumventing the limitations of existing studies.

4.2.1. Agency in Surveillance Studies: Two Perspectives

A notable account is Walby's (2005) institutional ethnography that explores the role of human agency in surveillance. Yet his definition of agency differs from how the term is understood in this thesis. Walby locates agency within the context of surveillance institutions to understand for instance how CCTV operators conduct surveillance. Such an approach sheds light on the production and maintenance of surveillance systems. In the context of a computed society, his method could contribute to how professional agents such as programmers are complicit in a computational logic. However, the everyday experience of living with surveillance, which is the focus of this thesis, does not take place within the spatially bound settings of a CCTV control room but within a distributed environment composed of physical and virtual sites that may differ between study participants. Walby himself acknowledges that his approach only provides a partial perspective of agency by neglecting the experience of those under surveillance. It however highlights the benefits of combining multiple methods, between in-depth interviews and participant observation in understanding the experience of surveillance. Walby proposes that in-depth interviews should be complemented by a discussion between researcher and CCTV control room operator which uses their observed actions as a basis. Walby considers the practices of doing surveillance as a form of text. He then queries surveillance operators on these texts that he has recorded.

A perspective of the everyday experience of those under surveillance outside of the CCTV control room is provided by Toon (2000). He studied how youth gangs cope with and evade the sight of CCTV cameras in a UK town centre is an exception. Toon operationalises de Certeau's notion of tactics (1984) using a combination of observation and in-depth interviews to document and interpret the practices of youths in hiding from surveillance. Toon's approach is useful for this thesis because it highlights the importance to explore the relationship between human agents and CCTV cameras as interlocutors in managing visibility towards surveillance. However, his approach cannot be translated into this study. Just as in the case of surveillance operators, ducking and diving from CCTV takes place in a confined space. The *a priori* focus on resistance also neglects how the complex tension between complicity and objection to surveillance in a digital environment is enacted. While the study establishes CCTV cameras as an interlocutor, Toon only looks at the cameras themselves as material objects. He does not consider what takes place behind the CCTV cameras and thus does not need to consider how to

operationalise the relationship between study participants and the abstract notion of computation.

4.2.2. Agency in a Digitally Mediated Environment

Empirical material on the subjective experience of digitally mediated surveillance is limited. Andrejevic is one of the few authors who have investigated everyday life on the internet in a context of pervasive surveillance (Andrejevic 2005). However, Andrejevic does not reveal his research methods, limiting the ability to build on his empirical work. He also only looks at peer-to-peer surveillance as specific manifestations of surveillance, which does not offer guidance on how to operationalise the relationship between human agents and computation. Andrejevic focusses on social networking sites (SNS) and does not consider how the fluid nature of digital experience may merit a reconceptualisation of field sites.

Extending the search for research precedents to the area of privacy shows that this compartmentalisation into distinct sites is prevalent in both qualitative and quantitative approaches to digitally mediated communication, which prioritise SNS (Barnes 2006; Albrechtslund 2008; boyd & Ellison 2007). This focus has merits as users often encounter privacy issues on SNS. However, it also stands at odds with the dispersed and networked nature of digital surveillance across different 'leaky' contexts (Turow 2011; Lyon 2007; Nissenbaum 2009). Zimmer (2008) has documented the interplay between search engines and SNS to expand their surveillance capabilities, but empirical designs have not paid sufficient attention to this dynamic. The compartmentalisation of surveillance into distinct digital contexts simplifies research logistics because it narrows scope and provides justification for the selection of field sites.

Yet studies on surveillance and SNS provide useful references for a research design. In his study on modes of resistance towards surveillance, Sanchez (2009) conducts a content analysis of *Facebook* user comments in reaction to a change in *Facebook* privacy policy. He provides an example of using the internet as a resource in the digital methods paradigm (Rogers 2013). Similarly, Livingstone's (2008) work on teenagers and privacy on SNS is of methodical merit. Arguing for a multi-method approach, Livingstone combines participant observation and open-ended face-to-face interviews with teenagers in front of their computers while they are using SNS. This has two benefits. Firstly, although Livingstone focusses on SNS, adopting a modified version of this interview

setting would allow a researcher to let the research subjects themselves define the sites of lived experiences while they are online, instead of imposing it through an *a priori* decision. Secondly, the combination of participating in lived experience in front of the computer as well as its interrogation facilitates a depth of understanding that conventional in-depth interviews or observation alone could not provide. Livingstone's approach can be considered an example of live sociology introduced above (Back & Puwar 2012).

Outside of the explicit context of surveillance, Bucher (forthcoming 2017) most recently conducted interviews and Twitter exchanges with 25 internet users about the Facebook algorithm to understand how people make sense of algorithms and whether awareness of such algorithms affects their use of SNS. While I could not consider her contribution in my methodology and research design (Bucher publishes long after my fieldwork was completed), her study underscores that it is possible to routinely speak with ordinary people about complex and abstract matters like algorithms. This echoes my own fieldwork experience in the context of this thesis and helps opening up the perspective of human agents in a computed world to further empirical research.

4.2.3. Implications of Research Precedents

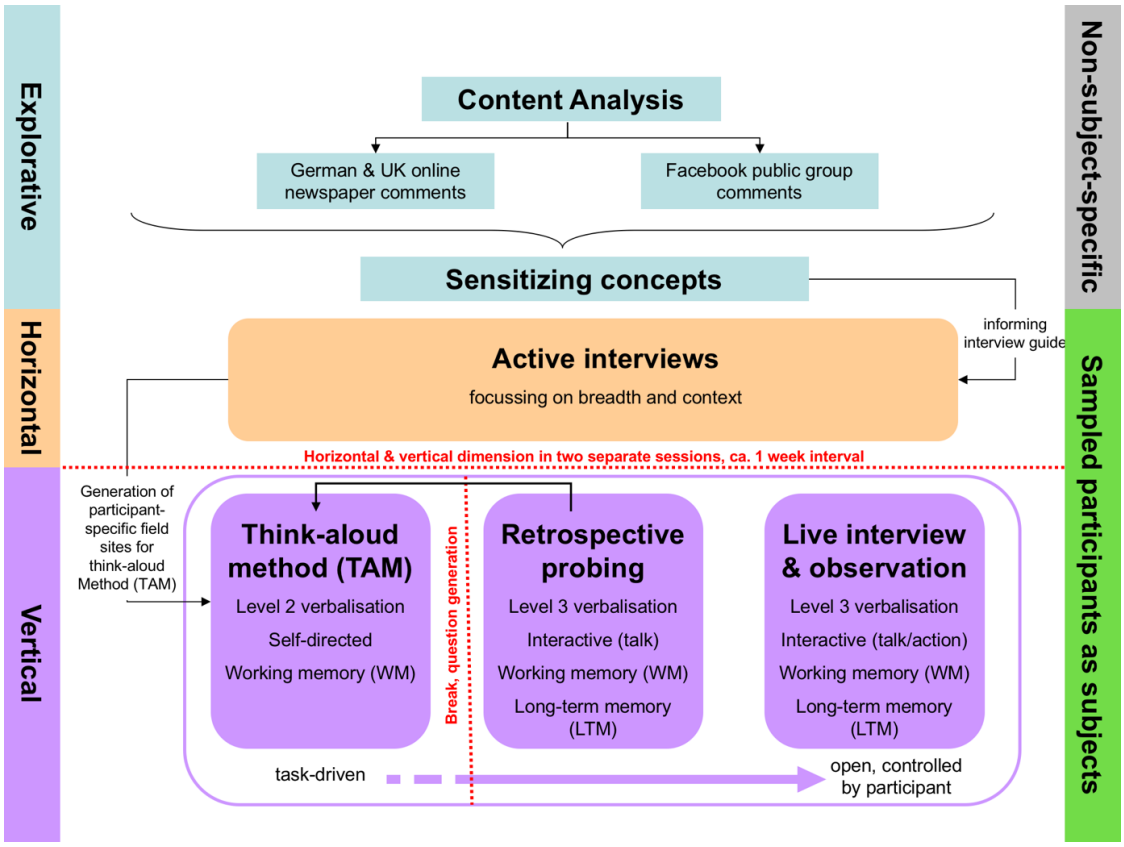
An analysis of research precedents has shown that there is no established template that this study can rely on. Surveillance studies have produced little empirical research on agency towards surveillance, and those studies that are available are both limited in scope and preoccupied with CCTV surveillance. Studies on agency towards surveillance in a digitally mediated environment are equally scarce, and an extended sourcing of literature around online privacy shows a preoccupation with SNS. Yet a review of existing research nevertheless supplements the insights gained from a discussion of digital methods. This review supports the value of a triangulation of methods and the importance of a dynamic conception of field sites. It also emphasises the importance to operationalise the relationship between participants and technological artefacts of surveillance, and offers guidance on how to combine interviews and participant observation in a live sociology in order to tap deeper into the lived experience of research subjects.

4.3. Research Design

The research design is informed by the debates around digital methods, techniques inspired by research precedents discussed, and general considerations of qualitative

research. This translates into a three-tier research design which I discuss in this section. In a first step, ‘sensitising concepts’ are developed through an analysis of news reports and internet user comments on surveillance in order to generate an interview guide for the successive tier and to make explicit potential issues of researcher bias. A second step, the ‘horizontal dimension’, consists of active interviews with participants in order to document the breadth of their engagement with issues of surveillance and how they generally assemble and construct knowledge about computed sociality and surveillance. This is complemented by a third research phase, the ‘vertical dimension’ that follows participants to field-sites which they have determined themselves. This vertical dimension is itself divided into several parts and consists of a succession and combination of think-aloud protocols, participant observation and live interviews accompanying people’s online practices to more deeply explore specific contexts of experience. The different components of the vertical dimension tap into different modes of cognition between affect and reflexivity. The below chart summarises the research design, which will be explained in further detail in the following sections.

Figure 2: Graphical Illustration of Research Design



4.3.1. Sensitising Concepts

As surveillance is designed into an ever wider array of social domains, it has become subject of pervasive public debate. This situation both enables and constrains a research design. It indicates that far from a niche subject limited to the biographical experience of few, surveillance is part of wider everyday experience. Talking to participants about surveillance therefore does not appear arbitrary, overly abstract or technical, but relates to how they experience the world. However, surveillance is also networked by its very nature and defies closed containers (Lyon 2007). In contrast to a compartmentalised approach to surveillance, this study seeks to incorporate this expanse of surveillance in its design. Yet while it is committed to emphatic understanding, enabling participants to set the agenda and speak from their own perspective without intrusion of external concepts and *a priori* structure, the vastness of surveillance requires basic signposts in order to ensure that the conversation is relevant. All interviews are collaborative achievements between researcher and research subject (Silverman 2006). Putting signposts in place with the intention to enable, rather than constrain or influence participants, further supports their own voice. Such signposts can take the form of probing

questions, or comparing a participant's perspective with views on surveillance purported in the media. At the same time, signposts support the self-awareness and reflexivity of the researcher. In this study, the researcher is not an outside observer in a different culture. I am myself embedded in the same macro-social context as my research subjects and experience surveillance in the news, encounter it on *Facebook* and in other contexts. Using signposts in the form of an interview guide, and entering fieldwork with a list of concepts derived from news media and other sources allows me to keep track of sources that may have influenced my own perception and to navigate those concepts carefully without subconsciously imposing them on the participant.

In order to address these issues, this research develops what I call 'sensitising concepts' prior to engaging with participants. These are key themes about surveillance and computation from news media, user commentaries and on SNS. Their aim is to generate signposts for conservation to enable participants, and provide stimuli yet checks for the researcher. These concepts were developed from empirical reality rather than from the theory underpinning this research because, as I have demonstrated, theory has neglected the subjective experience of computational surveillance. The rapid expansion of computational surveillance also outpaces the ability of theory to keep up, and to even provide a comprehensive inventory of contexts and manifestations of surveillance. In the anticipation that participants will draw analogies and make reference to current events when narrating their experience of surveillance, this research wanted to ensure that it is aware of such contexts.[27] Developing these concepts from empirical reality also hinted at a wide range of attitudes to surveillance that go beyond the binary of resistance and complicity that existing studies have focussed on.

Between November 2009 and April 2010, a content analysis of user-comments on *Facebook* and online news articles about surveillance in Germany and the UK was conducted.[28] Although user comments are not a widespread source of data in sociological analysis, their use has a precedent in Sanchez's (2009) study on resistance to surveillance. In this thesis, user comments on SNS were derived from *Facebook* discussion groups on *Facebook*'s plans to change privacy settings on the social network. Using qualitative data analysis software *NVivo,* key issues emerging across news sites and SNS were collected

[27] This proved particularly insightful in light of the deployment of *Google Street View* and the government's spy software (*Bundestrojaner*) in Germany.
[28] Online versions of *Der Spiegel, Sueddeutsche, Bild, The Guardian* and *The Sun* were analyzed.

and grouped into larger concepts. The collected comments have not been attributed to individual people and research participants were not recruited from commentators.

Drawing on online user comments comes with caveats. In addition to ethical considerations about using SNS data, which I address later in a separate section, online comments in news are not linked to contextual information about the author. For instance, assessing whether a comment has been made by an expert with a particular affinity to issues of data protection (e.g. working in computing, government) or by a lay actor is not possible. Also, the choice of contexts for gathering sensitising concepts (particular newspaper websites and *Facebook*) may foreground some, and neglect other issues about surveillance. Sensitising concepts may be closely aligned to the particular audience demographics of such newspapers, the tone and topic of articles as well as structural and user demographics of a specific SNS. For these reasons, this research only uses sensitising concepts as signposts. Yet as these signposts are non-prescriptive, their shortcomings are also productive. They allow an understanding of in how far participants' priorities overlap with and depart from the agenda set by the public debate.

4.3.2. Horizontal Dimension

The horizontal dimension consists of in-depth face-to-face interviews with research subjects guided by the previously developed sensitising concepts. These concepts have been used to initiate a conversation and successively, as interviews progressed, as checks and balances and to manoeuvre the interview towards the participant's subjective experience against the canvas of representations of surveillance in the broader socio-cultural environment. The juxtaposition of public representations of surveillance with individual experience helps understand how participants' experiences may be congruous with, or differ from these representations. It also facilitates an understanding of how representations of surveillance come to bear on participants and in how far they contribute to constructing those representations.

This stage of research is called horizontal because it seeks to capture participants' breadth of engagement with surveillance across their entire realm of experience instead of compartmentalising it into specific pre-defined containers. This horizontal approach starts without a broader conception of field site. Interviews took place in education buildings, cafes, sports and other leisure facilities, and in people's homes. These spatial environments were chosen for participants' convenience and to create a hospitable, open

atmosphere that they felt at ease with. In contrast to ethnographic work that incorporates physical space in studying internet practices (Miller 2011; Pink 2009; Burrell 2009), the location of interviews was not instructive for the understanding of everyday experience. However, a core tenet of this study's research design is that the horizontal dimension allows to identify specific contexts of heighted importance for participants. The emphases made by participants in the horizontal dimension were later used to define the field sites for the next stage of the research, the vertical dimension.

The interviews in the horizontal dimension were designed as 'active interviews', which go against the convention of keeping involvement of the interviewer to a minimum and to regard the interview merely as a means to neutrally extract information from respondents (Holstein & Gubrium 2004). Instead, the active interview deems the interaction between interviewer and respondent as a resource itself that sheds light on the procedures of knowledge production:

> "Conceiving of the interview as active means attending more to the ways in which knowledge is assembled than is usually the case in traditional approaches. In other words, understanding *how* the meaning-making process unfolds in the interview is as critical as apprehending *what* is substantively asked and conveyed." (Holstein & Gubrium 2004: 142, original emphasis)

An active interview is not a particular type of interview. Rather, it is a paradigm that recognises that all interviews implicitly are active and turns this into a productive feature. Such an approach to interviewing pays attention to the social construction of knowledge which underpins the theoretical framework of this thesis. Conversational in style, it has a storyline that unfolds through the relationship between interviewer and interviewee. As an 'interpersonal drama', it does not just convey information but is an interpretative frame in which meaningful reality is assembled through interaction (Holstein & Gubrium 1994). The notion of drama highlights that the interview is a scripted situation, and supported by basic coordination such as an interview guide, the roles of interviewer and the interviewee. Yet although scripted, the interview situation is not rigid. Seeking to bring out the subjects behind the roles of interviewer and interviewee, it commands flexibility. While the interviewee as a subject is the focus of the research, the subjectivity of the interviewer provides personal stimuli and resources from their own experience that relate to the interviewee and elicit answers (Holstein & Gubrium 2004). In contrast to other interview types, which seek to limit the interview situation to neutral and impersonal

stimuli, this personal approach recognises that an interview is a collaborative effort (Garfinkel [1967] 1984; Hammersley & Atkinson 2007; Silverman 2006) and that knowledge is not a "preformed, purely informational commodity" Holstein & Gubrium 2004: 155) that would be tainted if the interviewer was anything but passive.

4.3.3. Vertical Dimension

While the horizontal dimension focusses on the entire domain of subjective experience, the vertical dimension foregrounds particular contexts. These are contexts in which research subjects encounter particularly deep and complex configurations of surveillance and computation, and in which parts of the meaning-making of these phenomena takes place. As I highlighted above, these contexts were developed individually for each participant through the emphases they made during the horizontal dimension. In practice, these usually were SNS such as *Facebook* or the German *StudiVZ*, as well as music networks such as *last.fm*. After a basic analysis of each interview in the horizontal dimension, I selected two of those contexts for each participant to purse in the vertical part of the research. In the vertical dimension, field sites acquire a performative quality in that they both enable and shape research outcomes.

As I outline below, research in the vertical dimension combines observation and live interviewing. This involves both digital sites – the contexts selected – as well as physical sites in that the research took place in front of participants' computer screens demanding a co-presence of researcher and participant. Fieldwork in the vertical dimension was conducted in separate sessions from the horizontal dimension in order to avoid fatigue effects among participants. As the vertical dimension requires extra instructions for participants, subjects' attention span may not be sufficient to yield satisfactory results if conducted in the same session. Also, the vertical dimension requires that participants encounter previously unknown information, which required asking them to not log into SNS or other online sites for 48 hours prior to the research. The vertical dimension itself is split into three sub-sections, which I introduce below.

The Think-Aloud Method

The vertical dimension begins with a think-aloud interview. The think-aloud method (TAM)[29] emerged out of wider techniques of protocol analysis developed by Herbert and Ericsson (1984) and has its root in cognitive psychology (Lewis 1982; Charters 2003). The name is self-explanatory: research subjects are requested to think out loud as they go about a specific, pre-set task. In the context of the present research, this entails mentioning what one sees on the screen, where one clicks and what goes through one's mind as one performs the task. Prior to the TAM, participants were asked not to use SNS or other contexts selected for the vertical dimension. This step was necessary to ensure that enough new information had accumulated that justified navigating these sites for a sufficiently long time and to ensure that a portfolio of practices that is as wide as possible is represented in the TAM. During the vertical data-gathering session, respondents were then asked to access these sites and go about the activities they would usually engage in.

The intention to develop such a research method goes back to groundwork conducted by Ericsson and Simon (1980) who highlight the importance of introspective research techniques. They distinguish between working memory (WM), in which reasoning – the practice of making sense – takes place simultaneously with the performed act, and long-term memory (LTM), in which fragments of WM are kept, but in altered form and not necessarily in a form that can be verbalised (Charters 2003). The TAM intends to give researchers access to participants' WM, whereas interviews predominantly tap into LTM, where a reasoning process has already taken place and experiences and practices appear reflexively in a cognitively and socially processed form, frequently adjusted to fit wider values, norms. Tapping into WM is crucial for understanding experiences with surveillance because it allows access to the minute detail of practices which respondents might not be able to recall retrospectively as they happen in an intuitive and affectual manner, and may not be actualised in LTM. It sheds additional light on the process of construction of knowledge and meaning-making which even an active interview that stands in a social constructionist paradigm could not entirely capture.

Although the TAM emerged in an experiential, quantitative setting, it is not merely an artificially designed research method impinging on everyday conduct. In fact, Herbert

[29] I use the abbreviation 'TAM' when I refer to the method as such, and use the term 'think-aloud interview' when I refer to the specific interviews that I conducted on the basis of this method.

and Ericsson (1984) highlight that the TAM builds on thinking out loud as a naturally occurring process. People think out loud themselves in everyday situations, such as through a shopping list, or mumbling 'what did I want to do next' to oneself. Crucially, the researcher does not interfere in the think-aloud process, does not pose any questions and just listens. Yet despite the fact that thinking out loud occurs naturally, doing so on request for a sustained period of time may be an unusual situation for respondents. In order to prepare participants for this task, each think-aloud interview began with a preparatory task, where participants accessed a news website of their choice and said out loud what went through their mind for two minutes as they navigated the site. During the actual think-aloud interview, which took between five and fifteen minutes for each context, the only cues I gave as researcher were encouraging reminders to continue thinking out loud and not to fall into silence.

While it originates within the framework of quantitative, experimental research, the TAM has been increasingly used in the context of predominantly qualitative empirical investigations. Since the late nineteen-eighties, researchers from a variety of academic fields, such as education, psychology, second language research and human-computer interaction, have pointed out the potential of the TAM for qualitative research paradigms. Starting out from a recognition of the relevance of individual differences between participants in think-aloud studies, Rankin (1988) proposes to consider every participant performing a think-aloud protocol as a self-contained case study. Charters (2003) argues that qualitative think-aloud research unfolds its strengths particularly well in contexts where the goals are description and explanation, instead of a focus on cause and effect. Therefore, thinking-aloud can be regarded as an adequate approach for answering research questions that cannot be based on an identification of all the important variables of complex situations ahead of time and which imply a need for understanding the meaning-making of respondents (Vaino-Larsson 1990; Crellin 1990). Integrating the TAM into the plan of inquiry for this thesis reflects Beer's (2009) call to look outside established disciplinary paradigms to research digitally mediated life.

As the TAM intends to tap into a stream of consciousness, researchers commonly advocate to let participants focus exclusively on what they are actually doing (level two verbalisation), and not to provide reasons for their actions, or reflect on them (level three verbalisation) as it would disrupt this stream of consciousness (Herbert & Ericsson 1984).

This research follows this strand of thought and introduces reflexive methods to compliment such a TAM in additional stages of the vertical dimension.

Retrospective Probing and Live Interview

Instruction manuals for the TAM highlight that participants' verbalisation skills vary considerably, which affects quality and length of the protocols (van Someren et al. 1994). Four pilot studies in the context of this research project have confirmed this. One participant did not articulate his thoughts and merely documented on which buttons he was clicking. Pilots also revealed that think-aloud protocols vary in length, depending on how active participants are on SNS, and how information-rich other contexts relevant for them are. Whereas the TAM allows deeper understanding of subjective experience within a specific context, there may be further practices that participants engage in, but which simply did not occur during the limited time frame of the think-aloud protocol. Last but not least, additional understanding of subjective experience can be gained by letting respondents elaborate reflexively on the issues brought up in the TAM, as well as by taking advantage of the co-presence in front of a computer. Implementing an attitude to methods as put forward in the digital methods debate – whether as 'punk' or as an 'assemblage', allows to consider the TAM not merely as a method itself, but as a source for collateral approaches that build on the foundations it has created, whether it is a particular type of data, or a setting. In order to counteract limitations of a TAM and expand on the empirical opportunities it provides, the research design was revised after the pilot study to follow a modular approach within the vertical dimension.

A TAM without interaction between participant and researcher was complemented by a second module of retrospective probing. In a fifteen-minute break after the think-aloud protocol, I generated questions from my notes of the TAM session and asked participants to elaborate on the issues they mentioned while they had been talking out loud. This introduced a reflexive dimension to the spontaneous, unfiltered data of the TAM without altering it. Allowing participants to reflect on the TAM both clarified issues not comprehensible without context, and permitted them to branch out into domains of experience they had not previously actualised, but which were stimulated by the TAM. Probing the TAM data also revealed that some participants were surprised by their own affectual acts and subsequently tried to negotiate what their 'true' perspective was. Instead of tarnishing or polluting previously collected data, combing a TAM with a

reflexive approach takes into account that participants are not merely rational actors (Slovic 1999; Loewenstein et al. 2001), but act in a complex configuration of affectual, emotional self-management (Sennett 1998) and rational reflexivity (Giddens 1990).

A third module, following directly after the retrospective probing, consists of a live, action-based interview that is not directly associated with the statements made in the think-aloud interview, but takes advantage of the field site – a digital context reflecting the participants' deep engagement with issues of surveillance in front of their computers. It resembles the approach employed by Livingstone (2008) in researching children's use of SNS which combined conversation and action, and the idea of live sociology proposed by Back and Puwar (2012). I joined participants in front of their computers, where they navigated to the sites of the TAM. Equipped with visual cues as to what is happening on the screen, I asked participants to demonstrate what they usually do in this particular online setting, how and why. Recalling the TAM and reflexive probing, without prompting, many participants took the opportunity to illustrate the points they had previously made by means of example. For instance, some participants showed me a friends' *Facebook* post that warned about surveillance, or accessed their privacy settings to document how they protected themselves against surveillance. Others demonstrated the false trials they manufactured with fake information to fool advertising algorithms.

The three modules in the vertical dimension differ in two ways. Firstly, they reflect a different degree of interaction between participant and researcher as they move from a more rigid, closed approach (TAM) to a more open and discursive approach. Secondly, the modules vary regarding degrees of reflexivity and verbalisation. The think-aloud protocol is concerned with what is happening presently and focusses on affect rather than reflexion (level two verbalisation). The retrospective probing still refers to what has just happened, but introduces a reflexive dimension (level three verbalisation). Whereas the TAM only requests participants to tap into working memory, the retrospective probing also encompasses long-term memory. The live, action-based interview finally invites reflexion on general issues, inferred from both present and past user experience.

4.4. Sampling

Sampling techniques can be separated into probabilistic and non-probabilistic approaches. Probability sampling is based on random selection methods involving

procedures which ensure that each case in the universe under study has fixed and determinate – often equal – probabilities of being drawn for the sample. These include simple random, stratified random, multi-stage cluster and other sampling techniques. Probabilistic sampling is generally preoccupied with numerical measurements and used in studies that intend to make statistical inferences to large-scale populations (Bryman 2008). In non-probability sampling, the chances of a case being selected cannot be calculated, and the underlying motivations for assembling a sample are different.

Non-probability sampling is predominantly used in small-scale studies which investigate complex social phenomena where the research questions demand a deep interrogation, and which emphasise the explorative analysis of social patterns within its context over an abstracted statistical representation (Schutt 2014; Yin 2014). Non-probabilistic sampling encompasses several techniques, including convenience or accidental sampling (based on ease of access), snowball sampling (a participant referring another), quota sampling (reflecting proportional attributes of the population in the sample), theoretical sampling (the sample seeks to develop or test a theory), maximum-variation sampling (inclusion of different ends of a social spectrum to enhance diversity), and others with varying terminology. Sometimes purposive sampling is considered as a particular method in opposition to accidental sampling, but it is also used as a generic term for non-probabilistic sampling (Berg 2006; Schutt 2014; Silverman 2006).

This research design draws on non-probabilistic sampling because it is well-suited for qualitative approaches concerned with in-depth understanding (Ritchie et al. 2014). The design follows a combination of snowball, quota, and maximum-variation sampling.

Participants were recruited in the UK and in Germany. At the time of data collection, both countries were engaged in different public debates about surveillance. In Germany, *Google Street View* had launched to public outrage, the federal government had distributed a spy software, and newspapers were revealing new practices of mobile phone tracking. In the UK, a debate had formed around the intrusion of CCTV cameras in public space.[30] These countries also have different national histories of surveillance. In addition to the *Third Reich*, until the fall of the *Berlin Wall*, the secret police (*Stasi*) in East

[30] See *Chapter One.*

Germany was present in nearly all aspects of public and private life (De La Motte & Green 2015).

As a native German living in the UK, I wanted to take into account these national debates and socio-historical configurations. Far from embarking on a systematic analysis of national differences, I intended to take advantage of these histories to tap into a wider array of attitudes, experiences and practices towards surveillance. I also wanted to explore in how far these national issues affect people's understanding of computational surveillance, which is itself a global phenomenon where *Facebook*, *Google*, other interfaces and computational logics transcend national boundaries.

Fieldwork took place in 2010-2011[31] in London as well as Aachen and Erfurt, two German cities of about 200,000 inhabitants. As my place of residence, London offered a convenient setting for participant recruitment. I grew up in Aachen, so could draw on a range of sites that I had access to for recruiting and interviewing people. My local infrastructure also allowed me to spend enough time physically in Aachen to conduct fieldwork. The same rationale applies to Erfurt, where I used to attend university. But while Aachen is located in the very West of Germany, Erfurt is part of the former *GDR* and secret police past. I wanted to incorporate these fragmented national histories of surveillance between East and West in my German fieldwork and understand how they inform people's narratives.

In order to recruit participants, I posted flyers in universities, in public sports and leisure facilities and on supermarket notice boards (Erfurt) that called for participation. I also approached people directly in universities and sports and leisure facilities. I chose this combination of contexts to ensure a broader participation from varied social backgrounds, education and occupation profiles outside of the domain of university students that I had easiest access to. In order to enable an understanding of how issues of surveillance are navigated within the same social group, I asked participants to recommend people they knew. Lastly, I added two quotas to establish a 50% split between male and female of participants, and a 50% split between participants in Germany and the UK. In total, 40 participants were recruited for this study, and the desired gender split was achieved

[31] Two participants were interviewed in 2011. In the case of one additional participant, the vertical dimension was carried out in 2011 after a longer period of non-response following the initial interview in 2010.

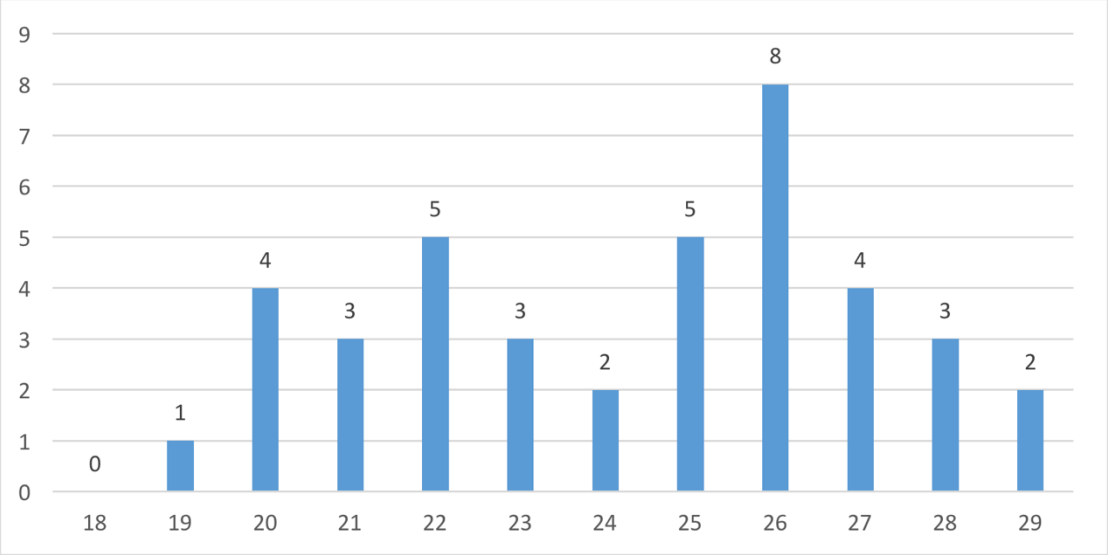
overall, as well as both in the German and UK subsamples. While university students are accustomed to participation in research studies, with a regular influx of requests similar to mine accompanying them through their university life, the same cannot be said for people who do not set foot in a university building on a daily basis. Lack of familiarity with such studies and lack of affinity with the underlying intentions (someone writing a thesis) may have resulted in a higher barrier for participation. I have therefore offered an incentive of €30 (£25 in the UK) for participation in this study, which I included in the calls for participants. This incentive was paid to all participants.

I limited participants to the age group of 18 to 29 years. The term 'digital natives', used to denote the generation born after 1980 into a world already saturated by digital technology (Prensky 2001; Palfrey & Grasser 2008), has been criticised for ignoring social nuances in technology literacy (Helsper & Eynon 2010) and equating generational criteria with expertise and mastery (Selwyn 2009). Yet in order to ensure a wider variety of computational practices, I wanted to focus on younger internet users. The most current internet usage report by the *Pew Research Center* at the time of research design suggested that this young generation still stands out in terms of frequency of internet use and the variety of online practices they engage in (Jones & Fox 2009), offering a richer canvas for studying surveillance across online contexts. For ethical reasons, I did not include minors.

Furthermore, participants with various degrees of education were recruited, as well as participants still in education and those already in the professional workforce. The overall composition was skewed towards university students, representing 18 of the 40 participants in total. The other participants were distributed across a range of professions (e.g. legal secretary, artist), and included a homemaker, an apprentice and a person looking for employment.[32]

[32] See *Appendix B* for more information on participants' demographics.

Figure 3: Age Distribution of Participants



The choice to include residents from both the UK and Germany was stimulated by differences in press coverage of surveillance in those two countries that I discovered during the coding of the sensitising concepts in *NVivo*. Privacy scandals, such as data leaks and hackers' intrusions into SNS, or changes in *Facebook*'s privacy policy, featured prominently in the German press. Frank Schirrmacher, the late editor-in-chief of *Frankfurter Allgemeine Zeitung*, in 2009 initiated a wider discussion on the future of personal data, artificial intelligence and surveillance, which was echoed in multiple other media outlets. Between 1 October 2009 and 31 January 2010 alone, German online news portal *Spiegel* published 60 articles related to surveillance on the internet.

In the UK on the other hand, media coverage on surveillance-related phenomena was less intense. Publications such as *The Sun* hardly reported on these issues; a recent murder case, where the perpetrator tracked down the victim via *Facebook* and a convict on the run taunting the police through *Facebook* were the exceptions. In Germany, *Bild*, a tabloid newspaper, instead offered instructions how to protect one's data, such as step-by-step guides to prevent public access to user profiles as a recurring theme. *The Guardian* demonstrated greater frequency in coverage of issues related to online surveillance, but lacked the emotional tone of German media. Between November 2009 and January 2010 *The Guardian* featured 22 articles (including blog posts) on online surveillance, less than half the quantity recorded at *Der Spiegel*.

Comparing Germany with the UK does not require to consider them as two bounded entities, as boyd highlights in a more general argument:

> "In a networked society, we cannot take for granted the idea that culture is about collocated peoples. It is not a question of mobility but of access to a hypertextual world. Geography can no longer be the defining framework of culture; people are part of many cultures including those defined by tastes, worldview, language, religion, social networks, practices, etc." (boyd 2008: 27)

Introducing a comparative dimension between Germany and the UK into this study helps understand in how far individual practices of surveillance reflect wider national public discourse and in how far they resemble each other based for instance on a cross-nationally shared social platform like *Facebook* as a translocal community. Instead of making generalisations about differences between how the British and German publics live with surveillance, to which a non-representative, small sample could not provide a valid answer, a comparative dimension therefore serves as an analytical tool to uncover the wider social context in which practices towards surveillance take place.

4.5. Generalisation of Findings

Patton (2015) emphasises that the choice for qualitative method does not prescribe sample sizes, that the information-richness of cases is more important than sample size and that sample size is contingent on the specific research questions. In this study, the sample size of n = 40 is based on the notion of 'theoretical saturation' (Yin 2014), a principle originally coined in the context of grounded theory (Glaser & Strauss 1967), where I stopped recruiting additional participants when themes and concepts had solidified and no new information was obtained during fieldwork.

The nature of sampling (non-probability) and the volume of cases affect the question of generalisability of findings. Quantitative research uses statistical generalisation in order to apply findings in the sample to the universe under study, where statistical procedures ensure the representativeness of results. Some qualitative researchers are exclusively concerned with the particular cases in their study and do not intend to make empirical or theoretical generalisations at all (Stake 1994). Yet such a view has been criticised as limiting the potential and impact of qualitative research (Mason 2002; Silverman 2006). Over-emphasising the need for statistical principles narrows, and simplifies the discussion about generalisation. Large-scale statistical surveys rely on averages and are

farther removed from individual cases than in-depth, qualitative work, eliminating nuances and converting real people into abstractions (Flyvbjerg 2004).

King, Keohane and Verba (1994) stress that differences between quantitative and qualitative research are merely stylistic. They provide a taxonomy of similarities and state that both have inference as their objective, either descriptive or explanatory, based on public procedures that are codified, transparent and open to scrutiny. Acocording to the authors, this leads to uncertain conclusions as inference is an imperfect process for reflecting the real world, and that inference is based on a set of rules.[33] While qualitative studies are not representative in statistical parameters, other logics of generalisation exist. Instead of statistical generalisation, the idea of analytical generalisation links empirical findings to a theoretical framework (Yin 2014), and Bryman (1988) similarly suggests that cases should be generalised towards theoretical propositions instead of populations. It is in this sense that I generalise findings from this study in order to shed light onto micro- and macro-sociological trends in society.

4.6. Design Limitations

The research design was developed in 2009 and fieldwork took place mainly in 2010. Modes of media consumption are rapidly changing. In particular, the proliferation of mobile devices has transformed how people's lives are digitally connected and 'always on' (Turkle 2011; Frith 2015). This research design has not considered this mobile transformation. The vertical dimension was entirely conducted using desktop and laptop computers, and the interview guide for the horizontal dimension did not emphasise the experience of surveillance and computation in the context mobile devices. Participants did not systematically bring up smartphones, or consider them as important in their subjective experience. At the time of writing, *Facebook* (2015) has more monthly active users on mobile devices than on desktop, *Apple* has launched the *Apple Watch* and arm wrist fitness trackers such as *Fitbit* have propelled self-tracking from a niche movement to a mainstream practice. The diffusion of technology and the emergent practices that surround it affect the reproducibility of this research design. While the overall design remains relevant and applicable, the interview guide needs to be updated and the selection of field sites revised. Preparations for the TAM also need to consider that asking

[33] I am paraphrasing their taxonomy here in abbreviated form. For a more detailed account of this argument, see in particular pages 8-9 in King, Keohane and Verba (1994).

participants to abstain from social media for 48 hours may not only be undesirable given the practical relevance of SNS in their daily lives and social expectations surrounding SNS use, it may also be unfeasible due to the push notifications many SNS sent to users' smartphones.

4.7. Ethics

'Who is watching the watchers?' This old adage from Roman philosopher Juvenal underpins Norris and Armstrong's (1999) seminal study on CCTV control rooms. It found that CCTV operators largely act in a realm devoid of any checks and balances. As experiences of fieldwork in surveillance studies became more readily available, researchers of surveillance have started to apply this question to their own practice. Reflecting on their research on urban police surveillance, Kemple and Huey (2005) illustrate that the researcher can easily become a subject of surveillance by virtue of the police, and also be perceived by research subjects as an agent of surveillance. Researching online surveillance is a far-cry from the often physically dangerous conditions under which Kemple and Huey have carried out their work. Yet the demands for heightened researcher reflexivity persist, in particular towards research subjects, and how modes of inquiry, such as participant observation, can be set apart, both in terms of actual and perceived practice, from modes of monitoring or 'snooping' on research subjects that would blur the distinction between researching, and doing surveillance.

This issue gains additional urgency at the intersection of the theme of study (surveillance) with the research tool and venue (internet). The digital methods debate has highlighted that surveillance itself is the primary mode of gathering insight on digital consumers by commercial agents, which academic researchers reject on ethical grounds. At the same time, surveillance-driven commercial activities compete with academic research for interpretative sovereignty over the social, creating pressure on academics to innovate (Lupton 2015). Doing academic research on surveillance on and within the digital domain then requires a sound ethical framework that negotiates possibility and practice of methods. It also needs to pay attention to how participants perceive role and objective of the researcher. Whereas Kemple and Huey had been mistaken for undercover police agents, researchers on digital surveillance need to avoid being seen as a 'stalker', 'creep' or other stereotypical role popularised through the rise of peer-to-peer surveillance and the normalisation of 'snooping'. (Andrejevic 2005). Risking such labelling is not merely

prohibitive on ethical grounds; it also constitutes a source of systematic bias leading potentially to non-response, falsified answers, or social desirability effects.

4.7.1. Ethics in Internet Research

Most research today is affected in some way by the internet, either as a field of study, as a means to derive insight, or as a site of inquiry. Originally rooted in the broader field of computer and information ethics (Moor 1985; King 1996), a growing array of disciplines are confronted with ethical questions for conducting internet-related research. As Buchanan & Zimmer (2015) highlight, these range from researchers' obligations to protect the privacy of research subjects and distinctions between public and private space, over confidentiality and anonymity, to consent, protection of minors and the ethics of covert research and intentional deception as means of obtaining information.[34]

The proliferation of SNS has amplified the urgency of such questions, for instance whether the terms and conditions that users have agreed to on *Facebook* are a sufficient basis for consent, causing a debate between legality and ethics (Gilbert 2009). In particular, the use of digital methods, such as harvesting data through large-scale scraping via APIs or other means has brought differences between commercial and academic research to the fore (Glickman et al. 2012; Lupton 2015). More recently, the rise of cloud computing and researchers' attempts to draw on cloud functionalities to assist in research services such as participant recruitment, data analysis and storage, as well as researcher collaboration, has amplified existing ethical concerns around privacy and ensuring confidentiality. The case of *Amazon*'s *Mechanical Turk*, which is a crowdsourcing marketplace that uses low-wage labourers to perform simple tasks, has added questions around the exploitation of labour and acknowledgement of authorship in the research process. (Scholz 2008; Aytes 2013).

Beyond recommendations by individual researchers in a methods debate or gained from a reflexive approach towards their own projects, various disciplines and their ethics boards have formulated codes of conduct to guide researchers through those questions (Buchanan & Zimmer 2015). Yet systematic literature on ethics in the context of surveillance and its intersection with the digital domain is absent. Below, I outline the

[34] I limit my discussion to introductory remarks with the aim to illustrate the relevance of ethical issues in this project and do not claim comprehensiveness. For an exhaustive overview on the history of debates, their various strands and a detailed documentation of ethical concerns, see Buchanan & Zimmer (2015).

specific ethical considerations I have taken in preparation, execution and analysis of the empirical part of this thesis.

4.7.2. Ethics in this Study

In interacting with participants before, during and after the research, I adhered to standard ethical principles such as being open about the purpose of the research, protecting anonymity of participants, treating personal information confidentially, and obtaining signed consent. In order to avoid being considered a 'creep' or a 'stalker', I clearly stressed the intentions of my research. The active interview, in which I shared personal experiences about being monitored, helped create rapport. All participants were anonymised and equipped with aliases, to which I refer in the empirical analysis when I discuss or quote participants.

A particular ethical issue emerged when participants showed me their *Facebook*, *StudiVZ* or other SNS profiles and newsfeeds in the vertical dimension. Here, I obtained a glance at their friends' profiles without knowledge and consent by these friends. I was concerned that this may undermine the idea of privacy as contextual integrity (Nissenbaum 2009), which suggests that people release personally identifiable information in a context they deem as clearly demarcated, making me an unwarranted outsider and trespasser on the boundaries between public and private realm. I needed to consider the ethics of implicating third parties into the research process. This issue also occurred in constructing the sensitising concepts, where I gathered data from *Facebook* discussion groups, posted by people in a non-anonymised way.

In its conference on ethics in researching SNS, the *Deutsche Gesellschaft für Publizistik und Kommunikationswissenschaft (DGPuK)* in February 2009 presented two criteria for determining informed consent. The first criterion refers to the interest of inquiry. It suggests distinguishing whether the research focuses on individual actions or artefacts, or whether the role of the individual as a subject or an author occupies a focal position. The second criterion refers to an informed judgement by the researcher regarding the degree of privacy that can be assumed for the context where the information was obtained. In case of prioritizing the role of an author over that of a subject, and if a low degree of privacy can be assumed, informed consent is not needed (Schmidt 2009).

According to these criteria, drawing on user comments in *Facebook* discussion groups is ethically unproblematic. My sole interest was to gain non-person-specific, aggregated data, which individuals have published as authors. These texts are created in user groups and on discussion boards, open for anyone to join and marked by *Facebook* as 'public'. Yet the situation is more complicated regarding the information I could glean from my participants' online contacts, which often are not public. I chose to incorporate these accounts into my data collection based on the following rationale. Again I was not interested in the subjects behind these accounts. I considered their texts as contributions to better understand a given participant as a research subject. The notion of self on SNS is interdependent and networked, as the term SNS itself suggests, where multiple people are co-constitutive of the online appearances of a given subject. I thus was merely interested in the context these other authors provide in shaping the everyday experience of my participant, who often talked about friends while showing me to them. I also made sure to never encourage participants to show me the SNS profile of a third person, and made it entirely contingent on their voluntary initiative. References to other people often occurred while participants were discussing their own newsfeed, where they had liked or shared these contributions, embedding them in a different context of recipients already.

The distinction in research design between a horizontal and vertical dimension is also informed by ethical considerations. Following Rogers' (2013) call to consider the internet itself as a source of data, I initially intended to complement the horizontal dimension through mining participants' web browsing histories, and to use the resulting data to help establish the field sites for the vertical dimension. Yet this would have had connotations of surveillance because mining web histories emulates practices employed in targeted advertising through the placement of cookies. While such an approach might be part of the suggested digital methods portfolio (Back & Puwar 2012), it clashes with the particular ethical requirements of researching surveillance. Such an approach could not only have undermined participant trust. It might also have elicited social desirability effects by avoiding controversial websites that are otherwise part of participants' routine repertoire. Had I proposed to mine web histories that already existed prior to the research,

participants would have had to grant consent retrospectively, potentially inconveniencing them.[35]

4.8. The Practice of Inquiry: A Research Diary

When I set out to commence fieldwork, I began a diary that recorded my notes of each day, storing remarks on interactions with participants that ranged from recruitment to data collection and debrief. Unlike a field diary in the ethnographic sense which primarily fixes participant observations on paper after a day in the field (Hammersley & Atkinson 2007), I conceived it as a personal diary that stood outside of the immediate research design and recorded my thoughts during the process, what I was learning as a research practitioner and how this could be used to advance the ongoing fieldwork. I saw it as a means to keep myself reflexive and self-critical while being in the field. It also helped develop strategies for building rapport with participants, which is an integral requirement for conducting active interviews that explore subjectivity in dialogue. Below I document extracts from this diary to provide more colour on the practice of inquiry, not just its plan.

4.8.1. Participant Recruitment

I recruited Anna, my first participant, on campus in Erfurt after directly approaching her with a flyer that outlined my research project. She immediately agreed to take part. It was generally straightforward to find students as cooperative as Anna, both in the UK and in Germany, and several participants said they regularly take part in such projects. Approaching students directly worked best, followed by message boards at German universities, which had lesser appeal to potential participants in the UK.

Despite the €30 reward offered, my flyers at supermarket message boards only added two additional participants. Flyers in sport clubs, from gyms to swimming facilities, did not provide any results. It was more time-consuming to find interested participants in sports facilities and I needed to take a proactive approach, spending more time explaining the study and the context before people agreed.

After all interviews with a given participant were completed, I asked whether they could recommend other people for the study. This was particularly useful for recruiting further

[35] The use of web histories to establish field sites has another drawback not connected to ethical issues. It would have equated the frequency of website visits with relevant subjective experience. If used for field site selection, web histories should be evaluated by participants first.

people outside the university context. The interview process, in particular through its active, conversational style, had overcome barriers, and I found even those participants who were initially hesitant to agree ending up proposing further research subjects that I could contact. At universities in Erfurt and Aachen, some participants told me that they had jointly signed up to the study with a friend already, and had been discussing the study before they took part. What began as an attempt to recruit additional participants turned into evidence that talk about surveillance is a naturalised social activity.

4.8.2. Rapport and Active Interviewing

The prominence of surveillance in public discourse reveals little about the degree of intimacy that people associate with their own surveillance encounters. Apart from my personal experience, I did not know how willing participants would be to talk about living with surveillance, how much they would open up and how we both would deal with potentially awkward moments of serendipitous privacy intrusion. When would I cross a line, how much should I reveal about myself in an active interview, should it be quid-pro-quo, or all-in? I was an outsider, not part of participants' social circle yet expected them to talk about personal aspects of their life on the internet, while many of them regularly deleted their web browsing history to prevent others from glancing onto their online data. While I was roughly the same age as the older participants, I was conscious about my role as the researcher, who could solicit an openness under the auspices of research, which in particular younger participants may not have granted in everyday social situations. As a male researcher, I also was alert about issues that might arise from gender relations, for instance private photos of female participants on SNS and how I should avoid giving off wrong impressions as a 'lurker' or 'creep'.[36]

Yet I discovered quickly that my concerns did not reflect research practice. Already the trial interviews suggested that the personal experience of surveillance is interpersonally narrated and shared. Throughout the fieldwork, participants pro-actively discussed their life with surveillance, sharing anecdotes, walking me through their privacy settings or eagerly trying to find an old *Facebook* post to illustrate a point. For many, encounters with surveillance, and even snooping on friends in acts of peer-to-peer surveillance, are

[36] These concerns convinced me to let participants take the lead during the live interview in the vertical dimension, I did not encourage them to access any photos and told participants prior to the session emphasised that they did not need to show what they did not want to.

topics of everyday conversation. I was entering into a dialogue that many participants were at least in part already having with others. The idea of active interviewing helped establish a lateral relationship that was characterised by working on the common cause of making sense of the reality of surveillance. Participants did not primarily perceive me as a gendered subject or an older researcher, but as a like-minded interlocutor.

4.8.3. The Vocabulary of Computation

The obstacles in conducting fieldwork were different from those that I had anticipated. While entering and sustaining a conversation about surveillance occurred naturally, participants struggled to verbalise their encounters with the logic of computation. The implication of computation in surveillance was not lost on them. On the contrary, it played a pivotal role in their conversation about surveillance with friends. But they did not have a technical vocabulary including terms like 'algorithms', 'big data' or 'code' readily available and instead relied on metaphors and circumscriptions that varied between participants and their specific social context. The interview situation demanded a degree of reflexivity from them that is largely absent in everyday interaction with friends, leading to a more abstract mode of conversation. I realised that I could not introduce technical terms and instead had to iteratively find out how participants described computational issues before carefully adapting to these ways of talking myself. Initially, I considered the search for vocabulary as a limitation of research design, but on recalling the social constructionist perspective that underpinned my approach, I decided to turn the struggle to actualise computational agents, both conceptually and linguistically, into a feature of analysis itself. Themes of computation featured more prominently in the vertical dimension, where both the TAM and the successive interview gave participants visual aids to illustrate their points by example.

4.8.4. Closing the Conversation

I had assumed that fieldwork would end with a simple debrief after the vertical dimension. But for some participants, talking about surveillance did not have immediate closure. I received two friend requests on *Facebook* from participants. I accepted because warding off participants after the fieldwork might have signalled that rapport had been disingenuous and betrayed participants' openness. During a live interview, another participant showed me a video explainer about surveillance on SNS that she had posted to her *Facebook* timeline that was followed by an exchange of comments between her

and several friends. I showed particular interest in this video because it documented how surveillance is not a solitary experience, and negotiated socially. The participant noticed my interest. She offered to take a screenshot. I accepted because it was self-initiated. I later used that image in the write-up of empirical material with blackened names.

After we had completed the vertical dimension, three other participants asked me 'how they did'. I had previously stressed that there are no right or wrong answers. One participant still considered the interview as a test and wanted to understand whether I thought that he was coping well with surveillance. Two others wanted to understand whether their responses were 'normal', how others had answered, and what tactics that other people commonly employed to hide from surveillance. These questions struck me because they underscored both the uncertainty in dealing with surveillance and the need for social orientation in evaluating one's own approach. In all cases I gave vague and encouraging answers that did not compromise others. Yet these questions also reminded me that talking about surveillance with people can attach demands of research subjects to the researcher who is expected to consult and provide guidance.

4.9. Chapter Conclusion

This chapter has detailed the plan of inquiry pursued in this project. It has placed the approach taken into the broader context of digital methods and research precedents before formulating the specific research design. This design is a three-tier process, consisting of (1) a sensitising dimension which gathers concept for an interview guide, (2) a horizontal dimension focussing on the breadth of people's encounters with surveillance through an active interview and (3) a vertical dimension that explored the in-depth experience of surveillance in narrower field sites. The vertical dimension is itself split into three components, the think-aloud method (TAM), a reflexive interview on the TAM and a live interview that combined participant observation with probing questions. As a qualitative study, this research intends to make generalisations and I have documented the epistemology behind those generalisations. Researching surveillance in the digital domain poses particular ethical challenges, which have affected the research design and the conscious exclusion of some digital methods. The research practice itself was iterative and required adjustment over time to elicit meaningful responses on complex and abstract issues of computation. The rapport built with participants and the combination of research tools in the vertical dimension have facilitated the construction of meaning.

Chapter Five: The Normalisation of Surveillance in a Landscape of Risk

The term 'surveillance' is generally uncontroversial in the academic literature (Lyon 2002) and has gained additional facets as it proliferated from the enclosures of total institutions in a Foucauldian paradigm to nearly all aspects of everyday life. However, as this study seeks to explore surveillance as a manifestation of computation from the perspective of ordinary people, it cannot superimpose a theoretical understanding of surveillance onto its lived experience. In fact, problematising the concept of surveillance and reconstituting it empirically from the ground up is a prerequisite for a more substantial analysis of how people engage with and act towards it. An analysis that explores people's understanding of and attitudes towards surveillance is able to identify the basic parameters that inform people's experience, locating areas of focus and defining a framework for narrating their lives under conditions of pervasive surveillance. This chapter takes on this task. It provides an introduction to the empirical analysis of surveillance that later chapters build and expand on.

This chapter draws on a series of theoretical concepts developed in the literature. Primarily, these concepts refer to the discussion in *Chapter Two* and its inquiry into the definition and nature of contemporary surveillance. Its point of departure builds on the diagnosis that surveillance is pervasive and part of everyday life (Lyon 2007). This diagnosis is supplemented by three theoretical paradigms established in the literature review. Firstly, it draws on my hypothesis advanced in the first theoretical chapter that existing approaches to the lived experience are too narrow and that an empirical approach to surveillance instead requires to de-centre the notion of surveillance. Secondly, it makes reference to the notion of computational surveillance. Thirdly, it embeds the experience of surveillance in a framework of risk as advanced by Beck (1992). Here, risk is understood as the uncertainty about consequences of today's acts for the immediate and distant future, and whether they will manifest themselves as threats or benefits (Nassehi 1997).

Within this framework, the chapter references additional theoretical concepts. In the first part, it draws on Deleuze's (1992) notion of societies of control as expression of the colonisation of the minute details of life through surveillance. Yet it only incorporates a Deleuzean perspective as a reference point to map people's own conceptualisations, and

not as an analytical paradigm. In a similar vein, it references Foucault's concept of the panopticon merely to illustrate people's narrow associations with the term surveillance, and how their understanding of surveillance does not extend from Foucault's disciplinary societies to societies of control. To illustrate how surveillance enters people's lived experience more widely, the chapter incorporates the relationship between information and surveillance (Kiousis 2002), debates around privacy on SNS (boyd 2008), data doubles (Haggerty & Ericson 2003) and peer-to-peer surveillance (Andrejevic 2005; 2007; Koskela 2003). Lastly, it makes a first reference to Berger and Luckmann ([1966] 1991) through their notion of the normalisation of experience. This concept stands for the unquestioned integration of a phenomenon – surveillance in this case – into everyday life as a mundane fact. However, it is the next chapters and their focus on agency that will draw more extensively on Berger and Luckmann.

In a first step, this chapter interrogates people's definitions of surveillance, how surveillance-related phenomena are embedded in their lives and how these phenomena inform participants' perceptions of surveillance. It concludes that surveillance is part of much wider practices and encounters which participants frame in other terms than surveillance. In a second and final step, this chapter locates experiences of surveillance in a framework of risk. It highlights the distinct role of computational surveillance in defining this sense of risk and connects surveillance to the broader theme of computation.

5.1. The Dissolution of Surveillance

This section argues that surveillance as lived experience can be understood through its erosion. It proposes that the expansion of surveillance into nearly all domains of life normalises surveillance-related phenomena as mundane facts and integrates them in a wider context of experience, leading to the dissolution of surveillance as a distinct concept.[37] In a first step, this section explores people's own definitions of the term surveillance vis-a-vis academic conceptualisations. It then continues to identify three phenomena through which the conceptual erosion of surveillance can be understood. These phenomena are the notion of a 'data deal', the adaptation of data doubles, and peer-

[37] The dissolution of surveillance is distinct from the suggestion that a computational logic is invisible, which I introduced in the theoretical discussion and which will inform later empirical analysis. The dissolution of surveillance denotes the erosion of surveillance as a term and concept through which people frame phenomena of watching, monitoring and data collection in a computational context. The invisibility of computation instead refers to people's inability to query and make sense of computational factors that impinge on them.

to-peer surveillance. Together, they show that the conceptual dissolution of surveillance paradoxically is evidence for how deeply embedded it is in everyday life.

5.1.1. The Limits of Surveillance

Enrico knows that he is being monitored on the internet. However, the 28-year-old history student struggles to articulate how he should frame this experience:

> [5, 01] "Well on the internet you are not really surveilled, well surveillance is more like the Stasi and the state and so on. Hmmm, well, yes, but it depends – how do I best describe this, well, it is not that distinct. Now the state, there I would feel surveilled, but on the internet, in general terms?" [DK: translation from German]

Enrico is not a Luddite. On the contrary, he is aware that his personal data on the internet is perpetually collected and analysed. We spoke extensively about his privacy concerns regarding *Google Street View*, and that data traces he leaves online can be misused. But Enrico is reluctant to equate being online with being under surveillance. For him, surveillance is associated with the government, and not the economic agents that systematically follow his traces on the internet. Nevertheless, he is confused. Enrico acknowledges that being online does carry traits of what he calls 'surveillance' and struggles to draw boundaries between different forms of being watched. His attempt to further explain himself sheds light on the characteristics he associates with surveillance:

> [5, 02] "Surveillance I'd say is exaggerated, that there is data being collected yes, but it is not that someone is chasing you personally and wants to get you." [DK: translation from German]

My first participant, Anna from Erfurt, has a similar view. When I asked the 20-year-old teaching student whether she felt under surveillance on the internet, she was quick to correct my question:

> [5, 03] "Not really surveillance, I would not say that. That there's someone sitting from the government and following you…or surveilling you, but of course, my data is always sucked in, and some company is spying on me what I clicked on." [DK: translation from German]

For Anna and Enrico, being under surveillance is an intimate act that involves a direct relationship between those conducting surveillance and the person under surveillance. They see it as a practice of deliberate intrusion into their personal sphere that is based on a specific interest in them as individuals. Surveillance is a directed, isolated effort set up by the state specifically to get under their skin. The everyday experience of being monitored on the internet, while acknowledged by both, does not fit this concept.

Dave, who is a fitness trainer at a gym in Erfurt, but about to take a job at a multinational firm in Munich as a marketing associate, agrees with the personal nature of surveillance and the state as its protagonist. However, he thinks that the state also carries out surveillance on the internet. Dave mentions the *Bundestrojaner*, a piece of code installed by federal institutions in Germany to monitor web users, which had caused a stir in the public debate a few months before we met:

[5, 04] "Now it's about these Bundestrojaner [DK: federal surveillance software]. Things that search certain things without you noticing it. Someone from the BKA [DK: Federal Criminal Police Office] could surveil you, the danger is there. I'm generally opposed to that. Although you invite this yourself with these Facebook things, also Google. It would've been a dream for the Stasi back then. They gathered information for months and installed bugging devices and wiretapped conversations – which the government now can do with just one click." [DK: translation from German]

Dave finds that the internet enables surveillance on an unprecedented level, facilitated by the proliferation of online companies like *Facebook*. Yet while such companies illustrate the potential of surveillance, he does not actually feel under surveillance by them. Instead, he places the data troves assembled by such companies in the context of what the state could do with it. Dave knows that companies spy on him and feels transparent and exposed, which leaves him with a feeling of unease and powerlessness. Surveillance, however, is a much narrower concept for him that is associated with criminal behaviour:

[5, 05] "Of course you are totally transparent on the internet, but I would only feel under surveillance if I had done something wrong, illegal and so on, if I was a criminal. Well not that I don't feel uncomfortable, this data collection stuff is pretty 'scary', but surveillance that is police and criminal and so on, so somehow different." [DK: translation from German]

Josephine, who is a hairdresser in Erfurt and attends a course in textile design, also extends the idea of surveillance to the internet. However, she struggles to grasp when and how surveillance exactly occurs. Surveillance on the internet does not fit into the narrow categories of spy narratives and government surveillance, but it remains an ambiguous idea that Josephine cannot untangle from other practices of monitoring. She feels that her experience online is related to surveillance, but different at the same time:

[5, 06] "I do feel under surveillance, but I think when it comes to surveillance you think about Stasi, 'The Lives of Others' or like in the movies, and on the internet, how shall I say, that is somehow more general, you don't really know how the data is being used, like why am I under surveillance and why are my data being collected, that is not always surveillance like at Amazon, that would be too crass, but you can never tell for sure." [DK: translation from German]

Her statement makes explicit a broader theme across participants' narratives. Paradoxically, the omnipresence of data collection and the spread of monitoring, their undifferentiated application and unclear purpose erode connotations of surveillance. Some participants echo this by narrowing down the definition of surveillance to exclude this ambiguity, whereas, for others, surveillance itself becomes ambiguous.

For German participants, these attempts to frame surveillance are embedded in a national historical context informed by the *Stasi* secret police in the former GDR and the wider totalitarian experience of the 20th century. While this particular collective memory is absent from people I spoke to in the UK, they approach the notion of surveillance in a similar manner. Their framework generally emerges from a different, more recent, collective experience – the proliferation of CCTV in urban spaces. For instance, Mike, who works as a graphic designer, highlights:

> [5, 07] "It's one thing to have piece of software on my computer and over time it is doing things and transmitting information. I think, if anything, I tend to not feel under surveillance because surveillance is something that...it precedes the internet. In my mind, it's like a camera on the wall, a photographer on the street. It's an offline thing to me […] Like I walk on the streets, and there is CCTV everywhere, and you read how people get an ASBO when they smoke pot, there have been stories of people from an estate here in the area."

Across Germany and the UK, the notion of surveillance does not capture people's lived experiences of being monitored online. In people's associations surveillance appears as an archaic term that denotes those practices of monitoring and controlling which are imposed from the outside, by traditional agents like the government, onto people. Surveillance is separated into distinct acts, bound in space and time. It refers to intrusions into individual lives with specific purposes in the physical world. Participants' narrow conceptualisations of the term surveillance and uncertainty about its applicability stand at odds with the progressive conceptual expansion of the term in academic literature away from the confinement – theoretically and literally – of Bentham's original panopticon (Foucault 1979). Various reinterpretations of the panopticon and alternative concepts (e.g. Elmer 2003; Haggerty & Ericson 2000) intend to open frameworks of surveillance for a digital age. It is, however, precisely some of the defining characteristics of the Benthamian prison design, a physical space with a personified observer, that inform and constrain participants' understanding of the term surveillance. Instead, they use a different language to capture surveillance-related phenomena, from 'spying', 'snooping' to 'watching' and 'monitoring'. In contrast to participants' narrow use of the term

'surveillance' itself, those other terms are employed far less restrictively. In fact, the indiscriminate and interchangeable application of terms suggests that they do not relate to firmly developed, distinct concepts but to phenomena in flux which participants struggle to demarcate. Interrogating participants' language of surveillance is not merely semantics. It creates the foundation for a deeper understanding of how forms of pervasive monitoring on the internet are embedded in people's lives. In the next three sections, I document how monitoring practices more widely complicate the experience of surveillance and how they are complicit in its ambiguity. In doing so, I will continue to use the term surveillance, but merely as an analytical category whose boundaries are eroding and which problematises itself. My choice also has practical reasons - alternative terms are not established and abandoning the term surveillance would result in a bulkier language, while academic concepts that can aid the analysis still refer to surveillance as an overarching category.

5.1.2. An Implicit Deal

Lars, a 26-year-old politics student in Erfurt and former police officer, uses music-streaming website *last.fm* to discover new songs. The fact that *last.fm* monitors his music consumption to generate its recommendations leaves him unimpressed, and he actively dismisses potential negative connotations:

> [5, 08] "That's the way it is, I don't really think about it, 'oh yet another data monster, surveillance' and stuff, it is just clear that you have to share your data if you want to get those recommendations." [DK: translation from German]

Lars does not separate between using *last.fm*, and making his data available. Both are intertwined and in his mind, jointly constitute participation in *last.fm*. He uses a language of economic exchange that frames monitoring on *last.fm* as a transaction between personal data and personal return. This transaction is based on an unquestioned agreement with 'how things work', an implicit set of rules. For him, this is in no way extraordinary, but a mundane fact that he does not challenge. The *last.fm* example is particular in that Lars knowingly and voluntarily submits his data to the music website. However, similar patterns referring to the co-constitutive nature of everyday online practices and personal data are widespread. Mark, a 25-year-old office clerk from London, sometimes is surprised himself how he has accepted online monitoring as an unquestioned part of being online:

[5, 09] "You have to log in all the time today, so you leave your email and stuff at least, and then they collect data about what you do everywhere. Yeah, you think about it and the longer you do you think whoa, like 20 years ago people would think this is crazy, but I guess here we are, and we don't know any different so no one's totally outraged."

Dave is similarly unimpressed. He has no illusions that whatever he does online is somehow, somewhere, being recorded. We sat together in front of his computer, and he navigated to his most-used websites; *Facebook*, German social networking site *StudiVZ*, *Amazon*, and a discussion forum for car enthusiasts:

[5, 10] "I just log in, and I do that automatically without thinking much about it. If you don't pay, you're the product, right? That's how you say it. That's pretty obvious to everybody." [DK: translation from German]

Dave uses a proverb to capture a fact about online life and surveillance. He had first heard it from friends. A while ago, they had talked about a *Facebook* privacy scare. The media had reported how *Facebook* used people's data beyond the *Facebook* website, and a commentator used this proverb. For Dave and his friends, it made explicit a shared knowledge that they had already intuitively lived by.

Like Dave, participants are aware that business models and functionalities of online offerings depend on their data. Participating in life on the internet, therefore, requires a degree of complicity, or as one female student from Aachen called it:

[5, 11] "[…] a pact. You know what you're getting into. I don't read the small print, but if there is small print in the first place, you know anyways 'your data may be used, blah blah blah'." [DK: translation from German]

The notion of such a deal is recurring throughout participants' answers, independent of their level of knowledge about surveillance and technical expertise. But it manifests itself differently between people. Some, like in the examples above, abstract from their experience and reflect on the role of being monitored. Others just mention it in passing and do not pause to reflect, or highlight this idea explicitly, suggesting how mundane and unspectacular it appears to them. For instance, Luise, who lives in a flat share in Erfurt with other students from her university, walked me through her most-used websites, logging in, logging off, clicking through a plethora of buttons and entering search terms. She uses the internet mainly to research issues relating to her studies, to do online banking, book holidays and other administrative tasks. She does not browse much, and the majority of her internet activities involves inputting information. Only when I asked her what she thinks happens with her inputs, she matter-of-factly stated:

[5, 12] “For me, the internet is like a tool, I use it for all the everyday stuff. And it is logical that I also have to feed the internet with my information.” [DK: translation from German]

Yet the everyday complicity between providing personal data and participating in online life is not just confined to a technical or economic dimension. It is also engrained in social expectations. Dennis, a 26-year-old geophysics student from Germany illustrates this in the context of *Couchsurfing*, a social network that connects backpacking travellers with hosts that offer a sleeping place for a small, or even no fee. Travellers need to be personally accepted by hosts. Dennis again uses a language of transaction, in which submitting his personal data to *Couchsurfing* plays a central role:

[5, 13] “You can say that's the deal you have to strike, so you have to reveal something, for instance, that's the thing at Couchsurfing. You have to tell a lot about you so that people are interested in the first place, and people want to host you. And you can't just write fake stuff; you have to be trusted as a serious person and no as a looney. And of course, that data can be extracted. Well, I don't know if it really happens, but yes.” [DK: translation from German]

Dennis is unable to restrict his profile to a pre-approved list of trusted people, both by design of *Couchsurfing* and by individual intention. In order to find a lodging place, he needs to communicate trust towards an undifferentiated set of strangers and reconcile his presentation of self with the risk of being monitored. While he does not believe that other people on *Couchsurfing* would spy on him, he is aware that providing his data to create social trust makes him vulnerable to being monitored by online companies, and to his data being harvested.

Dennis’ story is an example for the inevitability of monitoring that surfaces in other many accounts, such as Lars’s. While Lars can decide himself whether he wants to be monitored by *last.fm*, participants often highlight that everyday conduct online just has to take place within the parameters of such deals. Consider Frank, whom I met in Dave’s gym. Frank works as a clerk for the city’s public transport company. He highlights that his only chance to avoid being monitoring would be to become a Luddite:

[5, 14] “Yes I would say you have to live with the fact that someone is gathering data, there is no other way. In particular, because for me, I cannot be without internet because many important things go via the internet [...] Yes you are, or at least in my case, I am dependent on it [DK: the internet] because otherwise, it would be too complicated to keep in touch with some people, and that data is being collected and that I don't know who or when, that's part of it.” [DK: translation from German]

Yet neither Frank nor any other participant is outraged, or surprised by the implication of personal data in online practices. Tim, a 26-year-old anthropology student from London,

compares his acceptance of monitoring to his dad's approach of coming to terms with it. It sheds light on the basic paradigm of being online that participants, all below 30, consider themselves in:

> [5, 15] "My dad, he really reads all the t's and c's. He sometimes prints them out; it is ridiculous. And then it takes him hours to register anywhere. I mean come on, we all know that they collect our data and it is not any different [inaudible]. So why read it all the time? I mean, I've not done it once. Ok, my dad, he's old."

Tim thinks that his dad fundamentally misunderstands the nature of being online because he sees being monitored as a deviation from the norm. Conversely, Tim and other participants have normalised monitoring as a default state. In their narratives, they do not separate descriptions of using the internet from diagnoses of being monitored. Kiousis (2002) has argued that information and surveillance are inseparable, bound together by a mutually constitutive feedback loop. This argument is not merely theoretical, but already part of people's lived experience.

The normalisation of monitoring does not mean that people embrace it unchallenged. Their accounts, like in the examples above, include references to privacy, or expressions that on closer reflection, pervasive monitoring can be 'scary'. Accepting being watched as default is not a general expression of attitudes towards surveillance, or even a resignation to its powers, but merely an acknowledgement of the basic framework in which lived experience takes place. As I will show in later chapters, many participants employ tactics to circumvent and foil attempts of surveillance or seek to modulate this default through their acts in other ways.

5.1.3. Data Doubles

The idea of surveillance as a distinct phenomenon is further challenged through participants' approaches to their personal data more widely. Social networking sites (SNS) are a key domain in which such considerations take place. During the think-aloud interviews, many participants showed me their social media presence. They walked me through their privacy settings and explained how they design their profiles. Consider law student Luise, who takes great care in choosing how to represent herself on *Facebook*. She changes her profile picture regularly depending on her mood and has a rotating stock of about ten images that she chooses from. Her face cannot be clearly identified in these photos. Either they are shot from a distance, or she takes other measures to obscure her face. On one photo, her hair is combed forward to cover her face, and another photo

zooms in on her left eye, cutting out the rest of the face. She only posts sporadically on the newsfeed in order to avoid coming across as a spammer, and does not simply 'like' every post she finds interesting, but only posts about what she calls 'serious' issues, such as politics, gender equality, global warming. Such practices of impression management on SNS between self-exposure and privacy are commonly understood and have for instance been documented by danah boyd (2008) in the context of American teens. For Luise, they are routine, everyday acts of managing life on SNS. Yet they are joined by a very different set of practices which are just as mundane for Luise. These practices shed light on the deep-seated role of personal data in people's everyday considerations. When Luise walked me through her settings, she paused her cursor on the field containing her demographic data:

[5, 16] "I only enter my name and where I am from and my email address, that should be enough for people who want to find me. I don't share more, so no hobbies or whatever else is being asked for." [DK: translation from German]

Luise tries to strike a balance between allowing others to find her on the one hand and preventing *Facebook* from knowing more than necessary about her on the other. In this process, she thinks about *Facebook* not merely as a canvas on which she constructs her online identity through photos, biographical information and curated posts, but as a database that she is part of. Luise takes into account her role in this database with the same ease and attention as arranging her profile pictures. Being online for Luise naturally entails considering one's representation through data. Although she sees herself as an average user, thinking about data is not an alien concept reserved to the domain of professionals or particularly advanced users, but a routine part of the fabric of life. Other participants are even more explicit about their implication in data. Showing me her *LinkedIn* profile, Christina explained:

[5, 17] "[…] if someone searches for me…I don't want to give away too much, but I want people to find me, so I think what information LinkedIn will pick up when someone enters my name."

Christina sees herself as part of a database. This affects how she presents herself on *LinkedIn*. While Christina is concerned about privacy, feeding the *LinkedIn* database with sufficient data for others to identify her has priority. Christina considers *LinkedIn* as a tool to make new professional connections, and as a business journalist she needs to ensure that she is adequately represented through her data when others query the database. When the 26-year-old added her name, job title and other information to *LinkedIn*, she

knew that she was creating two profiles at the same time. One profile is visible on her personal *LinkedIn* page, intended for visitors to read. The second *LinkedIn* profile is its data equivalent. But Christina does not think about them as separate but as two dimensions of one phenomenon.

Such acts are not confined to the creation and maintenance of online profiles and occur across participants' activity on SNS. Sarah, a linguistics student, remembers when she was prompted by a friend on *Facebook* to install *Farmville*, a computer game that resides within *Facebook* and connects to her account. Before Sarah installs a tool such as *Farmville*, she automatically thinks about implications for her data:

[5, 18] "And then there is also this tick box at the games. Many have Farmville. And if I install that, I also first think about whether it is getting some of my data and then I double-check in settings. So like what there is now from my data, how that's being protected." [DK: translation from German]

Her language offers a broader perspective on how people relate to their personal data. Sarah speaks of a 'data set'. Instead of dispersed data points, she sees her data as an aggregate entity. A similar conception is implied in Luise's and Christina's attempts to be discovered in a database. All three narratives suggest that participants see themselves as having a 'data double' (Haggerty & Ericson 2003) online that serves as digital equivalent, or at least approximation of their selves. While no participant claimed that such digital imprint either reflected their 'true self', or that it should aspire to, people take the existence of at least rudimentary digital bodies for granted and incorporate them into their understanding of everyday life online. Concepts like 'data double', 'dividual' and 'data individual' are being used in academic literature with primarily negative connotations, denoting the assemblage of digital reconstructions of people for purposes of analysis, control and surveillance. Despite people's existing concerns about privacy and being monitored, the notion of data doubles is not just connected to such worries, or even constituted by them. Much more widely, data doubles are a category of self-expression and self-perception that underpins everyday life online.

The incorporation of data doubles into everyday practices also extends to practices of imagining other people, as Jack's story shows. The urban planner from London wanted to find his old friends from elementary school on *Facebook*. But instead of entering the names of people he recalled directly, he opted for a different approach:

[5, 19] "I think, well I am not sure, but Facebook can tell who your mates were back in school. So I put it [DK: name of school] in my profile and got some recommendations, and there were even people I did not think of."

Jack used *Facebook* as a database not to find specific people, but to assemble people based on the data conveyed through his search query. While Jack like many participants is concerned that online companies collect personal data and monitor him, he does not relate his own search query to *Facebook* as an agent of surveillance.

Data doubles as digital equivalents of people are not just analytical categories that diagnose macro-sociological trends, but have found their way into people's lived experience. As such, people's attention to personal data on the internet is well documented, for instance through teen's practices of curating their social networking profiles (boyd 2008), or attitudes to online privacy (Fuchs 2013). But beyond these tropes, people relate to, engage with, and communicate through their data doubles themselves, revealing much wider issues about the mundanity of living with online surveillance.

5.1.4. Watchers and Watched

Participants generally associate surveillance with a clear distinction between 'watchers', who conduct surveillance, and 'watched', who are exposed to it. Surveillance appears to them as a linear process within the binary of the state or CCTV on one side, and people under their gaze on the other. This dualism continues to exist in people's wider conceptions of monitoring on the internet, which they often frame in other terms than surveillance, and which incorporates online companies as watchers. Yet participants' narratives discussed so far already hint at a sometimes more complex configuration of watchers and watched. For instance, talking about his *Couchsurfing* experience, Dennis indicated the role of another type of agent in the monitoring process – people like himself. This is echoed in stories about data doubles. Participants engineer their data doubles both to be found by others, and to search for others as well. Online destinations such as SNS, in addition to gathering and analysing data themselves, become intermediaries for new configurations of watching and being watched between people. However, the examples introduced so far are only marginal expressions of the wider phenomenon of peer-to-peer surveillance. This section explores how peer-to-peer surveillance manifests itself, and how it contributes to the dissolution of surveillance as a distinct category in everyday life.

When I asked Martin who he thinks is interested in his personal data, the sales manager from London immediately produced a long list. Alongside his employer and online companies, he mentioned friends and their peers:

[5, 20] "Of course, Google and such, my colleagues, friends of friends, my friends, actually everyone. When I post something, I get like 'Oh, have you done this and that', and I am like 'Well, it also wouldn't have interested you if I had just met you on the street'. I think everyone is generally interested."

Martin's friends are not powerful corporations or government agents that exercise any form of top-down power over him. They are internet users just like him, not particularly technically advanced, neither trained in surveillance tactics and data science, nor with access to specialist online tools. Despite this lateral relationship, he mentions them in the same vein as hierarchical forms of surveillance. This is not an expression of the magnitude of his concern, and Martin later added that he is more worried about companies spying on him than his friends snooping around on his social media profile. Yet his statement shows that other ordinary people join more established, top-down agents of surveillance as just another group of watchers that participants encounter.

Being monitored by friends is not a rare occurrence, but a systematic component of being online that is embedded in an overarching framework of other surveillance experiences. The immediacy of reactions from friends on his *Facebook* posts remind Martin that someone, somewhere, is always watching, and other participants acknowledge the perpetual gaze as well. This is echoed by Amanda. I met her while I was pinning my calls for participation at a university message board in London, where she was posting flyers for her badminton society. The finance student admits to being addicted to her smartphone. One of her most-used apps is the location-based service *Foursquare.* She opens the app on her phone to virtually 'check in' to places she visits in the physical world, like cafes, airports and her university, earning online points and badges for each time she shares her location. *Foursquare* for her is a way to share her whereabouts with friends and sees it as a fun way to compete with others for badges earned at regular places. Amanda has been at her local coffee shop so often that she received the 'major' badge. But like other SNS, *Foursquare* is not all carefree:

[5, 21] "If you have shady ex-boyfriends or shady best friends or frenemies or whatever they want to call them, you should definitely be cautious online and with your movements. And I mean everyone has them, sometimes you just don't know yet [laughs]. That's the question that all of these new features, these location-based features bring into play, you

> know. Like Foursquare, you check in you're here, so they know you're not home. Or if you have a stalker boyfriend, he knows where you are."

Unlike Amanda, who voluntarily uses *FourSquare*, Christina, the business journalist, reported how she became exposed to peer-to-peer surveillance on *Facebook* without actually having a *Facebook* account. She felt compelled to join *Facebook* in order to intervene in peer-to-peer surveillance taking place at his expense:

> [5, 22] "The whole reason that I joined was Facebook was to try and control. Because when it came about and went big some years ago, I was told that people saw pictures of me, and they talked about it on Facebook. They knew about my life, and things that I did not even know and they talked about it on Facebook. And there was this creeping idea that there were all these pictures of me, and I did not even know what they are."

Participants recognise that exposure to peer-to-peer surveillance is inevitable and just as much a part of being online as leaving data traces. In particular, SNS produce unintended consequences which allow people to track others' conversations and whereabouts. Legal secretary Joanna from London, even suggests that the prospect of peer-to-peer surveillance is baked into the appeal of SNS and an important motivation for people to join in the first place:

> [5, 23] "Everyone's doing it, right? I mean that's why most of us log in to Facebook all the time, to see what's new and to snoop around a little. Maybe some people don't notice, but to be honest, you gotta be really naïve if you don't see this, I think it is why everyone is on Facebook, it's the perfect spy tool."

The 26-year-old's statement shows that peer-to-peer surveillance is not just a nuisance or potential threat, but also a source of entertainment. It is through narratives of surveillance as entertainment that participants frame their own complicity in peer-to-peer surveillance. Participants find themselves in a dual role of being watched, and taking the role of watchers themselves. Karen enjoys snooping on her friends. Although other participants admit to spying on love interests or other specific people, the dental hygienist from London is not plotting a scheme against a particular person, or systematically following someone. Instead, she highlights more widely how surveillance as entertainment is familiar and often uncontested to participants:

> [5, 24] "Now Facebook is so like, it shows you any activity that anyone does. So you don't have to do any stalking yourself to kind of be updated on what anyone does. And if you want to know more, you can still snoop around on their profiles and yes I admit, can I say that, I am not a creep, but it is kinda fun."

Karen did not make an active to choice to participate in peer-to-peer surveillance. Her complicity just happened by means of using *Facebook* and its technological affordances.

For many, using these affordances and engaging in at least the casual monitoring of others is socially expected by those who are being watched. Apart from an intrusion, the deliberate submission to being watched is an integral part of everyday monitoring between peers. Franzi, a 24-year-old physiotherapist from Aachen highlights:

> [5, 25] "There are these expectations. That I like or comment on a photo and that I do that quickly. If I now, and someone did that to me once, if I only like a photo after a year or so and comment, that's weird, and then I'd say that person is creeping on me. But apart from that, it is kind of expected that you follow the lives of other people. What is Kerstin doing, so a friend of mine? I always have to keep an eye on that. Otherwise, she is upset." [DK: translation from German]

Peer-to-peer surveillance is embedded in a system of complex social norms that determine when monitoring is acceptable and even desired, and when it is frowned upon. It is not a monolithic phenomenon but contains many nuances which determine what is unwanted surveillance, and what is accepted monitoring. The act of watching itself is present across these forms of peer-to-peer surveillance, but its interpretation changes.

All these examples show that peer-to-peer surveillance is a complex phenomenon. Yet despite differences, at large, peer-to-peer surveillance erodes the binary relationship between online consumers on the one hand and specialist agents of surveillance on the other. Surveillance moves from a hierarchical to a lateral relationship and modalities of being watched and watching alternate and overlap. Participants live in a surveillance-saturated world where mutual monitoring is part of popular culture that they actively participate in and which is normatively coded. Through peer-to-peer surveillance, various forms of monitoring become part of daily encounters and interactions with other people, contributing to the normalisation of surveillance as a fact of life.

Participants are not adamant to differences between peer-to-peer surveillance and forms of surveillance conducted by other types agents. The often frivolous and playful nature of peer-to-peer surveillance for people has very different consequences than in particular computational forms of monitoring, which people struggle to grasp in their processes and intentions, as the next chapters will show in more detail. However, as in particular Martin's example has shown, participants still experience peer-to-peer surveillance as part of a wider universe of experience composed of different forms of surveillance. Embedding peer-to-peer surveillance in this broader framework also shapes people's relationship to surveillance at large. Peer-to-peer surveillance not only stands for the familiarity and mundanity of being watched by other people. It also problematises

people's relationship to other forms of surveillance. Franzi feels uneasy about being tracked on the internet by large corporations, but she is not sure whether she is entitled to feel that way given that she spies on her friends:

[5, 26] "Can I really be upset about this if spy on other people myself? That's a contradiction somehow." [DK: translation from German]

Franzi does not equate peer-to-peer surveillance to corporate tracking but nevertheless puts the two in a relationship. Living in a world of pervasive monitoring, she struggles to separate between permissible forms of surveillance and legitimate reactions to it. The omnipresence of monitoring makes it difficult for her to take a moral stance on surveillance, evaporating possible dissent.

As the above discussion has shown, peer-to-peer surveillance contributes to the normalisation of surveillance in multiple ways. It adds a lateral form of monitoring to a traditionally hierarchical relationship and creates a sense of familiarity with those who watch. It further embeds surveillance into everyday experience, establishes it as a potentially desirable, entertaining phenomenon that is surrounded by a set of social norms and expectations. Lastly, it erodes the boundaries between watchers and watched, turning participants into agents of surveillance themselves. Taken together, these factors normalise the lived experience of surveillance and complicate the assessment and judgement of other surveillance phenomena.

5.1.5. Synthesis: Between Omnipresence and Dissolution

As surveillance becomes ubiquitous, it ceases to be a distinct phenomenon. The proliferation of data, the incorporation of data doubles as meaningful categories in lived experience and the rise of peer-to-peer surveillance expand people's exposure to and implication in various strands of surveillance in the broadest sense. Surveillance becomes normalised as an integral part of everyday life that is enmeshed with and indistinguishable from other practices, and that has multiple connotations. Deleuze (1992) has claimed that in societies of control, surveillance leaves the contained environments of disciplinary institutions and becomes ubiquitous. Two decades later, participants' narratives confirm this diagnosis. They also suggest that surveillance as a concept blurs and dissolves in the context of its perpetual expansion. While people's definitions of surveillance as they perceive the term vary between Germany and the UK, participants in both countries share similar experiences of the normalisation of the phenomenon 'surveillance' as it is

conceptually understood in academic literature. In the domain of online life, being monitored, calculated and controlled is neither an outside act, nor an intrusion into an idea of life that is ideally free from such interventions, but a constituent part of it. This changes how people perceive surveillance, define and relate to it.

5.2. A New Landscape of Risk

Surveillance in the widest sense is a mundane and routine phenomenon deeply intertwined with and often indistinguishable from other everyday practices. However, although people accept the general existence of surveillance as an unchallenged fact, they do not stoically succumb to it, are apathetic towards it or engage with surveillance in an un-reflexive manner. The previous analysis already contained a broad range of statements from participants about their concerns and useful or entertaining associations with surveillance. This section documents how such attitudes are embedded in experiences of risk. Framing surveillance as risk establishes a framework through which people's relationship towards surveillance can be understood. In a first step, this section highlights that computational surveillance takes a particular role in the experience of risk. It then outlines participants' conflicting perceptions of surveillance and how their inability to resolve these contradictions fuels a narrative of risk. The last step illustrates that surveillance risks are associated with broader questions around agency and computation.

5.2.1. The Risky Nature of Computational Surveillance

Evelyn from Erfurt has gotten used to being monitored online and thinking of surveillance sparks a sense of indifference. At the same time, she is concerned:

[5, 27] "You are being spied upon everywhere on the internet these days, I really got used to it, it is just like that. And I don't think 'shit, that's crazy' but just take it in. Still, I'd say that I am somehow afraid." [DK: translation from German]

Accepting surveillance as a mundane part of everyday life and yet having a sense of fear are not conflicting attitudes for the 20-year-old psychology student. Her fear is abstract and diffuse, not concrete.

[5, 28] "Fear, in general, that things can happen with my data, that I…I can't describe what could really happen, that it somehow has negative consequences somehow at some point." [DK: translation from German]

Evelyn's fear can be understood as a sense of risk following Beck (1992) that surveillance sparks unintended consequences which cannot be anticipated in the present. This feeling

of risk is widespread among participants. Ann-Kathrin, who is a fellow student in Evelyn's course in Erfurt, highlights:

[5, 29] "You gotta see the big picture behind it. With Google, I don't have Googlemail, it is said that they store data. And then this car, err, Street View. You have to see this together; it is all Google and the data, that's all connected. And if Google wants to abuse that, they have the perfect basis, because all data is there. And I am afraid of that, also that I don't have any form of control and what could happen." [DK: translation from German]

Ann-Kathrin acknowledges the complexity of online surveillance and its networked character. However, appreciating this complexity also prevents her from assessing a specific threat and possible outcomes of surveillance in the first place. Katy, who lives in Kent but studies in London to become a translator, agrees. For her, acknowledging the complexity of online surveillance is not the basis for understanding it, but the beginning of recognising the inability to assess it:

[5, 30] "That companies are spying on you… it is in the news so I did a bit of reading. But the more you want to understand what's going on, the less you really get it. At least that's what I think sometimes."

For many participants, the notion of such risk is unevenly distributed and particularly pertinent in the context of online surveillance conducted by commercial computational agents. In part, this attitude relates back to the narrow conceptualisation of surveillance in their own terminology. Evelyn adds:

[5, 31] "The state, you kinda know what they want to do with the data and since I am not a criminal I am not afraid." [DK: translation from German]

Ian, a 25-year-old charity worker in London, adds a similar view towards peer-to-peer surveillance. Its intentions and possible outcomes are straightforward, and Ian can grasp them in their entirety:

[5, 32] "I'd say when my friends are spying on me, that's kind of, well if you are honest with them and hide what you don't want them to see, it is not dangerous really. And that's different when you look at all these data collection companies, you can think ah ok, they may want this for their advertising but you can't be sure what they do with your data, and maybe they sell it on, it is completely in the dark."

Although surveillance is a pervasive phenomenon that in all its different iterations contributes to the normalisation of monitoring, attitudes towards surveillance are complex and embedded in a nuanced assessment of risk. Such assessments are structured based on possible consequences of surveillance, not its actual depth of intrusion. In the context of computational surveillance, participants struggle to spell out what these consequences

might be, how and when they might manifest themselves and what steps to take to avert them, establishing a hierarchy of risk.

5.2.2. Risk as Contradictions

Despite people's concerns, they do not just consider computational surveillance as a potential threat. Participants' narratives about the normalisation of surveillance have already indicated a more complex set of attitudes, where surveillance has utilitarian or even entertaining dimensions. Yet the notion of risk also includes the struggle to determine whether a phenomenon will have negative consequences at all, and how to balance such future consequences against present benefits (Nassehi 1997). In this vein, participants struggle to ascribe a fixed set of attitudes to surveillance. For instance, the inevitable 'deal' they strike when online also has positive connotations as Paula, a homemaker and part-time yoga instructor from Aachen highlights:

[5, 33] "They always show you what you've bought, what else could interest you, what other customers have… that's always pretty amazing. They definitely analyse your clicking behaviour, your purchasing behaviour and somehow offer you things so adequately. […] Well, I always like when it says 'customers who have bought this article have also…'. Sometimes that's quite interesting; you somehow find something that you wouldn't have thought of yourself." [DK: translation from German]

Paula does not want to miss these recommendations. But she also thinks that *Amazon* has a dark side. This dark side remains vague for her and is based on speculation. Paula struggled to answer my question how she stands towards surveillance. Instead, she recognised me as an expert, who could help her build an assessment of the diffuse sense of risk that she experiences:

[5, 34] "It can of course happen that they continue to analyse my data and if they get hacked, that this can be used in some way against me. That's always a double-edged sword and if you ask me now how I stand towards it… hmm…honestly, I don't have the skills to assess that. How dangerous is this really? I have often wondered; could you tell me?" [DK: translation from German]

While Paula is wondering about hypothetical consequences of being monitored, Bashir, a medicine student from London, reported a specific incident that made him consider the role of surveillance in a particular situation:

[5, 35] "A while ago I got this new debit card, and I went out to buy groceries. And I still remember, I got this frozen pizza. A few days later I got an email from this online supermarket, and there was a promotion of a new frozen pizza. The thing is, I never really buy frozen pizza, just this one time because it was exam week and I could not be bothered to cook a proper meal. So I was like – does my bank sell on my information? I mean, what are the odds really? That was just too convenient. But then I can't imagine banks are allowed to pass

> on this information, so I calmed myself down. But yeah, I still don't know for sure to be honest when I think about it."

Like Bashir and Paula, for many participants assessing the risk of living with surveillance is an unfinished exercise that they struggle to conclude. Andre, aged 29, works in a car body shop in Aachen. Although he generally prefers the 'real world' as he calls it, to the internet, during the evenings, he can frequently be found tinkering with his PC or finding car parts on auction websites. The adverts on these car sites originally made him think about being monitored, and now he cannot quite resolve what stance to take:

> [5, 36] "This is always like hot and cold. Am I being spied on or not? You don't know, and it always is a fourth and back. But you don't get closer to the truth and in one moment I don't care, and then again I'm paranoid. With all these internet companies that analyse you, you just don't where you're at." [DK: translation from German]

These narratives illustrate that attitudes towards surveillance are not straightforward and embedded in a web of changing assumptions, experiences and assessments. The risk of living with surveillance does not manifest itself as a specific threat but through the intransparency of intentions and modulations of computational agents.

5.2.3. The Computational Halo of Risk

When I met Stuart, who works as a loans advisor at a bank in Piccadilly, he was not concerned about exposing his personal data on the internet. He regularly encounters news reports that warn about data collection and some of his friends go to great lengths fine-tuning privacy settings. But Stuart does not see any risks to exposing himself:

> [5, 37] "Risks? I can't think of any risks. Like the only risky thing I do is I go to my bank's website. And I think banks should have this stuff figured out and protect my data, so I am not really afraid, so I don't really think about that when I'm online like doing my stuff…that someone can do…what someone can do with my data. And I mean what's so important, and why would someone be interested in me? I am not that important, like there are thousands, millions, whatever. So there is nothing particularly interesting that I would imagine…I could not imagine, that it is that there is anything interesting to find out about me."

Stuart, who is aged 26, joins a small group of participants who shrug off an otherwise pervasive need for data protection that surfaces in other narratives. Stuart thinks his data traces are ordinary and that he does not stand out, allowing him to disappear in plain sight. He also alludes to an argument often purported by defenders of mass-surveillance that those who have 'nothing to hide' also do not need to fear surveillance (Solove 2011). Even if he was monitored, Stuart cannot imagine that his information would generate any interest or spark any consequences for him.

Annegret recently started her apprenticeship to become an optician in Erfurt. She highlights:

[5, 38] "I don't have anything to hide, why should I be worried? We're all naked anyways and then it does not make sense to hide, it is just not contemporary anymore." [DK: translation from German]

Annegret, who is 19 years old, believes that she has long lost any privacy to computational surveillance and that whatever measure she takes, it cannot be restored. Annegret has stopped worrying about exposing herself and has accepted that she lives in an age where privacy is non-existent. Both Stuart and Annegret embrace a post-privacy paradigm to their everyday lives online. But although they appear to dismiss any surveillance risks, they are not as indifferent to surveillance as their statements suggest. Annegret regularly uses *Amazon* to order books and relies on its recommendation feature to discover new products. But one purchase seems to have confused *Amazon*'s recommendation algorithm and rendered it useless to her:

[5, 39] "You always get these recommendations on Amazon 'you could also like this' and so forth, and I always think oh damn, if I could somehow influence this, because the recommendations are all wrong, well I once bought a book, and this was a one-off for my sister and now I suddenly don't get any decent recommendations anymore. I always found that a real cool feature and it was really handy but what I get now, how can I turn that off?" [DK: translation from German]

Amazon's recommendations are based on monitoring Annegret's browsing and purchasing habits. Instead of objecting to this data being collected, like some other participants do, Annegret embraces it and has come to rely on *Amazon*'s calculations. But a single act, her purchase, suddenly disconnected *Amazon*'s conclusions from her actual preferences. Annegret does not know what went wrong. She does not know whether her purchase, *Amazon*'s conclusions, or a combination of both had been behind the loss of relevant recommendations. She does not have any insight into the computational logic behind *Amazon* and, at the time that we spoke, had been unable to revert to a state where *Amazon*'s recommendations were of the same value to her as before.

Stuart encountered a similar incident right during our interview. When he logged into his *Facebook* profile following our think-aloud session, he saw his ex-girlfriend showing up as a recommended friend next to his newsfeed. He sighed:

[5, 40] "Here, not again, this always happens, she's my ex, and we unfriended each other a long time ago, and I thought I blocked her, but she always shows up. It is so annoying, fucking Facebook. I really don't want to see her, and Facebook just keeps recommending her. To

> be honest, that completely ruins my day when that happens. And it gets worse when my friends who are still friends with her like her stuff and it appears in my feed."

Stuart and his ex-girlfriend did not break up on good terms. They unfriended each other on *Facebook* and eager not to be reminded of the past, Stuart blocked her in his settings. But although he exhausted all technical means to the best of his knowledge, *Facebook* neither acted on his explicit inputs on the user interface, nor did it infer that Stuart did not want to see how his friends interacted with a person he had unfriended. Stuart felt powerless, unable to communicate his intentions to *Facebook* and uncertain when he would be exposed to unwanted memories of the past again. His *Facebook* experience had slipped from his control, and it mattered to him.

Both Stuart and Annegret claim not to care whether they are being monitored and have given up on the concept of privacy. A conventional understanding of surveillance would suggest that both participants do not share others' experiences of risk stemming from online monitoring. Yet taking a wider view on surveillance as it sinks into the everyday reveals a more complex picture, where risks of surveillance return to Stuart and Annegret in the guise of other encounters. Stuart and Annegret problematise situations that entail, or are based on being monitored. These situations do not fit into a traditional rhetoric of either resisting surveillance or submitting to it. They are not even framed specifically as surveillance encounters and instead appear as problems arising from the unintended consequences of computational logics. Stuart's and Annegret's stories highlight that rejections of surveillance risks only extend to an insular understanding of surveillance as a distinct phenomenon. Widening the analytical prism on surveillance shows that consequences of being monitored are much more far-reaching. Stuart and Annegret worry about their sovereignty as individual agents in a computational world and face the risks of exposure to unwanted experiences.

5.2.4. Synthesis: A Landscape of Risk

Living with surveillance is embedded in a landscape of risk. People attach different measures of risk to various forms of surveillance, and computational surveillance stands out as participants struggle to grasp its intentions and consequences. Attitudes to surveillance are not straightforward and alternate between threat and more positive connotations. These often are not grand claims about surveillance, but situated statements that refer to specific online practices in which surveillance plays a part. At the same time,

as surveillance erodes as a distinct concept, implications of surveillance can be found in experiences that are not surveillance-centric. Paradoxically, it is those statements which refute the notion of surveillance as risk that most explicitly hint at the implication of surveillance and computation in creating a much wider experience of risk.

5.3. Chapter Conclusion

This chapter created a foundation for exploring how people relate to computational surveillance, the core theme of this thesis and the analytical focus of the next three chapters. It set out by problematising the notion of surveillance itself. Theoretical approaches note a pervasive spread of surveillance in contemporary societies of control. This is echoed by empirical analyses that document people's attitudes and acts towards surveillance, for instance in the context of CCTV (Toon 2000) or online privacy (boyd 2008). Yet such approaches assume that surveillance enters people's lived experience within conceptually defined boundaries as separate and distinct phenomena. This chapter has shown that a much wider perspective is necessary to understand how surveillance is embedded in people's everyday experience, and that doing so requires to de-centre surveillance research. In a first step, this chapter has shown that people's narrow definition of surveillance itself is related to the omnipresence of surveillance in everyday online practices. Paradoxically, as people perpetually encounter and engage with surveillance, the concept of surveillance erodes and sinks into their wider lived experience. Surveillance becomes a mundane fact that has become normalised and entangled beyond recognition with other practices. In a second step, this chapter has shown that the normalisation of surveillance does not imply indifference. In particular, people struggle to assess the benefits and threats emerging from computational surveillance, leading to fluctuating attitudes and conflicting assessments of surveillance that are always temporary, until further notice. Living with surveillance takes place in an environment of risk. These risks often do not relate to surveillance as such, but to the computational context which it is part of. Together, the two constituent parts of this chapter illustrate that an empirical analysis of the lived experience of surveillance requires, and cannot be separated from an understanding of wider online practices and how people relate to computational agents. The following chapters build on this conclusion.

Chapter Six: Experiencing the Fleeting Conditions of Knowledge

I had just occupied an office on the sixth floor of a 1960s high-rise building on the university campus in Erfurt, Germany. It was the time of the football World Cup, and Germany was to play Ghana tonight. Looking out of the office window, I glanced over a park where stagehands were busy erecting a large screen on a metal scaffold, as well as setting up drink and sausage stands for the night's live broadcasting event. The ground was covered in cables, amplifiers, electrical switches, a test image illuminated the screen, speakers were being wired, sound checks performed. Against the green nature, this technology hub looked strangely out of place, isolated, starkly naked, its contours pronounced in juxtaposition. From up here in my temporary office, the entire event's infrastructure was laid bare. It was visible and comprehensible. Each cable, each wire, was placed in a grid, bundled together, lines running in parallels. Their routes could be traced from beginning to end, input to output. From the electrical generator to the LED screen, each object's single purposes could be inferred, their joined orchestration could be grasped.

The arrangement I looked down on, where the screen and its infrastructure are visible in unison, represents a particular way of perceiving and understanding the world. It also stands for a theme I was going to explore in my tower office with local students, just as with other participants before. I wanted to speak with them about screens and their surrounding infrastructure. But my interest did not lie in tangible objects like cables and wires. Instead, I intended to explore their relationship to the infrastructure of computation that orchestrates online surveillance. The theoretical framework of this thesis has hinted at the complexities of this relationship and problematised the difficulties of grasping computation. To recall the basic argument: I have proposed that computational principles, which jointly from a computational logic, stand at odds with human modes of making sense of the world. However, such a logic increasing shapes the social world and how people perceive it, what Kallinikos (2009) has called the computational rendition of reality. This computational logic constitutes an infrastructure. Parks (2012) suggested that infrastructure exists on a spectrum of visibility and invisibility and I argued that a computational logic is categorically invisible. Drawing on Brighenti (2007), I framed visibility both as a domain of perception and of power that facilitates understanding and

agency. I concluded that in dealing with computation, people are confined to its representation of the interface on the screen, and lack the ability to query its underlying infrastructure that contains its logic.

This chapter takes an empirical perspective on this problem. It investigates how people in everyday life experience the relationship between their ability to make sense of the world and the computational logic it is governed by. On this basis, it explores how, if at all, people are able to construct knowledge about computational surveillance. It then continues to discuss how this stock of knowledge and modes of generating it influence people's self-perception as capable agents. In order to tackle these questions, the chapter draws on the catalogue of theoretical concepts that I introduced earlier. Specifically, it leans on those concepts in *Chapter Three* that I used to illustrate the crisis of perception and understanding in the context of computation. In this introduction, I briefly take stock of these concepts.

I already referenced the idea of a computational logic, the concepts of interface and infrastructure, as well as the notion of visibility above in justifying this chapter's approach. Additionally, the chapter makes reference to Lash's (2007) concept of generative rules. Lash argues that algorithms – what I more widely call a computational logic – operate on the basis of rules. Unlike constitutive and regulative rules which are historically conveyed through ideologies and consensus of human agents, generative rules operate from the inside of algorithms themselves. They are hidden from view and not represented through intersubjectively comprehensible codices. I use Lash's concept to shed light on people's self-understanding of agents in the context of these rules. A further concept I reference is that of Hayles' (2007) cognisphere. Hayles suggests that people are increasingly embedded in cognitive systems of global, interconnected data flows. Largely, these flows are characterised by data exchanges between machines. In this cognisphere, comprised of both human and machine cognition, humans can only grasp fragments of the much wider exchanges taking place between machines (Hayles 2007). I set the idea of the cognisphere in relation to Marks' (2006) concept of unfolding in order to describe the modulations of the cognisphere that people experience. Marks argues that all code – another shorthand for the computational logic – is usually enfolded, hidden from view in an endless virtual domain. Unfolding denotes the process by which specific images reach people out of the pool of enfolded information. Lastly, this chapter

introduces a complimentary concept in order to bridge empirical reality and theoretical framework. To shed light on people's practices in the context of interface and infrastructure and the corresponding idea of visibility, I reference the notion of exosomatic organs. Coined by Innis (1984), the concept denotes artefacts, such as camera, telephone, microscope, or binoculars that reside outside of the human body, but which can be appropriated to augment human sensory abilities and mediate between them and the outside world.

The overarching theme of this chapter is the construction of knowledge. It is situated in the wider framework of this thesis that incorporates Berger and Luckmann's ([1966] 1991) notion of the social construction of reality, Kallinikos' (2009) computational rendition of reality and the associated concept of computed sociality (Kallinikos & Tempini 2014). The succeeding chapters will make more explicit references to Berger and Luckmann, including the social aspect of constructing knowledge and issues of resolving glitches between objective and subjective reality. This chapter's main emphasis is neither the social dimension of the construction of knowledge nor the agency towards computational surveillance that comes from it. Rather, it is an exploration of the conditions under which knowledge takes place, and the possibilities and limits which these conditions afford. The chapter's emphasis, therefore, reflects the positioning of the theoretical concepts it uses within the wider theoretical framework, which prepare for the later theoretical introduction of Berger and Luckmann. Just as concepts of infrastructure, interface and visibility constituted groundwork in the theoretical framework that resulted in my adaptation of Berger and Luckmann's theory, this chapter provides groundwork for the next two empirical chapters which lean more strongly on Berger and Luckmann's concepts. However, as the chapter is interested in the conditions of knowledge, it makes repeated references to Kallinikos and Tempini. The computational rendition of reality highlights the problem of knowledge, and the notion of computed sociality delineates the particular social configuration in which people's encounters and experiences take place. While the idea of a computational logic and associated concepts are well suited to illuminate the empirical material discussed below, these references help to sharpen the argument in light of the overall thesis outline and simplify the narrative connection between the themes discussed here and the next chapters that draw more heavily on Berger and Luckmann.

This chapter is divided into three sections. It begins by discussing how people experience and define what I call ‘conditions of possibility’. These are the limits and affordances presented by the categorical invisibility of the computational logic and its generative modus operandi. The next two sections deal with how people construct knowledge about surveillance on the basis of these conditions of possibility. The first of these sections explores how people try to circumvent the need for knowledge by drawing on technological tools that act as outsourced agents on their behalf. The last section looks at unfolding events, or how computational surveillance appears to people against all odds. It documents people’s lived experience of unfolding as well as their attempts to reconstitute their role as agents in control over the conditions of knowledge through acts that provoke unfolding events on their own accord. The empirical material discussed in this chapter reflects all participants. Although only a selection of them is referenced in my narrative, the patterns analysed in this chapter are applicable to the entire pool of participants. I include dissonant voices from single participants whenever a phenomenon was not consensual or more nuance required.

6.1. Conditions of Possibility

Constructing knowledge about online surveillance first and foremost is not a set of practices or a process, but a problem. The principal agents of online surveillance are computers that operate through algorithms, code, big data and related concepts – what I have previously called a computational logic. When I spoke with participants about how much they knew about surveillance and their ways of figuring out its presence and workings, conversations often shifted to how little they knew, and the obstacles in their way to understand surveillance. People wanted to emphasise the conditions under which they make sense of a computed world and saw these conditions as justifications and explainers for their understanding of surveillance. These conditions also featured implicitly in their accounts when they reflect on themselves and on idealised ways of coming to terms with surveillance. I call them conditions of possibility because they structure any further approaches to surveillance. I introduce them in this section and distinguish between a rational and reflexive logic of computation on the one hand, and its mode of appearing to participants, or visibility, on the other.

6.1.1. Becoming Like Machines

Andre from the car body shop, whom I introduced in the preceding chapter, does not come across as a particularly frightful character. Speaking in a firm voice, serene and mellow, he appears confident when talking about surveillance on the internet. While he is aware of risks associated with surveillance, he does not seem scared or overly uncomfortable about the prospect of being monitored. Yet he suggests that being online requires constant vigilance:

[6, 01] "In theory, you always have to walk on eggshells." [DK: translation from German]

Andre's statement implies a particular state of consciousness characterised by heightened awareness, diligence, self-questioning, and constant re-assessment of situations. Such paradigms of watchfulness are recurring themes in participants' narratives. For instance, Mark highlights:

[6, 02] "When it comes to Facebook or Google spying on you or all the other online companies, you can't afford to be sloppy. You should always keep your eyes open ideally."

Yet while similar analyses are pervasive, participants also acknowledge that such imperatives are unattainable as qualifications such as 'in theory' or 'ideally' illustrate. Andre expanded on this when he talked about a file-sharing service that he uses to download movies and music:

[6, 03] "I would really say that I am a realist. It is not possible to keep all these things in mind. You cannot put together scenarios, play through a game of 'what happens if', before you do anything on the internet. So even when I download a movie or so, I certainly know that people have received cease-and-desist orders because someone had monitored their online traffic. And then I sometimes do think, umm, now you have to be careful, or you do need to be more careful, but not all the time – that is virtually impossible." [DK: translation from German]

In his eyes, constant vigilance requires anticipating, imagining and thinking through what he calls 'what-if-scenarios', a constellation of potentialities that connect individual online behaviour with surveillance-related consequences. But Andre feels that he cannot live up to the principles he sets out himself. Similarly, Mark struggles to provide a blueprint for watching out for surveillance:

[6, 04] "I can't really tell you the best way. It's not that I say this and that, that's what you have to do to, you have to be open for everything that could happen. It could be anywhere really, I mean you cannot see that it's actually happening and where and when. I guess, and you probably just have to have a sense of it and try to be careful whatever you."

Both Andre and Mark are among those participants who want to protect themselves from the gaze of surveillance. But discrepancies between an envisioned approach to surveillance and actual practice extend across different attitudes to being monitored. Several participants are not concerned about surveillance, and others have given up on figuring out where and how surveillance operates altogether. They nevertheless engage in similar rhetoric about vigilance. For instance, Katy, a student from London is carefree with her personal data, sharing it to receive better online recommendations and useful advertising. Still, she hopes that she could understand the principles by which a computational logic operates in order to better engineer her exposure. Vigilance for her is not a means for protecting herself from surveillance, but a precondition for engaging with surveillance in a way that is beneficial for her. Others, like Linda, who just finished her maths degree and moved to London, claim that they 'don't care anymore' about surveillance because there is nothing they can do about it. Yet as conversations progressed, such participants emphasised that their attitude towards surveillance stems from a systematic lack of access to its logic. Martin is stuck in the middle. He worries about surveillance but has adopted a laissez-faire attitude:

[6, 05] "Uhm, if I thought about it constantly, I'd probably not be able to sleep anymore. […] I try and don't think about it with every click I make. I'd go crazy."

At first, I understood his statement as an expression of worry, where he bracketed the concerns about pervasive surveillance from his consciousness in order to eliminate ongoing, nagging fears about the consequences of being monitored. But as our conversation progressed, he helped me see his statement in a different light. Martin alluded to the dimensions of time and complexity and not to the issue of fear. He meant that trying to figure out how surveillance works would be so time-consuming that he would not be able to fit it in a day, and that probing into the mechanisms of surveillance would exceed his cognitive abilities, leading him to 'go crazy' if he attempted to decipher it.

These very different narratives illustrate that at its most basic, the idea of vigilance is not principally related to personal protection from surveillance, but to the issue of generating knowledge about surveillance. Independent of personal attitudes to surveillance, the struggle to constantly monitor one's web activities in relation to surveillance alludes to categorical differences between human and computational agents. These differences structure awareness of the occurrence of surveillance and knowledge about its shape,

modalities and intentions. They become explicit in accounts that construct an us-versus-them rhetoric in which participants create a dualism between man and machine. Linda highlights:

[6, 06] "Google and all the others, it's like they have computers, unlimited resources, I mean it's different. You are now being faced by machines, and you got to behave like a machine ideally if you want to fight back. Like machines don't tire, and they are faster."

This juxtaposition between human and computational attributes occurs time and again. Andre recognises that his personal attributes of being in the world and making sense of it are not compatible with how computational agents operate:

[07] "I can't think as fast as a computer, and I can only be at one place at a time, but we are surrounded by computers everywhere – how should I as a person know how computers work, it is not that simple to figure out." [DK: translation from German]

Andre makes a distinction between his bodily presence and the networked nature of computation. He also hints at obstacles of figuring out how computation operates, an issue that other participants formulate more explicitly. Some lament that they are not coders or programmers, and thus position themselves as lay agents who are exposed to coming to terms with a phenomenon that requires expert skills. Others do not dwell on expert and lay distinctions, but emphasise the inaccessibility of a computational logic at large. Constanza, who is an Italian-born artist based in London, says:

[6, 08] "Like how shall I figure out how an algorithm works and all that data that is being sucked in how that is processed, I guess nobody knows really, it's all a black box. I know that they are using my data, but I don't know which data and what they make of it, like how they read it, and you hear stories sometimes how that is not always correct. I guess that's the issue, where shall I start and what can I really do even if I wanted to?"

These stories stand for participants' profound awareness that they are embedded in a computed world which produces knowledge about them, but which is not accessible as an object of knowledge in the same way. Both Andre and Constanza try to justify themselves through rhetorical questions as if they needed confirmation and self-assurance from others that they really could not do more. In particular those like Constanza who consider themselves proficient in their use of computers, are aware of latest software and effortlessly use terms like 'algorithms', feel a sense of shame that they have hit a glass ceiling, and have to capitulate to the logic of computation. Being vigilant is firmly connected with this sense of shame. It is an expression of the need to adopt to the modus operandi of computation itself in order to systematically establish it as an object of knowledge. To recall, Lash (2007) has argued that computation operates on the basis of

generative rules. These are hidden rules inaccessible to human agents characterised by self-questioning, self-learning, rule-finding and constant reassessment - they are perpetually reflexive. According to Lash, dealing with computation in everyday life requires people to adopt the same paradigms that underpin generative rules. Participants' narratives show that his argument meets a world in which people have already formulated a maxim of calculative rationality and reflexivity to echo the modalities of computation. But people know that being calculative, rational and perpetually reflexive is an unattainable task. People know that in order to understand computational surveillance, they have to think more like computers, but face the limits of their minds and bodies that prevent a closer, systematic approximation.

6.1.2. Out of Sight, Out of Mind

When I met James, who works as a barista, our conversation kept coming back to a single topic. James experienced a sense of blindness that he could not let go of. Surveillance was a threat to him, and he was more concerned about CCTV than internet surveillance. Yet at the same time he found it easier to live with the bigger evil - CCTV surveillance - because he could see the cameras. They communicated their physical presence, allowing him to assess the situation he was in. His experience of internet surveillance was different. I struggled to get answers to my questions, such as where he was being monitored, and how he thought his data was being used. James replied with slight variations of a one sentence statement, from 'I don't know, I can't see how it works' to 'You just don't see it, so how should you ever know.' James felt that he could not answer my questions in more detail because without his human senses being able to both perceive and understand surveillance, everything was speculation. Online surveillance for him was confined to the back of his mind as a lingering, unspecific and ambient awareness:

[6, 09] "I think nowadays it's in the back of your head most of the time. Not like in a panicky way where you end up worrying all the time: It is more, I would say it is a general sense that it's there. […] But you can't see it so you don't really think about it."

It was only when I broached the subject of *Amazon* that James opened up. Participants I had spoken to previously had repeatedly referenced *Amazon* as an example of online surveillance. James concurred:

[6, 10] "Oh yes, Amazon. It is an exception, the recommendations you get, that is obvious, and also how it follows you around on the internet, the Amazon ads you get when you have looked at a DVD or something. Yeah so this is different from what I said before – am I contradicting myself? I mean, there you have it right there. But it is one of those rare

> moments where you go ah ok. Like as I said before, you can see how you are being traced, but that's an exception."

James's story stands out through his persistence of not speaking about what he cannot see. But it also vividly illustrates, in a single account, a common relationship between visibility and knowledge of surveillance among participants. They consider visibility as both a mode of perception and understanding, whose scarcity in a world of computation is complicating and limiting knowledge of surveillance. While James was initially confused how to accommodate *Amazon* into his narrative, his story also stands exemplary for how people's encounters with surveillance are structured between a default of invisibility and particular instances of visibility.

Giddens' (1991) distinction between 'discursive' and 'practical' consciousness illustrates this further. Practical consciousness is a background modality that accompanies everyday life unobtrusively, just like James's statement that online surveillance is 'in the back of your head most of the time'. Implicit and taken for granted, it is free from interfering with or disrupting everyday acts. Yet once surveillance becomes visible, like in the *Amazon* case, it turns into directed, focal attention where participants problematise and negotiate their own position to surveillance and generate specific insights into its workings. To stay with the *Amazon* example, here is how Luise from Germany narrates her experience with surveillance that suddenly became visible:

[6, 11] "Some recommendations, I always think whoa crazy, all the things they know about me, and then they can conclude so many things, that is quite heavy. And you always realise it again in these situations." [DK: translation from German]

For Luise, *Amazon* is not covert about its surveillance practices. Instead, the online retailer lays them out in front of her every time she visits the *Amazon* website. Its purchase recommendations are a continuous reminder for Luise, both *that* her every click on the website is being monitored and *how* – through an analysis of her consumption and clicking habits.

Participants identify a set of contexts where surveillance appears time and again. Alongside *Amazon*, they repeatedly reference the advertising industry, which people think reveals its own logic of surveillance. For instance, another participant from London, 22-year-old Adam, said:

[6, 12] "Like, I wanted to buy a pair of sneakers, and suddenly there were sneaker ads wherever I went. So I thought 'here we go again', someone has been spying on me. It's kind of in

> your face, actually – 'hey look, I know you wanted to buy these sneakers, so I will follow you pester you until you get them'. It's not very subtle, to be honest."

But these contexts are far and few between. As Adam's phrase 'here we go again' insinuates, revelations of surveillance through advertising or *Amazon* are mundane and routine. They reoccur in the ever-same contexts, but participants provide few stories of such systematic revelations in other environments. This also means that visible instances of surveillance often reconfirm, rather than foster additional knowledge because, after a while, they do not shed light on new ways in which surveillance works. Luise followed up on her remarks about *Amazon*:

> [6, 13] "Well, I am not sure I can say how much I really know about surveillance. I mean, there is the Amazon case that we talked about, but what do I know apart from that? And yes I know that Amazon targets me, and that is crass, but if you have seen it 100 times you don't really feel shocked anymore I would say." [DK: translation from German]

At large, the domain of online surveillance then remains invisible like James has emphasised. Participants consider knowledge of computational surveillance as intertwined with their ability to perceive computational agents with their human senses. For instance, after I had finished a think aloud protocol with Luise, she opened her web browser to show me her privacy settings. Immediately, a website which she had selected as her default page, opened. I asked her whether she was being monitored right now:

> [6, 14] "Whether I am being monitored right now or now? No idea. Well, I don't see that sort of thing, but that does not say anything at all because it could be there nevertheless. But to reflect on it concretely is difficult because there is no evidence." [DK: translation from German]

The lack of visual anchors affects participants' construction of knowledge about computational surveillance. Its pervasive invisibility even goes so far that people struggle to find a language to describe computational agents. Previously, I introduced Italian artist Constanza who confidently speaks of 'algorithms' and 'data'. But other participants fail to find suitable vocabulary. They pause to find the right terms, stop and restart their sentences, use their hands and gestures in attempts to capture and express computational agents. My interview with Luise did not seem to progress well when I asked her to describe how surveillance works. She tried to come up with an answer, but paused several times, before finally replying:

> [6, 15] "Well yes I also don't know how to describe surveillance on the internet really now that you are asking. A lot of what's happening, it's not really noticeable. You feel kind of excluded and don't really know how to express it. You could be surveilled right now, but also not. And you don't know by whom because as I said it is not visible. They always say

> you are being watched, and that probably is also true. But where and how exactly, that is not clear most of the time. On Facebook, you know that you are being watched in general, and Mark Zuckerberg is always criticised in the media because of that. But you don't know the specifics. You are as I said somehow powerless." [DK: translation from German]

The systematic invisibility of computational surveillance then not only curtails people's amount of knowledge but also affects the process of constructing knowledge itself by limiting ways to think about and express computational principles in language.

6.1.3. Synthesis: A Default of Improbability

The above discussions have illustrated that people are faced with two dichotomies which structure their construction of knowledge about computational surveillance. The first of these dichotomies is expressed in a clash between a human and a computational logic. A computational logic is underpinned by generative rules, which are rational and reflexive. But people struggle to systematically adopt a rational and reflexive paradigm in their everyday life to keep up with those generative rules. The second dichotomy is that of visibility and invisibility. Computational surveillance lacks phenomenal anchor points that transport it into the realm of human experience. For participants, the ability to see stands metaphorically for access to the world through their human senses. They relate their sensory experience to the ability to frame, define and understand computational surveillance. Together, these dichotomies define conditions of possibility in which constructing knowledge about surveillance takes place. For analytical reasons, I presented those dichotomies as separate points. But they are also interconnected. Generative rules are hidden from view. This means that the invisibility of computational surveillance forecloses a better understanding of the specific rational and reflexive modus operandi of computation. While people acknowledge and experience the computational rendition of reality (Kallinikos 2009), it then coincides with the experience of improbability of access to its underlying modes of making sense of and structuring the social world.

These dichotomies do not claim to describe exhaustively how people construct knowledge about computational surveillance. The remainder of this chapter will add further observations, and I will present a social perspective in the next chapter. Instead, these dichotomies represent much broader groundwork. As conditions of possibility, they form a baseline, a default that stands in the way of constructing knowledge of computational surveillance. Either explicitly or implicitly, all other attempts of constructing knowledge are positioned towards overcoming the limits imposed on

participants through the rational and reflexive nature of computation, and its invisibility. This extends from knowledge to practice. In the last empirical chapter, I will discuss how people act towards computational surveillance in order to negotiate how they are being computed, where the conditions of possibility outlined here further will inform an interactional framework based on Goffman (1971).

6.2. The Technological Promise

Generating knowledge about surveillance is riddled with complex obstacles. This section discusses how people try to overcome the conditions of possibility that constrain their access and understanding of computational surveillance. It is the first of two sections which take on this perspective. Here, I look at the technological fixes that people employ in lieu of their own abilities. The next section addresses ways through which people try to reconstruct the ability to generate knowledge about computational agents through their own human logic.

6.2.1. Exosomatic Organs

Karen struggles to stay on top of surveillance on *Facebook*, be it in the form of a third-party application like *Farmville* scraping her data, *Facebook* monitoring her clicks and 'likes', or friends turning into unwanted spectators. Yet she does not dismiss *Facebook* as a mere data collection machine, where membership is a Faustian bargain of social connection traded for personal information that leaves her trapped in a surveillance web. As much as *Facebook* is a source of surveillance, Karen also draws on it to manage the gaze of computational agents that surround her. During our interview, Karen clicked on her *Facebook* privacy settings and pointed her finger at the computer screen:

[6, 16] "I have ticked the boxes, here, here, and here so I don't have watch out all the time, and Facebook does it for me, like what data about me Farmville and all the other apps can get. You have to tick the boxes because you obviously need to change the default settings. Maybe I check again when Facebook has changed. But I really don't need to think about it all the time, and that's pretty good."

Karen knows that *Facebook* continues to monitor and gather data about her no matter which privacy settings she applies. Instead, she rather uses privacy settings to stay on top of those surveillance threats that can be influenced. Karen applies a visual metaphor, 'watching out', to a software interface. She delegates a task to for which she would otherwise need both her eyes and a particular cognitive state of heightened attention.

Conceptually speaking, *Facebook*'s privacy settings turn into an exosomatic organ, an artificial sense (Innis 1984). Usually, exosomatic organs are prostheses that augment and expand the range of human senses. They enhance already existing human abilities such as seeing or hearing. But participants' use of software settings and tools also operate entirely in lieu of human senses. Further to Karen's story, Enrico suggests:

[6, 17] "I don't know what Facebook does with my data. Well, on the newsfeed and such, but not how that is shared and what is happening in the background. Yes, you do feel powerless because you just cannot watch out, because you do not see these things. But privacy settings are good because they control that in the background. There you still have the feeling that you can influence things." [DK: translation from German]

Enrico acknowledges a divide between interface and infrastructure that determines his grasp of surveillance. He is limited to the interface of the screen, where information is displayed in a form that he can cognitively process and understand. The interface provides some clues about how surveillance works. Changes in personalisation, such as in the newsfeed, allow Enrico to spot some modulations of surveillance. These are visual references to the underlying surveillance logic. But at the same time, the expressions on the interface signal the existence of a much deeper world of surveillance on the level of infrastructure that he cannot stay on top of. Privacy settings as exosomatic organs establish a connection to this hidden layer. But Enrico also makes clear that this connection is not immediate. His access to the realm of intangible surveillance is only by proxy. Once set up and configured, privacy settings operate independently and without his further contribution. While they stay vigilant on his behalf, they do not relay the world of surveillance directly back to him so that he can watch out for himself.

Exosomatic organs extend beyond privacy settings. Evelyn uses a program that prevents data to be collected for targeted advertising:

[6, 18] "I do have an ad blocker running, TrackMeNot, there you don't have to constantly think "uuuh, what is happening now with my data now that I am on website XY?" [DK: translation from German]

The program, *TrackMeNot*, is vigilant on Evelyn' behalf, no matter whether she accesses a news website or is surfing on a social network. In this sense, it goes beyond the scope of *Facebook* privacy settings. But it is limited at the same time – it only replaces her own grasp on surveillance with regards to targeted advertising. Other instances of surveillance are not considered. Compared to this, James, a technophile, has opted for a more radical approach:

[6, 19] "I have like anti-virus, anti-phishing, ad block, and also some other tools, like against cookies. I mean it's amazing the stuff you can get for free. So as I said, I kinda have my filters running all the time so I don't have to look out for nasty stuff all the time."

Without technological support, James suspects he would have to be on guard permanently. But exosomatic organs take over this task on his behalf. He has constructed a system of exosomatic organs spanning across as many internet activities and addressing as many surveillance intrusions as possible. James's assemblage is an extreme example that is not widespread among participants. However, it encapsulates the vast array of exosomatic organs, be it one or the other, that participants rely on beyond mere privacy settings.

The notion of exosomatic organs illustrates how participants are trying come to terms with the invisible nature of surveillance and the dilemma of perfect vigilance. As they cannot systematically convert invisible surveillance into their sphere of perception and understanding, participants draw on software to keep track of surveillance around them. Participants automate vigilance of surveillance by translating it from a human into a machine task. Freed from the limitations of human abilities, this delegated watchfulness also becomes a continuous watchfulness. Software never sleeps and operates autonomously without further contribution by participants.

6.2.2. Seeing Through Software

People's use of exosomatic organs sparks wider questions around the relationship between computation, the visible world and ultimately the production of knowledge. Considering that exosomatic organs operate autonomously in a realm that is inaccessible to human senses, it begs the question how they structure people's relationship to this invisible world, and whether they help at all in making surveillance appear to participants directly.

Bashir, a medicine student, is sceptical about the ability to grasp surveillance on the internet. Although he uses privacy settings from *Facebook* to web browsers, it remains 'all pretty unclear'. For him, human agents are barred from understanding a computational logic:

[6, 20] "It's all technology, so your only chance is to respond with technology because as an average person, you just don't get this stuff at all […] I kinda know, or hope at least that it works, um… that the privacy settings work, and that's that. What's really going on, I don't know."

This statement sheds further light on Bashir's relationship towards the use of software. As surveillance takes place in the domain of technology, so too does it have to be approached in and through technology. Exosomatic organs remain confined to the technological arena and do not cast open a door into the world of computation. Access to the domain of computation, remains foreclosed.

A term frequently used by participants in this context is the notion of an imaginary 'wall'. For instance, when Dennis from Germany walked me through his *Facebook* privacy settings, he concluded:

[6, 21] "So, I select something there, tick the boxes and that's that. What is happening exactly – no clue. That's like a wall to be honest." [DK: translation from German]

Dennis never sees, hears or otherwise perceives how the software tools he uses engage with surveillance. For him, a divide between interface and infrastructure cannot be overcome. The world of human experience stops on the interface.

Most participants either directly or indirectly affirm the experience of a wall between human experience on the interface, and underlying processes on the infrastructure level. Browser settings and other tools may display certain categories of threats, but they do not shed light on the actual workings of surveillance. When Stuart talked about his privacy settings, he was unable to tell more about what they actually do:

[6, 22] "I can't really see from this what these settings actually do. And to be honest, they also don't really tell you much. More privacy is better I guess, so I selected everything and clicked no, no, no. Here, here and here."

For Stuart, there is not much to infer about the way surveillance operates from the choices that software settings present. They allude to the powerful world of computation underneath the interface, but interfaces themselves remain vague and do not offer a feedback loop. What happens in the realm of infrastructure remains hidden from view.

Instead of being able to 'see' with the help of exosomatic organs, they act as substitutes for participants' human senses and do not open the world of computation to human experience. This has further implications for the production of knowledge about surveillance. As privacy settings and other software tools operate in the background, participants do not consider them as a source of knowledge about surveillance. Instead, attention shifts to exosomatic organs as objects of knowledge themselves. Asked if he

knows more about how surveillance works by using privacy settings and ad blockers, Martin says:

[6, 23] "Well not really. I think today you can rather know which tools you have to use. It is like with Google and Wikipedia I think. They always say, you only need to know where to find things, you do not have to know about ityourself. The tools I use, I don't expect that."

Martin's statement is epitomised by the proverb 'there is an app for that', or what Morozov (2013a) has called 'solutionism'. The phrase hints at a virtualisation of competencies through technology. In contrast to for instance print books finding a digital equivalent in eBooks, where the human ability to read is still necessary, a virtualisation of competencies means that any task-related knowledge, skill and expertise now resides in technology itself. Human agents are merely required to know how to find the right technological fix. Privacy settings and other exosomatic organs represent such a virtualisation of skills.

6.2.3. Doubts of Delegation

Despite the use of technological tools, participants have not abandoned efforts to generate knowledge about computational agents themselves. Consider again Karen's statement, which I referenced in the previous section:

[as 6, 16] "I have ticked the boxes, here, here, and here so I don't have watch out all the time, and Facebook does it for me. I mean, you have to tick the boxes because you obviously need to change the default settings because you have to know what you want. Maybe I check again when Facebook has changed, but I really don't need to think about it all the time, and that's pretty good I guess."

A close reading suggests that she shifts her attention to a meta-level, reviewing the privacy settings time and again. These review instances are not arbitrary, but follow changes in *Facebook*'s privacy policy which Karen keeps track of. Like Karen, many participants have doubts over uncritically delegating vigilance to software tools. Evelyn, who uses ad blockers to watch out for her, underscores that the technologies she uses cannot replace her personal reflection on surveillance:

[6, 24] "Yes, I know very well that an ad blocker cannot solve everything and for instance, on Facebook, it also does not work at all and with Farmville, which everyone seems to be playing now, this is also accessing my data and cannot be blocked. […] You cannot lean back and say 'now I don't have to bother with this anymore'." [DK: translation from German]

Such concerns are joined by critical voices about the clarity with which software is able to 'see'. Josephine, the textile design student, highlights:

[6, 25] "It is kinds of perverse to be honest. Facebook is spying on you but also gives the tools to protect your data. But it is clear that those tools are not as good as Facebook's capability to spy on you." [DK: translation from German]

While many believe that they can only systematically keep tabs on surveillance through the use of software, this reliance on a computational entity sits uneasily with participants.

As conversations about such tools progressed, many were worried that their tools are themselves opaque and inaccessible to human scrutiny. For instance, Bashir does not trust all software that claims to protect him:

[6, 26] "Like when it is Norton, it is a brand; you trust it. But privacy settings on Facebook it more like a placebo and now there is a ton of software out there that maybe you read about or that a friend has recommended or that is pre-installed, but then you sometimes wonder if it's not a bit dodgy, like when you use it that it spies on you also, there are these stories about that, but how to you verify that? It is better if you keep your eyes open as well."

Others are concerned about differences in power between software that monitors surveillance on their behalf, and the computational agents that monitor them. James initially seemed proud when he presented his elaborate system of technological sensors. But his faith in technology started to bear fissures and cracks as our conversation progressed.

[6, 27] "[…] as I said probably everyone collects your data. Everyone does it. But I mean Google and Facebook they have the smartest programmers so really what your freeware can do is probably not on the same level. And then, […] you are fucked anyways."

Enthusiasm and deflated feelings about software often coincide. During their biographies of coming to terms with online surveillance, people realise that technological fixes cannot replace the need for knowledge of their own. Attitudes to software tools also are unstable, changing between connotations of a fix-all solution to critical tones within a single conversation, pointing towards a troubled and conflicted relationship. Available tools are too narrow and distrusted, and participants see them as inferior to the surveillance technologies that online giants like *Google* and *Facebook* deploy. Participants' binary distinction between a human logic on one side and a computational logic on the other then gains an additional dimension. Technologies are not created equal. Far from a monolithic category, people see a hierarchy of computational logics. Power does not merely reside in computation per se, but in the technology of the others - the surveillors. Classic connotations of power between watchers and watched therefore are reproduced on top of a binary between human and computational powers.

6.2.4. Synthesis: A Broken Promise

In a computed world, where the ability to understand surveillance is constrained, people draw on technological tools in a bid to 'fix' the relationship between their human abilities to make sense of the world and its computational co-constitution. Relying on such tools is a first indication that people recognise the erosion of common-sense knowledge and experience the emergence of 'discrepant worlds' (Berger & Luckmann [1966] 1991) through computation. Resorting to technological fixes highlights that given the inaccessibility of these discrepant worlds, people strive to move the intersubjective negotiation of common-sense into those worlds by proxy. But these technologies do not systematically open up the world of computation to participants, resulting in a situation where the need for knowledge about surveillance is merely outsourced. Paradoxically, as people draw on technological tools to pitch computation acting on their behalf against computation that represents surveillance, they realise the limits of technological solutionism and become aware that their own, human logic remains a vital component in constructing knowledge about computational surveillance. This resurgence of the human senses is the theme of the next section.

6.3. Appearances of Computation

Beyond outsourcing knowledge of surveillance to technology, participants themselves also attempt to reconstruct their own ability to understand computational surveillance. This section documents how surveillance that is usually hidden from view reappears on the interface of the screen and becomes open to human understanding. It draws on Marks' (2010) concept of 'unfolding' to illustrate this. The section begins by documenting how people experience unfolding events that they are confronted with serendipitously and proceeds to show how people provoke unfolding events themselves.

6.3.1. Unfolding Events

Mike from London usually spends his lunch breaks at work watching videos of funny mishaps on *YouTube*. Sometimes, these videos have been flagged as offensive by other users, which means that Mike cannot watch them without logging to *YouTube* with his user account. Some time ago, Mike had just clicked on an age-restricted video like so many times before, as he was suddenly diverted to a webpage that prompted him to connect his *YouTube* and *Gmail* user accounts. He was bewildered. Reflecting on this incidents, Mike said:

[6, 28] "And there was YouTube, and Gmail and an arrow between them […] That was so obvious that they did that to get into my Gmail, because you know I am there with my real name and all the people that I am in touch with over email, it's also their real names…but that's got nothing to do with YouTube and Google? I mean I am gonna watch that video, and that worked before so that's what I don't…I mean why do they need to know who I am? So it's so obvious that that's really fishy. They kind of lure you into that because they think, ok you are gonna really want to watch that video, creepy."

Mike did not know that *Gmail* and *YouTube* both belonged to *Google*, which had decided to merge its user account across different web properties. His everyday experience was unexpectedly disrupted when a previously unknown configuration of surveillance unravelled in front of his eyes. The workings of surveillance became tangible through an image containing the logos of both *Google* and *YouTube*, connected by the shape of an arrow between them. Lyon (2007) uses the term 'leaky containers' to describe what Mike witnessed: the merging of formerly distinct databases containing personal information. Whereas this usually happens by re-routing flows of data, ungraspable by the human senses and confined to the expert knowledge of technicians, marketers or policymakers involved, Mike encountered a visual representation. He did not have to conduct any research on surveillance, probe into any inconsistencies or contradictions he encountered during his internet use or exhibit a particularly heightened vigilance towards surveillance in order to detect it. Instead, the computational logic behind surveillance revealed itself in its intentions through an image. For Mike, this was sufficient to deduce the underlying motivation: a computational agent wanted to acquire his consent for merging and exploiting his personal data.

Mike is not alone. Many German participants are avid readers of online newspaper *bild.de*. During the time of my interviews, the newspaper introduced a feature that allows users to comment on news articles using their *Facebook* account. A plug-in on the website at the bottom of each article displays how many people have already shared it and contains a timeline that imports *Facebook* recommendations and comments, including names and profile pictures. When people add their comments to the news article, it would also automatically be recorded on their *Facebook*. For participants like Andre, this was a new manifestation of surveillance:

[6, 29] "[…] and I thought, cool, that's nice. You can post the article directly on Facebook and don't need to write a new comment first. But wow, then I saw that it can be seen everywhere and that anyone reading Bild knows it then. Then I thought 'wow', that's pretty intense, maybe I shouldn't do it then." [DK: translation from German]

Both Mike and Andre could make inferences about the workings of surveillance through a visual representation of a computational logic. In both cases, surveillance required the complicity of human agents to operate and revealed its motivations in this process. Hidden on the level of infrastructure, surveillance is usually enfolded. By creating an image of itself, it unfolded into the domain of human experience. As Marks (2010) has shown, unfolding can either be triggered by human agents, or through the interior logic of computation. In these examples, unfolding was driven by the computational logic itself.

Such unfolding incidents are different from participants' routine encounters with *Amazon*'s recommendation engines and other mundane appearances of surveillance, as one participant summarises:

[6, 30] "Yeah it's difficult to really figure out how it all works. I mean yes, *Amazon* and stuff and also maybe the whole targeted ads thing, you kinda know, and it does not surprise you. Like you see it and its 'ah ok, here we go again'. You know it and you just expect it. But then sometimes you figure out that you are being tracked in a way that you did not think of, and that is really eye-opening then."

Routine encounters with surveillance already are part of people's repertoire of knowledge and reconfirm their understanding of computational surveillance. While people may see surveillance as a risk, routine encounters provide certainty that they still know, at least in part, how surveillance operates. In contrast, unfolding events create uncertainty because they remind people how little they know, and how vast and complex the web of surveillance is. The next section explores the unease that unfolding events create in more detail.

6.3.2. Unfolding Events and Uncertainty

Unfolding events unexpectedly foreground issues of surveillance into consciousness. Whereas routine encounters with surveillance such as *Amazon* recommendations are part of a stable experiential horizon that lacks news value, unfolding events unveil previously unknown instances, aspects, or processes of computational surveillance. Rebecca's experience, who also observed the integration between newspaper *Bild* and *Facebook*, stands for the feeling of surprise and shock that participants regularly report. The student who had moved to Erfurt earlier in the year, said:

[6, 31] "My jaw dropped. Really crass. You don't suspect a thing and then bang – you realise you are being monitored, everything is controlled and maybe has been all the time…and

> you had zero idea and suddenly realise 'this is how it works'. I do not have the technical know-how, but just like this, it is eye-opening, I'd say." [DK: translation from German]

Similarly, when Anna from Erfurt reflected on the same incident, she highlighted a sense of disillusionment:

> [6, 32] "The facade has collapsed so to speak." [DK: translation from German]

Both Rebecca and Anna were unprepared. They did not expect an ordinary situation to turn into an encounter with surveillance. Based on attitudes, beliefs and everyday practices, they had a set of fixed, sedimented expectations associated with the *Bild* website. I call these 'contextual expectations'. Surveillance was not part of them. Through an unfolding event, their contextual expectations collapsed as reality suddenly emerged as more layered and complex than they had assumed.

Participants struggle to deal with these revisions of reality, as Ian from London expresses:

> [6, 33] "[…] actually, sometimes you run into a situation where you think, fuck, I did not see that coming. And that kinda fucks you up a bit. Like especially where you don't expect it. I mean, that some dodgy site tracks you, ok, but when I then went to the Guardian, I saw they had the same ads. So I was, 'oh come on', I thought that well, a more, how to say, 'quality' newspaper does not do that. But that's it nowadays; I guess they all need money probably, so you cannot expect any higher principles. But still…it's not the same, like I am not sure if this sounds stupid, but I was disappointed in a way."

Ian's account reflects a deep sense of uncertainty. In his interview, he portrayed himself as computer literate and proficiently spoke about surveillance risks. But he admits that his own confidence is undermined when surveillance emerges in unanticipated ways and contexts, exposing the fallibility of individual assumptions and calling into question personal judgement. James, whom I introduced earlier, adds to this sense of betrayed expectations. He feels like living in

> [6, 34] "[…] a constant beta"

where certainties about how surveillance operates are only temporal, incomplete and fallible. Martin adds to this. As unfolding incidents occur time and again, he feels that his confidence in his own knowledge is being undermined. He cannot trust himself:

> [6, 35] "I have come to think that I know quite a lot and that I can see the dangers pretty well. But once in a while, there is a moment where you realise ok now I realised this. But this also means that I knew less than I thought."

These accounts echo a language of risk society and late modernity. They erode fragile certainties and transform knowledge about computational surveillance into a reality 'until

further notice' (Beck 1992; Giddens 1991) that can change, or entirely collapse at any time.

6.3.3. Unfolding New Understanding

Despite the uncertainty generated by unfolding events, participants welcome them as rare, direct connections between human senses and the world of computation. Time and again, participants highlight how unfolding events foster knowledge about surveillance that is otherwise not available. Paula was another German participant who noticed the use of a *Facebook* plugin on a newspaper website and remarked:

> [6, 36] "You see directly where you are at, you realise how they really implement it. It is just much more concrete than the usual waffle that you are being tracked on the internet." [DK: translation from German]

Unfolding events convert an abstract awareness about surveillance into a direct, tangible experience.

Often, surveillance reveals itself through these unfolding events in ways that could not be anticipated. Ann-Kathrin remarks:

> [6, 37] "As in the case of the Bild story, you always learn something. I mean, I could not have figured out how this works, as a normal person. And that it happens in the first place. You need to see it with your own eyes. In that sense – yes, I would say really not good what's happening there and also shocking, but then again also good because you then know, what is going on there and probably also elsewhere. In that sense, I learned something again." [DK: translation from German]

Ann-Kathrin, who references the same incident as Paula, highlights the value of individual, direct experience of surveillance as a source of knowledge. Her language illustrates that a divide between 'normal' people or lay actors, and those agents responsible for surveillance, is suspended through unfolding events. She adopts a visual language that references the importance of human senses in perceiving and understanding surveillance, and specifically her personal experience through her own human senses. This emphasises the personal experience as a source of knowledge of surveillance in the context of exosomatic organs, but also towards explainers stemming from public discourse. Her statement also reflects the contradictory nature of unfolding events characterised by the dual process of knowledge erosion and knowledge accumulation.

Also Mike found merits in the shock that *Gmail* and *YouTube* were jointly spying on him. Following his story, we talked about the personal consequences he drew from that particular incident:

[6, 38] "It was a complete surprise really. But then I thought, it is not so bad really. Um, I mean, they would have sold my data anyways probably, so I guess I was lucky in a way that they made it so obvious you know. It was right there for everyone to see what they are up to. You didn't need read about it somewhere, like 'Facebook scandal', or this is in the news also. It was right there when I logged on."

In our conversations, many participants acknowledged that talk about surveillance is part of public discourse, but feel that they learn more about how surveillance operates when they experience it directly. Although Paula, Ann-Kathrin and Mike are critical of surveillance, they favour actually experiencing the process of surveillance over it going on unnoticed. Since they cannot escape surveillance, feeling its gaze is preferable to an abstract paranoia. Such a view on surveillance is very different from surveillance portrayed for instance in Foucault's panopticon where the process itself constrains and limits people through coercion. Here, being under the gaze itself, not just its consequences, is a negative experience. In post-disciplinary, computational surveillance, the very absence of experienced exposure obstructs knowledge about surveillance and contributes to its negative perception.

6.3.4. Limits of Unfolding

Knowledge gained through unfolding events is bittersweet. It does not happen on participants' own terms but is dictated by the pattern of unfolding itself. Like others, Simona has experienced instances of unfolding. Simona is a 26-year-old business analyst based in London, who recounted how she participated in a wine tasting event that her company was hosting for clients. As part of the event, participants were supposed to guess the price of the wines tasted. Simona wanted to cheat a little:

[6, 39] "So I googled it. Just type in the name of the bottle and a couple websites came up. But when I clicked it, there was this popup, or like block from Vodafone. You don't have access; please call this and this number to verify your age."

For Simona the conclusion was apparent – Vodafone was tracking her entire mobile web traffic. The company's monitoring was sophisticated enough to determine that Simona was on an alcohol-related website. Probed about whether she thinks this event helped her to be more proficient about surveillance risks, Simona resumed:

[6, 40] "So yeah, this is how I figured out I was being tracked all along probably. But to answer your question, do I think I know more about this stuff now? Well, not really. I mean I just happened to be in a situation where I was looking for wine. I'm not a wine drinker generally, so the chances...the chances, like the likelihood, I mean I normally would never have found out!"

Ann-Kathrin, who merits the knowledge gained through the *Bild* incident, is also worried that she is dependent on the forces of surveillance unveiling themselves. After she had discussed how she stumbled across the *Bild* incident, we talked about whether she finds such moments useful in learning more about surveillance in her daily life:

[6, 41] "I would also say, it is difficult to influence what will be uncovered and how. And if it will be uncovered at all. In that sense, I would not rely on it." [DK: translation from German]

Unfolding incidents are neither finite nor structured, but piecemeal and haphazard. They are inserted serendipitously in participants' experience of everyday life and do not form part of a linear trajectory towards a more comprehensive understanding of surveillance. Which instances, or in which contexts surveillance is unfolded, remains outside people's control at the mercy of computation itself. While unfolding events show that human agents can obtain access to the interior logic of computation in principle, they are merely scraps of evidence.

Unfolding incidents also have to be recognised as such. During the fieldwork for this study, eight participants did not broach the issue of unfolding at all. During my fieldwork in Germany, after the interview was formally concluded, some participants were keen to hear what others had said to compare their own experiences and assessments about living with surveillance. I asked two participants, which had not mentioned unfolding events, whether they had heard about the *Bild* and *Facebook* integration that so many others had referenced. Both declined although they were both *Facebook* users and readers of the online newspaper in question. I have argued above that unfolding events are commonly initiated through the interior logic of computation. But they only occur when the overspill of computational surveillance into specific human experience actually takes place. Unfolding is an interactive process that requires people to recognise, decode and interpret them. Knowledge about surveillance fostered through unfolding events hence does not systematically suspend a power differential between human and computational agents. Its logic of appearance – driven by computation - reaffirms a hierarchy of power in agenda setting between computational surveillance and human agents. As the ability to recognise

unfolding incidents varies between participants, they also create a hierarchy of power between different human agents.

6.3.5. Engineering Unfolding

The unfolding events described so far were chance encounters: unsystematic, unpredictable, and triggered by the logic of computation instead of human agents. Although unfolding events temporarily suspend divides between interface and infrastructure, their haphazard nature limits participants' ability to actively construct knowledge about computational surveillance. In this section, I demonstrate participants' attempts to reverse the dynamics of unfolding by making computational surveillance appear on their own terms.

Richard, a 24-year-old financial advisor from London, considers himself 'a bit of a geek'. In his passion for technology, he does not see his web browser as a static interface through which he accesses the internet, but as a tool that can be customised. For Richard, this applies particularly to *Mozilla Firefox*, his browser of choice. Richard is an avid user of plug-ins, sets of software components that add functionality to the browser. For him, plug-ins are a remedy for the daily nuisances of pop-up windows, surreptitious advertising and pervasive surveillance. During his interview, we had just completed a think-aloud protocol, Richard left the *LinkedIn* website on which he was dwelling and introduced *Ghostery*, his most cherished plug-in. He explained how *Ghostery* blocks a website from sending information about him to advertising companies. With a few clicks, Richard showed me what *Ghostery* was capable of: Whenever he accessed a new website, a pop-up window appeared, listing all those companies which are extracting his personal information from a particular website. Richard describes his discovery of *Ghostery* as revelatory:

> [6, 42] "At first I was really excited because I could see what was really going on. I mean there is a lot in the news and the whole privacy debate that is going on now but to be honest…I don't know. I kinda felt I only really got it with Ghostery. The news just go on about this, but here i's this company, this company, and you have the entire list. That's brilliant really. I didn't, umm don't necessarily know them, and I guess they are pretty much unknown to anyone. So I googled them, and they have websites and everything, like normal companies. I guess once you know about them, they are pretty open about what they do."

Richard's use of *Ghostery* is a practice of discovery in which exosomatic organs and unfolding conflate. In its basic function of keeping companies at bay, *Ghostery* substitutes for the human senses like exosomatic organs discussed previously. However, Richard

does not merely delegate vigilance to technological tools that act on his own behalf. He also uses *Ghostery* to systematically trigger unfolding events.

For Richard, *Ghostery* reveals computational surveillance in three ways. Firstly, it confirms and expands his awareness of the fact that websites send user information on to other parties. Thereby, it makes the data flows of the advertising and data-mining industries tangible. Secondly, it lists the names of institutional, computational actors previously hidden from access, giving anonymous computational agents that act on him a face. Lastly, the unfolding through *Ghostery* allows Richard to continue unmasking surveillance himself. Richard showed particular enthusiasm that with the help of *Ghostery*, he had discovered the websites of some of the companies behind online surveillance. He felt as if he was entering a hidden world:

[6, 43] "It was pretty freaky. Like not Google and the kind of companies you know, but unknown companies really. All neat websites and you could see that what they are doing was data mining, and they had charts where they showed like what people prefer to shop and stuff. I was really like woah."

However, while his use of *Ghostery* enabled Richard to take control of the process of unfolding, after an initial period of discovery and excitement, he disabled it:

[6, 44] "Seeing this pop-up all the time about who tracks you…it was just getting boring after a while. It was always the same companies and I kind of thought; I don't really gain anything from this. Like, don't get me wrong, I really think we all should learn more…know more about this whole privacy thing and how it works, but it was just getting annoying and not leading anywhere. So I just have it [DK: Ghostery] running in the background nowadays."

After a while, *Ghostery* was not leading to new discoveries, its ability to generate unfolding of surveillance had stalled. New discoveries had become mundane, and *Ghostery* did not allow him to further his knowledge about surveillance beyond its own technological affordances. Similarly, Josephine from Erfurt has *Norton*, an Anti-Virus software, installed on her computer. Her dad advised her to do so. This software acts like an exosomatic organ, keeping spyware at bay. But it also features a pop-up window that notifies Josephine whenever surveillance takes place, allowing her a glimpse into the mechanisms of computation. However, Josephine admitted that she intended to deactivate the pop-up window: after a while, it did not yield any meaningful insight and was just bothering her.

Software tools offer participants a systematic, albeit limited way of taking the unfolding of surveillance into their own hands. But they are not the only way. Everyday practice of

being online is interspersed with moments in which people try to tease out the logic of computation to the interface of their screen. Enrico sometimes stops catching up with his friends' lives on *Facebook* and directs his focus to *Facebook* itself in order to explore how it works. He clicks 'like' on random posts, repeatedly accesses a friend's profile and watches what happens. A few days later, he finds the results of his clicks: recommendations that link back to the posts he liked or a friend's profile he repeatedly accessed now featuring more prominently in his newsfeed than usual.

> [6, 45] "Mostly at night, like when I have nothing else to do, I just mess about a bit. It's just, I got this feeling how Facebook works and want to test it." [DK: translation from German]

Targeted clicks on the interface allow Enrico to infer how *Facebook* computes his inputs. While he admits that his approach is 'not perfect', acknowledging the complexity of computation, it casts a window into an otherwise alien world on his own initiative. Occasionally, he reads about changes to *Facebook*'s newsfeed and adjustments to its algorithm. Enrico struggled to explain what algorithms really are when I asked him, but he knows that they change how *Facebook* orders his experience. While he does not follow a rigid regime of immediately testing each change he that reads about, he uses these instances as opportunities to repeat his 'test'. They give him a sense of comfort. As he told me, to date, none of these apparent changes had altered the fundamental way that *Facebook* organises his experience – he still feels in touch with at least the basic premises that underpin *Facebook*'s logic.

Similar attempts feature in other participants' stories. Usually, people decide to probe into a computational logic based on a news story, or an unfolding incident that they previously encountered. For instance, Ann-Kathrin noticed that *Google* shows advertising next to its search results that do not relate to the particular search term she had just entered. She suspected that *Google* was getting information from her activities on other websites and wanted to put the search engine to the test. She surfed the web and after a while, returned to *Google*, entered a search term and monitored which ads came up. This way, she confirmed her suspicion that *Google* had been tracking her all along, not merely on its own website. Ann-Kathrin used a set of calculated acts to expose at least a part of *Google*'s modus operandi. Yet such investigative practices often are not standalone quests to further knowledge about surveillance. They are embedded in a more complex interactional relationship between human and computational actors. Specifically, they are a prerequisite for participants' practices of acting towards surveillance to influence

computational inferences about them. In these instances, participants take matters of unfolding into their own hands. Unfolding is part of establishing a social situation in Goffman's sense which allows participants' to define their interlocutors and anticipate their courses of action. The last empirical chapter in this thesis is dedicated to the structure of interaction and will shed light on this wider role of unfolding incidents in greater detail.

6.3.6. Synthesis: A Landscape of Unfolding

Unfolding events stand for the unlikely appearance of a computational logic in the domain of human experience on the interface of the screen. Conceptually, they are modulations in the cognisphere that Hayles (2006) has described, where human agents only have access to a fraction of the cognitive systems expressed through computational data flows. Participants encounter a range of different unfolding events, either triggered by the logic of computation or generated by themselves through software or targeted acts that tease out the computational logic. Unfolding events are ambiguous in their consequences. While they help to advance knowledge about computational surveillance, they also shatter established certainties and cause participants to revisit the status quo of their knowledge about the social world. Against the available conditions of possibility set by the ever-rational and reflexive nature of computation and its pervasive invisibility, people's attempts to understand computational agents can be considered as restorative acts. These are acts that seek to repair the ability to generate knowledge about computational surveillance and the social world it affects against all odds. In Berger and Luckmann's ([1966] 1991) parlance, through unfolding events, participants uncover discrepant worlds that are separate from the world of common-sense that is shared between human agents. These discrepant worlds become – at least in part and for a moment in time – tangible and open to scrutiny. Bringing together Berger and Luckmann's concepts with the notion of computed sociality (Kallinikos & Tempini 2014) and Alaimo's (2014) work on the reassembling of consumers shows empirically that through such unfolding events participants are presented with a reality that they may have been complicit in creating, for instance through 'likes' on SNS or Amazon purchases, but which they were not aware had congealed into institutionalised social facts. Such acts of unfolding are not an end in itself. As narratives about engineering unfolding have demonstrated, knowledge about surveillance is a precondition for the ability to renegotiate meaning within computed sociality. Knowledge about computational agents

through restorative acts thus are embedded in, and enable wider relations between human and computational agents.

6.4. Chapter Conclusion

This chapter had two objectives. In a first step, it documented the general conditions under which the construction of knowledge about computational surveillance takes place. It then secondly explored specific modes of generating knowledge under these conditions.

Living in a computed world coincides with the loss of acquiring systematic understanding about it. People realise that a computational logic constructs meaning, also on the basis of their acts, but outside of their symbolic universe. This changes the foundations for the social construction of reality that Berger and Luckmann ([1966] 1991) have articulated. It also demonstrates that the computational rendition of reality (Kallinikos 2009) is not an abstract concept, but that at least its existence is part of the experiential world. In everyday experience, people get reminded that the rules and mechanisms by which computation operates differ from their own ways and abilities of making sense of the world. Awareness about the computational rendition of reality also permits people to make inferences about it. They portray computational agents as rational and reflexive and impose the same principles upon themselves in order to keep up with computational occurrences and ways of working. At the same time, computation operates in an invisible domain, and people connect the ability to perceive a phenomenon through their human senses with the ability to understand it. These factors impinge on people's self-understanding as agents in control of the world around them. They demonstrate a divide between their inherent perceptual, cognitive and analytical capabilities on the one hand and the requirements of navigating a computed world on the other. This environment constitutes a default of conditions of possibility that problematises knowledge about computational surveillance, and against which further attempts to foster understanding are positioned.

Within these conditions of possibility, several modes of generating knowledge about surveillance nevertheless emerge. Feeling resigned about the lack of access to a computational logic, people outsource the need for knowledge to software tools. These tools do not enable them to perceive and understand surveillance, but operate autonomously in lieu of people themselves, eliminating the need for knowing about

surveillance. Yet serendipitously, computation surfaces by virtue of its own logic in unfolding events, where it lays bare aspects of its modus operandi on the interface of the screen. In order to reclaim control, people also look at ways to provoke, and tease out a computational logic – either through software or through manual interventions. Unfolding events are restorative acts that overcome the otherwise limited conditions of possibility. By restoring the ability to understand surveillance, people build a foundation for much a much wider set of relations with computational agents.

The themes discussed in this chapter have shown that knowledge about computational surveillance is fluid. In a general environment of metaphorical darkness, the contours and shadows of computational surveillance emerge every now and then, revealing a glimpse into its logic, confirming or dismantling existing knowledge in every new instance. Living in a computed world, people are in a perpetual state of coming to consciousness, where a succession of unfolding events reveals more information, momentarily sharpening people's senses, without changing the general feeling of being inadequate, lagging behind, chasing ephemeral computational agents. The next two chapters further elaborate on the themes established here. They document how participants amongst their peers collaboratively develop everyday practices that transcend the limits of unfolding experiences, and how they directly interact with computational agents to negotiate consensual interpretations of reality.

Chapter Seven: Collaborative Inquiries and the Troubled Nature of Common Sense

A pessimistic reading of the previous chapter may encourage a dystopian view of people in a computed world as lone agents deprived of systematic opportunities to reveal instances of computational surveillance, to obtain knowledge about its workings, purposes and consequences. Yet this chapter documents that people's encounters stand in a wider context that complicate and expand their relationship towards computational surveillance. People's experiences of such surveillance are firmly embedded in public interaction and routine part of the social construction of knowledge through which people intersubjectively make sense of the world. The chapter builds on and extends the narrative developed in the previous chapter. So far, this narrative has explored the limits and affordances of knowledge in a computed world – its conditions of possibility – and how people deal with these conditions. In order to carve out the basic conditions of knowledge construction, it conceptualised people as lone, individual agents. This had analytical reasons: people encounter computational surveillance on their screen, often in solitude, and it is their individual data that is being computed. The previous chapter focussed on the direct encounter with computational surveillance as it happens in a prototypical setting in front of the computer screen, in order to combine the immediate experience of computation with the domain of knowledge. The following analysis in this chapter adds a wider social context.

Drawing on Berger and Luckmann's ([1966] 1991) social construction of reality, this chapter argues that a collective inquiry into the workings of computational surveillance is already taking place. At the centre of the chapter are the concepts of objective reality and intersubjectivity. To reiterate, objective reality in Berger and Luckmann's sense stands for the undisputed conditions under which people live. It is the taken-for-granted world that appears set in stone, and natural. Society is a man-made product and thus always constructed. But the constructed character wanes over time as institutions solidify and become abstracted from the forces that created them. In the previous theoretical discussion in *Chapter Three*, I have reformulated Berger and Luckmann's framework. Specifically, I have argued that the rise of computation as a social force means that social order is not merely a human product, but co-constituted by computational forces, which operate in and through objective reality. People possess a common-sense knowledge

about the world, but this knowledge is increasingly under siege due to the obstacles in understanding computation. Based on this reformulation, this chapter explores how people construct and reconstruct common-sense knowledge about the computational aspects of objective reality. For Berger and Luckmann, common-sense knowledge is intersubjective because it is shared between and mutually constituted by people. This chapter hence places particular emphasis on the complexities of the intersubjective understanding of computational surveillance. By documenting the collective inquiry into computation through my reformulation of Berger and Luckmann, I extend the notion of computed sociality (Kallinikos & Tempini 2014). While sociality is rendered by computation, this chapter shows that parallel processes of social construction between human agents not only remain relevant, but change in light of computational dynamics. It also highlights that reflection on computation is a manifestation and integral part of computed sociality itself.

Throughout the chapter, I will make references to more detailed concepts from Berger and Luckmann's catalogue to illustrate how such common-sense knowledge operates in practice, and how its modalities differ from the pre-computational world that Berger and Luckmann have described. Instead of outlining these concepts at the outset of the chapter, I will introduce them progressively in my argument in order to closer embed them into the empirical experience narrated by participants. I will also return to concepts that I have introduced to augment and extend Berger and Luckmann's theory, such as the notion of mediatisation (Hepp 2013).

The chapter sets out by delineating a number of communicative arenas in which participants jointly probe into computational surveillance – news media, social networking sites (SNS) and face-to-face interaction. These arenas introduce the basic patterns of the social construction of knowledge. The next section problematises the construction of knowledge within these arenas. It outlines that common-sense knowledge about computational surveillance is inherently unstable, fragmented and does not translate into a coherent picture of reality, leading people to deploy tactics of querying and imagining a social consensus in which they feel safe to participate. The final section explores how people intersubjectively maintain knowledge about computational surveillance despite its instability, and how they create a sense of social coherence that nurtures and solidifies their view of computational reality.

7.1. Talking about Computational Surveillance

In Meckel's book *Next* (2011), the protagonist is a personified algorithm who lets the reader in on its personal view of the world and how it continuously enmeshes people into an algorithmic web of dependency. The algorithm narrates the story from the inside, a perspective that human agents struggle to obtain. Meckel chose a science-fiction format over an academic publication in order to reach a non-expert audience, arguing that the social consequences of computation are largely absent from the public agenda (Meckel, interviewed in Geyer & Haas 2011). Meckel's personified algorithm joins a growing body of popular literature devoted to uncovering the hidden mechanics of computation, such as *The Filter Bubble* (Pariser 2011) or *Super Crunchers* (Ayres 2007), whose promise to reveal what is usually invisible is already conveyed in their respective subtitles; *What the Internet Is Hiding From You* and *How Anything Can Be Predicted*. Surveillance has more widely long been a theme in popular culture (Lyon 2007), and Mathiesen (1997) proposes that analysing popular appearances of surveillance are a rough proxy to public knowledge. But the social thematisation of surveillance is much more widespread and, far from top-down, includes lateral interaction between people. This section outlines three communicative arenas in which the social construction of computational surveillance takes place: news media, social networking sites (SNS) and face-to-face interaction. I understand communicative arenas as conceptually delineated and generalisable domains in which participants are exposed to talk about surveillance, or routinely probe into surveillance through interaction with others. My interest is not in these arenas per se. Rather, by describing them through several of Berger and Luckmann's concepts, they help outline a basic structure of social knowledge construction about surveillance.

7.1.1. Surveillance in the News

Although Sarah, a 21-year-old German linguistics student, struggles to grasp surveillance, she is surrounded by its representations. Every day, she checks the news online and occasionally watches the 8 o'clock news. Mentions of surveillance are nearly as commonplace as political affairs, stock prices or sports results. Exposure to debating surveillance is not a choice but a necessary consequence of engaging, even passively, in the wider public sphere:

> [7, 01] "You read about it sort of every day now, in the media. There's always, like recently with StudiVZ, there's always a data scandal where someone stole some data. You kinda can't escape it these days." [DK: translation from German]

This abundance of information about surveillance is widely echoed by participants. Their stories usually open with expressions such as ‘every day’, or ‘nearly every time I check the news’ to underscore the frequency of media reports about surveillance. As if words were not enough to capture this omnipresence, Stefan, who attends university in a different city than Sarah, puts it onomatopoetically.

[7, 02] “It is really like bang bang bang nowadays, like a bombardment. There is always something.” [DK: translation from German]

Such media reports are not just reminders of the presence of surveillance or an inventory of its forms. Frequently, they offer interpretations and explanations of the inner workings of surveillance. Annegret, who studies with Sarah, recounts how the way *Google* operates is being unravelled in news media explainers:

[7, 03] “This one time, Google was in the news and it was mentioned again that they collect user data, and how that works if you have entered your information, how they store it and how it is used for advertising, although this is not the first time I had heard about it.” [DK: translation from German]

Consider also Dave again, the fitness coach from Erfurt. When we met at the gym’s bar, our conversation quickly steered towards *Google Street View*. Dave seemed to be intrigued by the thought of *Google* launching the service in Germany imminently and admitted that he followed the news closely. He pulled out his smartphone and while we talked, tried to search for new articles on *Google Street View* as if to underscore his excitement. Still, he admitted, many questions about *Street View* remained unanswered. Which cities were to be photographed next? What about his hometown, Erfurt? And how could people blur their private residences on *Google* once they had been photographed? The media offered Dave a glimpse into how *Google* operates:

[7, 04] “So recently I watched NDR and there was a documentary on about dangers on the internet, including Google Street View and pixelated houses. What was really good was that you then knew, I see, this is how it all works, this and this person has the data and they are being used in this way. […] This was not just about when Street View launches, but about background information, what as a normal guy, I would not necessarily know yet.” [DK: translation from German]

Dave experienced an instance of unfolding driven by public discourse. The media provided him with ‘behind the scenes’ access to surveillance and shed light on its otherwise imperceptible processes and aims.

Unfolding events demand a high cognitive effort for individual actors to be identified as such and for drawing appropriate conclusions. On the rare instances that they happen,

participants are left at their own device to discover and contextualise them. In contrast, the media provide a constant stream of facts about surveillance, converting unlikely into more common encounters. These instances of social unfolding take over the labour of discovery and offer ready-made interpretations of surveillance. Participants' personal and immediate experiences with surveillance are thus contextualised in a wider, more systematic body of knowledge that is socially constructed. Another participant, Lars from Germany, concludes:

[7, 05] "[…] I also think it's cool, I wouldn't be able to find out all of this by myself, what is going on there. In that sense it is really helpful actually. I check Spiegel and they write about what Facebook does with my data. Actually, if I think about it, most of the stuff I know about Facebook is not from the terms of use or so. That is so woolly and one does not read it. And it is pretty technical. So a large part I know is from the media, because it is such a huge topic nowadays." [DK: translation from German]

This topicality in the media that Lars describes is not confined to introspections into the workings of surveillance and templates for interpretation. Dave highlights:

[7, 06] "When I am on Bild or Spiegel.de, then you see an article or at least an advice box every couple of days, such as ‚Top 10 tricks to protect your profile', ‚How to protect yourself', and also on TV sometimes. Well I pretty much know all these tricks by now, but there could always be something new. I do tend to click in the end." [DK: translation from German]

Social unfolding events are joined by recommendations on how to act towards surveillance. While Dave just mentions what can be done, other participants put the media's advice to practice. When I met with Stefan, a biology student, I noticed pop-up windows and warnings that came up every time he loaded a new website. Stefan has a series of privacy tools installed on his computer, regularly clears his browser cache and revisits his *Facebook* privacy settings time and again. These are all suggestions he discovered in the media:

[7, 07] "They really hammer it in, also the media, you always get some kind of advice. And after a while, you know the rules […] you know what you are supposed to do." [DK: translation from German]

Stefan has internalised so-called 'recipe knowledge', defined as "pragmatic competence in routine performances" (Berger & Luckmann [1966] 1991: 56). These are shorthands for thinking about and acting towards surveillance which are produced and disseminated through the media. Stefan embraces these shorthands without much second thought. Just like everyday life is filled with manners, conventions and rules from the arrangement of cutlery at the dinner table over stopping at a red traffic light to following a netiquette in

online chat rooms, so does Stefan provide evidence that dealing with surveillance is normatively coded.

The media also open a social context about surveillance to participants. Frank stresses:

[7, 08] "Through this [DK: the media], you can see how the others see it and how you should see it yourself." [DK: translation from German]

For Frank, social unfolding directly connects to his personal encounters with surveillance. In his personal encounters, alone in front of his screen, Frank tried to interpret them and connect the dots. But his reasoning stood unverified. Through media stories on surveillance, Frank can infer what those around him know about surveillance. They allow him to assume a social consensus on how surveillance works and adjust his own interpretation. In his mind, what the media say about surveillance is socially endorsed. Once a fact has been published, a news report has been aired, he considers it as intersubjective consensus. While other participants do not accept media reports uncritically, such reports nevertheless serve as indicators for a potential social consensus against which participants assess their own experience. The media then convey modalities for thinking about and acting towards surveillance. Often, these are not suggestions for optional consideration, but express 'how things really are' and 'how it's done'. Books, like Meckel's personified algorithm, do not feature in participants' accounts. Instead, the media help shape people's knowledge about surveillance through a stream of news, small stories and revelations within the flow of everyday life.

7.1.2. Probing Surveillance in Social Media

Social networking sites (SNS) are considered amongst the most fervent collectors of personal information by participants, yet they also offer a forum for exchange and inquiry about surveillance. The social construction of knowledge on these sites is complex, and the following section distinguishes several modes through which participants engage in this communicative arena.

Collaborative Practices and Activism

Throughout their interviews, participants make reference to *Facebook* and *StudiVZ* as contexts where they discuss surveillance. In order to conceptually delineate SNS as a communicative arena versus the media, the experience of Luise from Germany provides a starting point. Her experience summarises core features of SNS as a communicative

arena that may otherwise only be grasped by looking at several examples in conjunction. At the same time, the formal group setting in which Luise's experience takes place is atypical for participants' experiences. Her example cautions against misconstruing surveillance talk in SNS as an expression of organised activism.

A while ago, Luise had joined a *Facebook* user group protesting against a looming change in *Facebook*'s privacy policy:

> [7, 09] "I think people were like 'yes, Facebook is selling your data', 'attention, fight back!', 'sign here and do this and do that because your data is being sold and don't play along anymore' and stuff. And over time, more and more stuff came together; one person said something and another one added something else." [DK: translation from German]

Luise witnessed a gradual process of constructing knowledge about *Facebook* through the input of many other *Facebook* users. Disparate hypotheses, ideas, suggestions and comments amassed and ultimately congealed into social consensus knowledge. Step by step, through input from various peers, her understanding of how surveillance operates extended and solidified:

> [7, 10] "It was actually really cool. You could really see how this was growing because everyone knew something and posted links and some were really knowledgeable and after a while it all came together. And as I said, everything on Facebook!" [DK: translation from German]

Luise's example highlights a fundamental characteristic of how knowledge about surveillance is constructed in the context of SNS, and this it differs from other mediatised debates. As an editorial environment, the media unveil processes, establish facts and offer interpretations of surveillance in a top-down way. Surveillance has already been analysed and contextualised. How others think about what the media say, whether they accept it as fact, or whether they have read or watched a news report about surveillance at all, is left for participants to speculate. In contrast, on SNS, knowledge of surveillance is peer-produced through collaborative practices (Berger & Luckmann [1966] 1991). It also is contingent on outcome – as Luise highlights, it was 'growing' over time.[38]

But as much as Luise's example allows grasping focal characteristics of constructing knowledge of surveillance within SNS, it also prompts investigating its organisational

[38] This is not to say that media representations of computational surveillance, such as news articles, are ignored in the social construction of knowledge. In examples that will follow, links to news articles and other media artefacts that are shared on social networks often initiate a process of debate and inquiry into surveillance. However, these form part of a wider intersubjective process of discovery, discussion and inquiry that is driven by respondents and their peers.

form. The group she had joined was an institutionalised environment comprising of strangers that systematically inquired into surveillance. The group pursued a clear aim: it was protesting against *Facebook*'s policy changes. Reports of such groups are widespread among German participants. But while nearly all of them have observed one of their *Facebook* or *StudiVZ* friends 'like' such a group, UK participants did not mention them at all. Anna from Erfurt spots a trend in her newsfeed:

[7, 11] "There are tons of these groups. In general, I think that people talk about privacy and surveillance a lot on Facebook. At least you get the impression because, well I have the impression that lately many have liked such groups, like 'Facebook, return our data' and stuff." [DK: translation from German]

Yet participants' practices of constructing knowledge are not expressions of media activism. Numerous scholars have highlighted, discussed or contended the role of SNS as platforms for political mobilisation and activism, for instance in light of the Arab Spring or the US elections. (Morozov 2011). Others have dismissed SNS as a breeding ground for superficial, dead-end activism. Indeed, Luise's behaviour could be considered 'slacktivism'; the ease with which people can associate in non-committal groups, or as 'clicktivism'; a fire-and-forget approach to activism where involvement in an issue begins and ends with a mouse click (Karpf 2010). Although participants find themselves in an everyday struggle with surveillance, they neither share a unified political stance towards surveillance nor are their acts - alone or in conjunction with others - decidedly political. There is no explicit, common political project for which they convene and cooperate, such as an "anti-corporate cyber-libertarian agenda" (Ritzer & Jurgenson 2010: 23).

Legitimising Inquiry

While most participants do not engage with such groups beyond a click or acknowledging their pervasive existence, these are neither cases of superficial activism, nor are they trivial. They form part of a wider setting, an atmosphere of inquiry, that legitimises SNS as an arena in which the workings of surveillance are queried. For instance, Anna finds talking about surveillance with her friends 'a bit geeky' and Paula considers it 'a bit too technical'. When Paula and I met for an interview over coffee, it was the first time that she was discussing this topic in the offline world. Yet on SNS, it is a different story. Paula says:

[7, 12] "Well it [DK: surveillance] is a topic that is being discussed more frequently. I don't know; maybe I would not post anything about like cars or something niche. But this [DK: surveillance] works. Yes, it is a topic, and you always see stuff about it on Facebook for

> instance if someone likes a post about the new privacy rules or so, this is why I would say: yes, you can talk about it." [DK: translation from German]

Facebook groups also document interaction between people on surveillance. The volume of posts and the number of members are clearly visible to anyone who visits the group page, assuring participants that talking about surveillance is a common activity. Yet, figuring out how surveillance exactly works usually does not take place in the confines of a formal group and associated 'likes', but elsewhere on SNS. Evidence can be found in participants' newsfeeds and profile pages. For instance, when Tim invited me to have a look at his *Facebook* newsfeed, one of his friends had previously posted a link to an article that explained how *Facebook* was 'stealing' users' personal data:

> [7, 13] "I guess he wants to tell us not to be too carefree - yeah, it's good to know these things nowadays, people sometimes post stuff like this. It is pretty… when you compare it with the other crap that people are posting, I don't know like so hung-over from last night… I rather read something like this because it actually is important in a way."

For Tim, this post was not unusual. He immediately contextualised and identified it as belonging to a wider, recurring theme of reminders and revelations of surveillance that pervade his newsfeed. Tim did not choose to inquire into how surveillance works at this particular moment in time. Although he finds the issue of surveillance important, he does not have a structured interest in probing into surveillance with a regular pattern. In his everyday life, inroads into the workings of surveillance emerge spontaneously as new artefacts on this *Facebook* newsfeed. These are not rare instances, random posts by cognoscenti users, who are 'in the know' about surveillance, but a recurring, familiar sight on the newsfeed by a diverse range of peers. Also Constanza, the Italian artist living in the UK, remembered that someone had shared an article on *Facebook*'s privacy settings not long ago. Eager to show me, she started scrolling through her newsfeed:

> [7, 14] "People post stuff about Facebook on… um…well…Facebook, it is funny really. So this is Rob, and he was the guy who posted this link a while ago, um let's see, is it still there? Yeah, Facebook does this and that and they don't let you control your data. That's basically what it says. There is always someone who shares something about that, so yeah, stuff like this regularly is in my newsfeed."

Like Constanza, participants regularly stumble across discussions about surveillance on their newsfeeds, making their presence as mundane as encountering a friend's pictures from a recent holiday.

Meaningful Reciprocity

In the examples so far, participants have observed how others inquire into surveillance. Yet, they also take an active role, be it by responding to what others have posted, or by initiating a conversation about surveillance. Dave, the gym instructor, had previously posted a news article about *Google Street View* on his *Facebook*. He had added a comment, claiming there was 'no escape' from surveillance. Similarly, a few weeks before we had conducted our interview, James, the barista from London whom I have already introduced in the previous chapter, had commented on a friend's *Facebook* post. His friend had shared a news article on data leaks. James excavated this post again during our interview:

[7, 15] "He wrote this here [DK: participant points towards friends' post] and I just said like I am being careful about what I share anyways."

Consider also Josephine again, the hairdresser and textile design student. She says about herself that she is 'more or less average in terms of computer skills'. In her newsfeed, she had posted a video entitled 'What facebook knows about you'.

Figure 4: 'What facebook knows about you' Video

Source: Screenshot from participant's Facebook account.

Josephine played the clip to me. It sheds light on *Facebook*'s data collection practices, visualises flows of personal data and explains what happen to all the collected user data.

Diagrams, lines, nodes and other symbols create a visual representation of the computational logic. Josephine chose to introduce her post with the statement ‘meine rede [sic]’, loosely translated as ‘as I keep telling you’. The video reflects what she had always suspected, but could not validate or express adequately.

It is worthwhile dwelling a little longer on Josephine’s story because it allows exploring the intersubjective process of figuring out how surveillance works in greater detail. By posting the video on *Facebook*, Josephine did not just make others aware of surveillance. She also validated her interpretation of surveillance through her peers’ approval. Indeed, when she showed me the video, her post had already received several ‘likes’. These ‘likes’ helped establish, or at least make explicit an intersubjective consensus. Josephine now had tangible evidence that her friends shared her views on how *Facebook* operates, and that her post was worthwhile and relevant:

[7, 16] “Well I mean, it is nothing special really, I did not make the video myself, it is more like ‘yes, confirmation that the message is correct maybe, cool video’, something like that.” [DK: translation from German]

Such feedback are acts of ‘meaningful reciprocity’ (Berger & Luckmann [1966] 1991) that consolidate knowledge between people. These acts may take other forms, such as a written comment below a post, an anecdote or a link with supporting evidence. For instance, Bashir had recently commented on a friend’s post. He navigated to his newsfeed to show me. His friend had issued a warning that *Facebook* had changed its terms of use, allegedly giving it extended rights for commercially exploiting users’ data. A discussion among friends ensued on how to counteract this. Bashir scrolled down to show me his response:

[7, 17] “Ok here, I basically just said that all you can do basically is to delete your account, and then here this guy replied and posted a link to this article – shall I click on it now [DK: participant opened the link in a new browser window] and that explains it point by point basically.”

Like Josephine and Bashir, participants are engaged in an intersubjective process to establish their own common-sense logic of surveillance. This reflects Berger and Luckmann’s claim that the logic of how an institution operates “[…] does not reside in institutions and their external functionalities, but in the way these are treated in reflection about them” (Berger & Luckmann [1966] 1991:82).

SNS are an arena in which such reflections take place, where participants are routinely engaged in a collaborative process of constructing knowledge about surveillance. Generally, this process is unstructured: facts about how surveillance works appear surreptitiously, are produced ad hoc and in passing. Spontaneous discussions emerge out of posts, likes and links. They are fragmented and do not connect into a coherent whole - just as participants feel that their surveillance knowledge is perpetually incomplete, as the last chapter established, the interface of SNS does its part. It organises information into a linear stream, such as most prominently realised in technologies like *Facebook* or *Twitter* newsfeeds. In a continuous progression of new posts and likes, revelations about surveillance are embedded in a stream of fleeting moments, appearing and disappearing in the newsfeed, rather than archived and consolidated. Writing about privacy threats, Marichal (2012) sees an 'architecture of disclosure' built into *Facebook* that encourages users to reveal and disseminate information about themselves. But conversely, participants have created an architecture of inquiry on SNS. Through creative practices, be it sharing links, liking posts or commenting on what others have revealed on SNS, they use the technological affordances of SNS to probe into how surveillance works.

7.1.3. Face-to-Face Interaction

Surveillance on the internet is not virtual. Its consequences impact people's material lives – both online and offline, as notions of 'social sorting' (Lyon 2003) and examples of offline repercussions based on online data (Meyer-Schönberger 2009) illustrate. But similarly, probing into surveillance is not just mediated by screens but a theme in face-to-face interaction.

Rebecca is a student in Erfurt, Germany. She is from a small town in Thuringia and commutes back home from university every weekend. Her boyfriend still lives there. When I interviewed Rebecca about surveillance encounters, she recalled a particular moment:

> [7, 18] "Facebook is also found via Google, as far as I know, and that is a bit scary. So my boyfriend googled himself and then there was immediately his photo and his name and ... we thought it was a bit weird, so then we talked about it for a bit, about the whole data collection thing." [DK: translation from German]

Rebecca and her boyfriend both had existing ideas of their own about how *Facebook* profiles and *Google* search intersect. But they were confined to their subjective experience. United in front of the computer, they jointly encountered an unfolding

moment that foregrounded their ideas. The couple then thematised their previously isolated thoughts and in conversation probed deeper into how *Google* works. Yet in many cases, a specific, shared screen experience is not even involved. Christina, the business journalist from London I introduced in a previous chapter, mentioned how computational surveillance regularly turns centre stage in booze-fuelled nights out with friends:

[7, 19] "Facebook is just a normal thing, you talk about it…like when you have nothing else to say, well not that it is boring as such, I mean more in a way that everyone has a say. You are with your mates, someone is really pissed or what whatever and jokes about Facebook, like 'don't put this on Facebook', and then everyone weighs in and it turns into this whole discussion on privacy."

In Christina's example, participants discuss their personal encounters and opinions with surveillance in an entirely different social setting. The friends share a joint implicit understanding about surveillance, as Christina's remark to not 'put this on Facebook' shows. Conversations can get more technical than this, as James, whose is an avid user of the privacy tool *Ghostery*, explains. At a party, he encouraged his friends to give it a try:

[7, 20] "We talked about the whole privacy thing. And then I said, here I use this tool, it's really cool, check it out."

Like on SNS, participants do not gather face-to-face in a concerted effort to unmask and decode surveillance. Face-to-face conversations about how surveillance works are void of a political imperative or an *a priori* agenda. They happen serendipitously, interwoven in the flow of conversation that is part of everyday life. Just like in the case of SNS discussed before, these conversations are also acts of meaningful reciprocity. Face-to-face conversations help participants to solidify their perceptions, hypotheses and worries about surveillance in an intersubjective consensus.

7.1.4. Synthesis: the Conceptual Grid of Knowledge Production

The social construction of knowledge about surveillance takes place in three communicative arenas; news media, SNS and everyday face-to-face interaction. These arenas are characterised by a number of focal concepts which have emerged in the analysis above. These concepts describe the basic structure of participants' social construction of knowledge about surveillance. The media present *shorthand knowledge* for 'how surveillance really works' and 'how things are done'. On SNS and in face-to-face interaction, participants probe into surveillance through *collaborative practices*. Knowledge of the workings of surveillance is contingent on an *intersubjective consensus*,

which is largely implicit in media representations and explicit in talking about surveillance with peers in the context of SNS or face-to-face interaction. Such consensus is often developed through acts of *meaningful reciprocity*. The role of these communicative arenas is indicative of emerging 'cultures of mediatization' (Hepp 2013) in which human agents' experience and meaning-making of computational surveillance is embedded. Hepp highlights that

> "[…] it makes sense to treat *media cultures as cultures of meditization*. By this I mean that media cultures are cultures *whose primary meaning resources are mediated through technical communications media*, and which are *'moulded' by these processes in specifically different ways*" (Hepp 2013: 70, original emphasis).

Computation moulds people' resources of meaning-making and generates meaning itself, as *Chapter Three* and *Chapter Six* have shown. However, recognising the agential forces of computation, people also construct meaning in reference to computation across all three communicative arenas I have outlined. They additionally use communication media (news media, SNS) as means to engage in processes of meaning-making in relation to these very media environments. The next section illustrates the practices associated with meaning-making in more detail and contextualises them through Berger and Luckmann's concepts.

7.2. The Troubled Common-Sense Reality of Surveillance

Communicative arenas help people to construct and to reconstruct the reality of surveillance through common-sense knowledge. Usually, the common-sense world is stable and unproblematic. As Berger and Luckmann attest, "the world of everyday life proclaims itself" (Berger & Luckmann [1966] 1991: 37) and challenges to these proclamations need to be deliberative acts. In principle, subjective experiences or external brokers of ideas, be they groups or individuals, can suggest "counter-definitions of reality" (ibid. [1966] 1991: 186). Yet, the authors concentrate on the successful construction of reality. The instability features as exceptional situations of crisis (Berger & Luckmann [1966] 1991) and as an outlook onto an increasingly complex world "in which discrepant worlds are generally available on a market basis" (ibid. [1966] 1991: 192). As the following section will show, the case of surveillance is different. Situations of crisis are not scarce, but constitutive of the social construction of surveillance reality.

It is riddled with contradictions and beset with struggle, making a stable and all-encompassing common-sense reality an unlikely state of affairs.

7.2.1. The Thickness of Reality and its Experience as Construction

When talking about the omnipresence of surveillance in the media today, some participants get reminiscent. Bemused and amazed, they pause and express their own bewilderment that figuring out how surveillance works has become part of their everyday life. Franzi, the physiotherapist form Aachen, says:

[7, 21] "Wow, if I talk about this now, actually…well, two years ago or so, you did not hear much about it. It has gotten really crazy over time." [DK: translation from German]

Whereas Franzi is surprised by the proliferation of surveillance knowledge, others find it peculiar that a subject like surveillance has entered public discussion the first place. Stefan alludes to the 'geeky' nature of the subject, that already others highlighted.

[7, 22] "Actually, the topic is pretty particular. Well, I don't know, it is not rocket science, but pretty geeky nonetheless. Well, if it wasn't for everyone being online nowadays, the internet is everyday now. I do not know how to say it. Well, it is really a pretty extreme subject, because it is so particular. Well I would rather think it is for computer freaks, but it is a topic for everyone still." [DK: translation from German]

Yet the pervasiveness of public debate does not mean that the knowledge about surveillance is finite or static, and therefore solid. Whereas reality 'thickens' over time (Berger & Luckmann [1966] 1991), the reality of surveillance is far from reaching a solidified state. The reality of surveillance is emergent and fragmented. Josephine calls it a puzzle:

[7, 23] "It is like a puzzle, because you have to piece everything together. Someone makes a post here, then here, and then you read something somewhere else. I think you have to piece it together over time, it comes more and more together and then you know more easily what the others think and how it works." [DK: translation from German]

The reality of surveillance has to be assembled, as Josephine's 'puzzle' metaphor illustrates. Other participants use different terms, but their conclusions are similar. Lars reflected on how his knowledge of surveillance and its workings came about:

[7, 24] "You just have to figure it out from the fact. You know the facts I'd say, from the media and stuff." [DK: translation from German]

This notion of assemblage inherent in participants' accounts has wider implications. It suggests that reality does not appear as self-evident. Fundamentally, this lends a new meaning to the idea of a social construction of reality. Usually, people do not consider

their own reality as constructed. The construction of reality is an analytical concept employed by sociologists. But Josephine's example changes this conceptual scope. The common-sense world of surveillance is perceived both as 'real', as well as constructed. The experience of construction is an intrinsic feature of the reality of surveillance. In particular, this is apparent in SNS as a communicative arena. Here, the construction of reality creates data about itself: on their newsfeed, in posts and comments, participants are witnesses of their own and their peers' labour of construction. Alongside a given consensus about surveillance, they see its conceptual scaffold. This does not make it less 'real'. Yet, this scaffold is a reminder of the incompleteness and the fluid, rather than thick state of the reality of surveillance.

In part, this assemblage in not a mere construction of reality, but a reconstruction. During my interviews, I learned time and again that participants position what they know about the workings of surveillance against a reference point: the world of surveillance from the inside perspective of computation. To use Berger and Luckmann's term, the reality of computation is a "finite enclave of meaning" (ibid. [1966] 1991: 39). It denotes a socially segregated reality that has its own logic and principles. It makes sense in itself and for itself, yet is insulated from people's experience. Participants believe that the unobscured truth about how surveillance operates is located within the logic of computation. Josephine's metaphor of the 'puzzle' already alluded to an external reality outside the common-sense world: what she knows has to be pieced together into a whole which already exists elsewhere. Other participants are even more explicit. Lars, the former police officer I introduced earlier, sees *Google* and *Facebook* as 'Datenkraken', or data leeches. He thinks that these companies have plotted a surveillance architecture that no one else oversees. Figuring out how surveillance works means trying to leap into their world:

> [7, 25] "As far as I know by now, you somehow have to get closer to Facebook. Because only they now how everything works. And I think this is what people somehow try. Like that you reconstruct, try to comprehend." [DK: translation from German]

People's common-sense world of surveillance is not self-referential, but also an approximation to computation as an enclave of meaning. Participants seek to 'tear down the walls' and integrate this world of computation into their common-sense world. Computed sociality (Kallinikos & Tempini 2014) then is not merely a new configuration of sociality that is rendered in the computational domain. Computational mechanisms of

meaning-making are joined by people's efforts to consciously relate to them beyond being mere 'dividuals' in their calculation and to bring together enclaves of meaning into a common understanding. Yet, as much as participants try to reconstruct what goes on behind the scenes, their own reality always remains different. Apart from the lack of access to computation, their efforts to reconstruct reality do not take place in a void, but within the context of their own biographical and social experiences.

7.2.2. Manoeuvring Communicative Arenas

Although participants think that a public discourse around surveillance helps them understand how surveillance operates, they feel that assembling specific facts, piecing together bits and fragments, finding out what common-sense is, are tasks left to themselves. Common-sense reality is always surrounded by finite enclaves of meaning to which everyday life relates, yet is removed from, such as the legal system, medicine, or flying an airplane. The more differentiated a society, the more acute the development of segregated provinces of meaning becomes. However, there are no institutionalised experts which mediate between the world of computation as an enclave of meaning and the everyday, lived experience of surveillance. There is no doctor, no pilot, no lawyer who claims responsibility for a body of knowledge and offers interpretation to outsiders: 'fasten your seatbelts', 'you can sue them', 'you will be fine tomorrow'. This section documents how participants order the revelations of surveillance which they encounter across different communicative arenas and how common-sense knowledge consolidates without public-facing expert systems. I illustrate this in two sections which document how people reconcile competing interpretations of surveillance, and how they imagine a social consensus.

Competition of Interpretation

Communicative arenas entail a competition of interpretation. 'How it's done', or 'how it works' is not always clear-cut. Stuart recalls a situation when a privacy scare was making the rounds on *Facebook*. One morning, he logged into the site and saw his entire newsfeed crowded with the ever-same status update posted by numerous friends:

> [7, 26] "Everyone was like 'I hereby declare'…and then they basically went to say that they don't give Facebook the permission to use their data."

Stuart could not recall what exactly sparked this mass-reaction, but he very well remembered what went through his mind when he saw all these posts. For a moment, he

wondered whether he should follow the others, copy and paste this declaration and publish it on his newsfeed as well. It seemed to be consensus, at least there was a group which vocally suggested it. Stuart was just about to accept it as the 'thing to do' when one dissident voice put his assumption of common sense on shaky grounds:

[7, 27] "I'm friends with this guy…and he was basically mocking the whole thing. Like he posted something like 'I hereby declare that I have no fucking clue and am not a lawyer so I don't know anything about privacy rights'. […] I don't really know him that well. We go to uni together. He is just a smart guy, so I thought I can believe what he says. It just did come together. He wasn't really like someone where I thought: 'oh yeah, I will do whatever this guy says'. And to be honest, it sounded quite obvious when he said it."

This episode highlights a fundamental problem: the intersubjective experience of surveillance is not homogenous, but fractured. It is riddled with dissonances of interpretation that hinder people to validate an apparent social consensus. Acts of "disconfirmation of reality" (Berger & Luckmann [1966] 1991: 171) are abound. In Stuart's case, this disconfirmation happened right after he stumbled across an apparent fact. It gets more complicated when conflicting versions of reality only emerge much later, in and another context. For instance, one participant lamented:

[7, 28] "You think you have understood how it works and that you can never be sure what happens with your data. And three weeks later your read that there is a new law and that it was all overblown and exaggerated." [DK: translation from German]

But Stuart found a way out. His *Facebook* friend did not just challenge the common-sense reality around him, but simultaneously offered a new interpretation. For Stuart, this friend spoke from a privileged vantage point. This illustrates that expert and lay knowledge are not dichotomous concepts. Giddens has already highlighted that technical knowledge filters back and is re-appropriated by lay actors (Giddens 1990: 145). In order to lend stability to the contradictory flow of surveillance knowledge, participants draw on tactics of ascribing surveillance expertise to selected others. Lars says:

[7, 29] "Well, after a while it just emerged. This is a buddy of mine, wait, this one, he often posts stuff about that and then I think it's pretty solid what he says. Well, over time I've found people for that, like this one. Or my brother, he knows a lot about that stuff, too. So I watch what they say, and if they say it's like that, then I trust them. Because, honestly, there's so much stuff that gets posted and also a lot of bullshit, as the day goes on." [DK: translation from German]

Instead of identifying trusted sources, others weed out misinformation. Anna is friends with many family members on *Facebook*. Her aunt notoriously posts advice on protection against surveillance, but Anna ignores it:

[7, 30] "[...] especially my aunt, she always shares some newspaper articles on privacy and Google and stuff like that. But she's just too old, she doesn't get it anymore. It's all very trivial. Either you know about it already for a long time anyways, or she also shares appeals like 'this is how you can protect your profile' and stuff like that. Of course, that's totally naïve. That's what people do who still play Farmville or share Diddl Mouse [DK: a cartoon character] pics. And then you immediately know, well, you know what I mean." [DK: translation from German]

Alongside those designated experts, nearly all participants highlighted situations where they had to make ad-hoc decisions, such as journalist Christina:

[7, 31] "You just have to make a decision, so I pick whatever sounds most convincing. Like someone posts a link and then someone says 'wrong!' or something and posts another link."

But such decisions do not come easy. Karen, the dental hygienist, said that conversations about surveillance tend to go in circles, and competing interpretations are often not reconciled:

[7, 32] "Like one guy, he said that Facebook sends you targeted ads. But then I was like 'how can that be', I mean if I look at the kind of ads that I get, that clearly is not targeted. And my friend agreed, - so we were in this discussion and at the end I did not know anymore, so yeah, that happens."

Figuring out how surveillance works then is systematically entangled with confusion and resignation. Participants are faced with competing hypotheses that are temporary, refutable and potentially contradictory. Berger and Luckmann claim that the validity of one's knowledge is a fundamental characteristic of everyday life: "validity of my knowledge of everyday life is taken for granted by myself and others until further notice, that is, until a problem arises that cannot be solved in terms of it" ([1966] 1991: 58). In participants' experience, this validity is inherently unstable. What is true about surveillance in one moment can emerge as a misinterpretation in another, and participants struggle to break this cycle.

Imagining Consensus

The uncertainties attached to surveillance knowledge also affect how participants interact with others. Paula told me how embarrassed she felt after her *Facebook* post on privacy had been dismantled by others:

[7, 33] "Well yes, because surveillance and privacy are always being such a matter of debate and because it's become so important, I thought, well I thought now you're going post something as well. Then the reactions were pretty stiff – like 'wrong' and 'that's totally not true' and so on. I don't always know how they'd know, but well, as I said that wasn't that great." [DK: translation from German]

Even on the day I interviewed her, Paula was still not sure whether her interpretation was indeed factually wrong. But the unanticipated opposition made her hesitant to post anything at all. Her experience is indicative of a general phenomenon. Participants struggle to gauge how much others already know, and wonder how certain they can be about what they know themselves. For instance, Ann-Kathrin says:

[7, 34] "Then I didn't dare to post such a link. Well, sometimes I just don't know anymore whether I'm up to date or about to out myself as a complete idiot." [DK: translation from German]

Whereas some are concerned that their contributions may uncover a lack of knowledge, others worry that they may come across as too eager. Linda, the maths graduate, worries about the expression she is giving off:

[7, 35] "I'm often like, I don't want to come across as a total nerd. Like someone who thinks it's is all ridiculously important. I mean people exist. I, well I wouldn't say I am an expert, but I probably know more than the others here to be honest, because I read a lot and I have always been around computers."

These concerns are expression of a struggle to identify one's own relative positioning within a collective discourse whose scope and boundaries are not apparent. Although talk about surveillance is pervasive, its rules of engagement are unclear. People do not participate impulsively in surveillance discussions, but try to assess the social situation to which they contribute beforehand. They try to imagine what the consensus about surveillance is, and position their own contributions accordingly. For instance, Amanda, the finance student I met at the university message board, told me how she had read an article about privacy violations on SNS that she wanted to share it with her *Facebook* friends. But she first scrolled through the newsfeed to see whether someone else had already posted the same discovery:

[7, 36] "Well I thought to myself, it wouldn't want to be someone who reposts stuff and someone else has already posted it and I was late and did not notice. But I didn't find anything, so I just posted it."

In Germany, Ann-Kathrin was worried that her recent discovery was in fact too simplistic to share on *StudiVZ*, outing herself as a novice. However, she recalled that one of her friends had recently made a similar post that received many likes:

[7, 37] "Well, it was about Google Street View. My friend posted something on Facebook, like that these days all these cars are driving around everywhere. I had read something, uhm, seen, an article, with a photo of what these cars look like. Then I thought to myself, 'you're going to post this'. But first I wanted to make sure that, well, that people would be interested. So I again checked my friend's profile, on Facebook, and he got quite a few likes there." [DK: translation from German]

Both Amanda and Ann-Kathrin engage in contextualising tactics to position their own contributions vis-a-vis a common sense. They construct reference points against which they assess what is appropriate to say. As surveillance knowledge is in flux, participants cannot fall back on a fixed notion of common sense. What exactly is common sense needs to be actualised at a given moment in time. By probing into the workings of computational surveillance, participants also probe into the structure of knowledge that surrounds them. In consequence, they adjust what they share and alter how they participate in the construction of knowledge. Based on incidents like social sanctions on SNS, discussions about surveillance are experienced as normative, even if de facto, such norms may not exist. The social construction of knowledge about computational surveillance takes places in an environment of imagined norms, which contributes to the dissemination of this knowledge as such.

7.2.3. Synthesis: The Hard Work of Common Sense

Seemingly casual posts on SNS and mundane banter about computational surveillance in face-to-face interaction are hard work. While people generate common-sense knowledge about computational surveillance in interaction with each other, it does not translate into a universal, comprehensive common-sense reality. People experience isolated instances of common sense. The body of knowledge remains fragmented and does not translate into an overarching, comprehensive consensus. It also is a common-sense until further notice that is unstable and prone to crisis. While knowledge thickens over time, confirmations of common-sense and disconfirmations coincide.

In contrast to other domains of everyday life, computational surveillance is not a finite body of knowledge where people can assess their level of understanding against a reference point. They constantly need to evaluate, assess and infer how socially shared acts that reveal computational meaning-making relate to the common-sense of others. Reconciling competing interpretations and imagining a social consensus are prerequisite acts for people that co-determine the development and dissemination of common-sense knowledge. These practices and problems further extend the notion of computed sociality in that they show how the computational rendition of reality (Kallinikos 2009) itself coincides with reconfigured modes and possibilities of social construction for human agents. Computed sociality therefore does not merely take place in and through

computation, but also manifests itself in broader social practices outside the computational domain that stand in relation to it.

7.3. Consensus-Maintenance

Although the reality of computational surveillance is emergent, far from 'thick' and ultimately unlikely to congeal into a stable and coherent whole, instances of intersubjective common sense between human agents are attainable. This section explores how people maintain and solidify common-sense knowledge to avert crises and disconfirmations of reality to which living in computed sociality is prone, as I have shown above. It provides an answer by embedding people's narratives into a reinterpretation of what Berger and Luckmann call "conceptual machineries of universe-maintenance" ([1966] 1991: 123). This slightly unwieldy term refers to mechanisms by which common-sense reality is legitimated, and how subjective experiences are attuned with collective knowledge.[39] Within these parameters, this section explores two types of mechanisms; the de-reification of computation, and folk tales of surveillance. These mechanisms ultimately demonstrate how in context of reconfigured modes and possibilities of social construction, human agents rely on collaborative practices to ascribe interpretations to computation. They provide evidence that in computed sociality, human agents are not just reactive to the parameters, frameworks and problems of consensus that computation imposes on them, but proactively stabilise a social consensus.

7.3.1. The De-Reification of Computation

Surveillance is an octopus, at least in Germany. During one of my interviews, a participant mentioned how a newspaper article discussing *Google* featured the illustration of an octopus, alluding to the concept of 'Datenkrake', a popular German expression that likens systems and institutions that collect personal data on the internet to an octopus spreading its tentacles. Although such visual representations of surveillance are scarce, participants do not imagine surveillance purely as abstract. Sarah had read an article about a privacy breach on *StudiVZ* in the news:

[39] This term is unusual, even for Berger and Luckmann, who have a penchant for bulky terms. Its machinistic connotation either appears at odds with the very human process of social construction, or implies that Berger and Luckmann consider universe maintenance as uncontroversial and thus occuring in an automatic fashion like a machine. There is evidence for the latter. As I highlighted in *Chapter Three*, Berger and Luckmann assume stablility as a social default at their time of writing and consider dissonances between competing enclaves of meaning as exceptional events.

[7, 38] "[…] this time a hacker had written a software and it tapped hundreds or thousands of user's data. StudiVZ was powerless before that, they said. And that I find pretty serious, that they couldn't protect the data – I mean they are professionals, all engineers and IT guys, they earn their money with that kind of stuff and there should be some software protection or something like that. But then one of them got interviewed and he said that it wasn't their fault." [DK: translation from German]

Sarah does not talk about *StudiVZ* as an abstract entity, but conceives it in terms of individual agents, technicians and IT professionals. She ascribes complex computational characteristics to personified human agents. Ann-Kathrin's view of computational surveillance is related:

[7, 39] "Yeah, I've read that a couple of times now, that somehow a journalist logged in via StudiVZ and then observed a person for several weeks, printed photos and could prove for a long period of time what that person was doing every day, who they met, and that's pretty scary. In reality it's not people who do that stuff but robots or something like that. But that's what they wanted to show: that SudiVZ is doing it like that by design, and that was pretty scary, as I said." [DK: translation from German]

Ann-Kathrin remembers that reporters have simulated the processes of computational surveillance with human agents as embodied placeholders. She extends this template in her own vocabulary. Somewhat clumsily, she refers to 'robots' doing the data aggregation and extraction work that has been simulated by journalists, subsuming computational processes into material bodies.

Some participants go a step further and identify specific individuals as main agents behind computation. Evelyn noticed a heated discussion about *Facebook*'s use of personal data on the social network itself:

[7, 40] "[…] things were posted, like …'this and that… that's how it looks like' […]. Then I also see how this, what's his name again… Mark Knopf … or whatever… the Facebook guy … is being discussed and then you see all that and then you're going to check your settings." [DK: translation from German]

Although Evelyn cannot recall his name and nearly confuses him with musician Mark Knopfler, she projects the institutional complex of *Facebook* on its founder Mark Zuckerberg. The role of Zuckerberg as personal culprit or mastermind of surveillance appears time and again. Tim from London was very vocal about companies like *Google* and *Facebook* making money from users' data. He spoke vividly about a looming change in *Facebook* privacy settings, just like others. But he put an emphasis on the persona of Mark Zuckerberg:

[7, 41] "[…] in the comments, there are always these jokes about Mark Zuckerberg [DK: on Facebook]. And also I saw someone post this cartoon where Mark Zuckerberg was photoshopped like Uncle Sam and it said 'I want your data' or something."

Based on what I learned from Evelyn and Tim, in my later interviews, I specifically asked whether participants ever encountered the name Mark Zuckerberg in their *Facebook* newsfeeds or talked about him as a person. For instance, Henning, who is 22 years old and just moved to Aachen to study Engineering, said:

[7, 42] "I once did it myself. Well, as a joke, but still, it's true. 'Zuckerberg you turd' and stuff like that. […] Well, because of all the data leaks and whatever other things there are, there are always these scandals coming up." [DK: translation from German]

In all these instances, people converted abstract, unknown computation into material entities that they can conceptually grasp and relate to. These tactics modify how Berger and Luckmann consider common-sense reality. For them, it emerges through reification. The term denotes the "[…] apprehension of human phenomena as if they were things, non-human and possibly supra-human" (Berger & Luckmann [1966] 1991: 106).

By making institutions or phenomena appear not man-made, they become adamant and set in stone. In many accounts that have been discussed so far, participants see the world of computation as exactly that - a non-human facticity that is impenetrable:

> "The reified world is, by definition, a dehumanized world. It is experienced by man as a strange facticity, an *opus alienum* over which he has no control rather than as the *opus proprium* of his own productive activity." (Berger & Luckmann [1966] 1991: 106, original emphasis)

By attributing computation to material bodies, participants engage in acts of de-reification. The reified world of computation is locked away in another enclave of meaning that people lack access to. Through de-reification, people re-integrate this removed enclave of meaning into the common-sense reality of the everyday. While Berger and Luckmann do not expand on the notion of de-reification,[40] Sewell's (2005) analysis how contemporary life is increasingly subject to 'de-reification' provides a clearer context for participants' acts. He sees de-reification as claiming back control over the production of meaning by making previously immutable and incontestable realities mouldable and open for negotiation. In participants' own narratives, this means that if Zuckerberg is deemed a surveillor rather than *Facebook*'s algorithms, the world of surveillance suddenly becomes man-made again and thereby enters people's domain of understanding. In this context, the notion of control that Berger and Luckmann speak of

[40] However, Berger and Luckmann realise the importance of analysing de-reification for future research: "The historical and empirical application of the sociology of knowledge must take special note of social circumstances that favour de-reification [...]" ([1966] 1991: 109).

means that an interpretation on the level of human cognition becomes possible again. It also sparks a sense of comradery. Lars summarises quite bluntly how a common, personally identifiable villain creates a basic social consensus.

[7, 43] "Well, they are all bashing this Zuckerberg guy. That's also stupid, but… Anyway I think that everybody thinks he's fishy. This means you will get a lot of 'likes'. I mean if you post something about him." [DK: translation from German]

Acts of de-reification then create a foundation through which collaborative practices of figuring out how surveillance works can be easier sustained.

7.3.2. Pigs and Folk Tales

All other fieldwork had long been wrapped up when one day, I got an email from Adam. I had initially met him nearly six months ago for an interview, after which he had just disappeared. Whether I still wanted to do 'that second interview', he asked. We met at my home in London. Adam, an art student, had brought his laptop. After the think aloud protocol, we took a look at his *Facebook* account to further explore the issues we had been talking about. In his first interview, Adam had attested that there was a lot of talk about surveillance in his newsfeed and he was eager to show me this time. After a few clicks, he brought up an image that featured two cartoon pigs with speech bubbles over their heads: 'Isn't it great', one pig is depicted saying, 'we have nothing to pay for the barn'. The second pig is seen replying 'Yeah! And even the food is free'. This dialogue is supplemented with the following subtitle: '*Facebook* and you. If you are not paying for it, you're not the customer. You're the product being sold'. The post had been shared by one of Adam's friends a few days prior to our interview, but it had originated elsewhere. Adam's friend merely added to its distribution by making it available to his circle of friends. When Adam and I revisited the post, it had garnered a lot more activity since Adam's first encounter. We counted 235 'likes', it had been shared 142 times and continued to receive comments by other *Facebook* users. Adam permitted me to make a screenshot, which I show below.

Figure 5: 'Facebook And You' Cartoon

Source: Screenshot from participant's Facebook account.

He commented on the cartoon as follows:

[7, 44] "The pigs, I mean that's really brilliant. It's exactly what we have been talking about, I mean what I was gonna say. I guess it's obvious, but it's good to see someone say it, like you are reminded, especially if it's this funny. And I mean everyone agrees."

The cartoon did not reveal anything that Adam did not already know about surveillance. The facts it presented were banal. Yet, a closer look at Adam's statement suggests that the cartoon nevertheless plays a critical role in the construction of reality. The cartoon foregrounded a well-known fact about surveillance in Adam's consciousness and reaffirmed it. As others supported the claim in the cartoon, Adam felt that what he knows is shared by others and accepted as common sense. Indeed, in the *Facebook* comments, people were chiming in. They affirmed the cartoon's claim and cracked jokes about their personal data being sold. What were little more than two pigs and a speech bubble can be

understood as an affirmatory token that ascertains reality as intersubjectively shared. The likes, shares and comments are practices of acknowledgement which performatively consolidate a consensus.

It took the cartoon on Adam's newsfeed and the flow of comments and shares below it for me to realise that apparently banal facts that had emerged in my previous interviews were more than they seemed. For instance, in Franzi's circle of friends, a conversation in the pub or at a party can easily gravitate towards *Facebook* and related questions. She does not always agree with her friends:

> [7, 45] "Well, we do fight, well, fighting is too much… let's say we don't always all agree. I for example don't have a problem with my pics being found online, but my friend, she's super extreme and has blocked everything, even for her own friends. She thinks… well, that Google and others won't get her data that way, because they can also search Facebook – completely paranoid! Well I do like her, but… but I always say you've got to decide for yourself. No matter where you go, you're always the commodity. Nothing is for free, you always give something in return, be it money or data. Well, and everyone pretty much agrees to that, even my girlfriend. But everyone chooses to deal with it differently." [DK: translation from German]

Franzi uses a very similar phrase to the one in the cartoon, describing personal data as a commodity. She sees it as a means of reconciliation in a disagreement with her friend. The phrase is a lowest common denominator, a fact about surveillance that everyone can agree on. If common-sense reality is falling apart or threatened to disintegrate when different subjective narratives about surveillance clash, affirmatory tokens ensure that a basic common ground is maintained. Disagreements are converted into questions about details, not fundamentals.

The message behind the pig cartoon surfaces time and again in various other stories. Participants routinely employ such affirmatory tokens to stabilise common-sense interpretations of surveillance. These tokens belong to the realm of mythology, which Berger and Luckmann identify as an important means of maintaining common-sense reality. This is particularly relevant to the context of surveillance, because mythology is "[…] close to the naïve level, in that, although there are specialists in the mythological tradition, their knowledge is not far removed from what is generally known" (Berger & Luckmann [1966] 1991: 128).

In the fragile reality of surveillance, there is no canonical mythology to draw on. Yet people craft and reproduce specific stories about surveillance which serve as affirmatory tokens. I call them folk tales in order to maintain a theoretical link to Berger and

Luckmann, but to differentiate them from common mythology as religious and containing a large corpus of interconnected narratives. The following two examples from Frank and Stefan illustrate how these folk tales are manufactured through people's own experience.

For instance, sometimes unfolding events, where surveillance is revealed, obtain a larger audience and are converted into socially shared narratives. Frank's story is particularly telling:

[7, 46] "You pretty much constantly hear these stories – hacked profile, and 'people watch out, hands off the games, I got a virus' or stuff like that. As I said, time and again you hear about it when you talk to people, that it happened to someone or that you know someone who it happened to." [DK: translation from German]

Such folk tales are woven into the fabric of everyday life and perpetually reconfirmed. Stefan felt awkward broaching the issue, but eventually found the courage:

[7, 47] "Can I say that? That's a bit embarrassing maybe. Uhmmmm, in my shared flat. Well when somebody closes the door [DK: to his own room] then we always say: 'Always remember to log out of Facebook first!' Because… well, it's a guys' house, if you know what I mean." [DK: translation from German]

This recurring joke between flatmates is part of an everyday household situation and reproduced through face-to-face interaction. Stefan and his flatmates have attached the theme of surveillance to an inferred behaviour that happens behind closed doors. Here, they believe, *Facebook* collects (potentially compromising) data about its users even if they are not on the *Facebook* website itself. Such banter between friends is an affirmatory token of surveillance reality. By attaching it to a mundane everyday situation, Stefan and his flatmates reconfirm a common feature about surveillance without having to engage in a conversation about surveillance specifically – the confirmation of common sense reality happens in passing.

Several male participants and one female, both from the UK and Germany, and from different cities within Germany, made a very similar reference to adult content and surveillance. For instance, Josephine highlights that she has heard a story about an embarrassing mishap a number of times already:

[7, 48] "Sometimes you hear, well, that probably was in the news once, there was this guy who was logged in at Facebook and then visited a porn site and apparently clicked something wrong – super awkward – then it was on his profile! Such-and-such likes porn – how embarrassing!" [DK: translation from German]

Whereas some affirmatory tokens, such as sharing a cartoon on *Facebook*, are calculated and rational acts, others like Stefan's story are affectual and embedded in everyday themes of conversation. Without people taking specifically about surveillance, these tokens inadvertently stabilise the common-sense reality of surveillance and ensure that the intersubjective construction of reality becomes possible by providing people with a common ground. Affirmatory tokens are collective practices but not agential by themselves. While they are not direct acts towards surveillance, the narratives they convey remind people of the need to act towards surveillance and provide templates for doing so.

7.3.3. Synthesis: Reality Checks and Social Grooming

In an environment where common-sense knowledge is unstable and does not congeal into an overarching reality, people employ tactics to maintain and solidify common understanding of surveillance. Affirmatory tokens, and folk tales as elaborate narratives of such tokens, are mechanisms of consensus-maintenance that provide people with reality checks that allow them to gauge whether their knowledge of surveillance is congruent with that of others. They also serve as a form of social grooming, implicitly indicating to each other that one believes in a common set of assumptions. These are both consequences and prerequisites for the construction of knowledge. Affirmatory tokens emerge out of what is known about surveillance and communicate to people that achieving a common-sense understanding is possible. Such mechanisms of consensus-maintenance do not overturn computational meaning-making and do not represent an infallible truth. Indeed, the intersubjective consensus about how computation operates may be technically flawed, or reductionist. People do not become experts that muscle in on a computational modulation of the world through such mechanisms. Instead, such mechanisms socialise the experience of living with computation and provide templates for interpretation. The intersubjective interpretation of computation then is part of computed sociality itself.

7.4. Chapter Conclusion

In his essay on the complicity of anthropological fieldwork, Marcus considers changing boundaries and relationships between ethnographers and their subjects. Through collaboration between agents, what Marcus defines as "'co-operation' in dialogue" (Marcus 1997: 93), new avenues of insight become possible. This chapter has shown that

Marcus' notion of collaboration is not confined to the production of knowledge between a professional researcher and research subject. Extending it to participants of this study resonates with Garfinkel's definition of ethnomethodology as: "[…] the actual methods whereby members of a society, doing sociology, lay or professional, make the social structures of everyday activities observable" (Garfinkel [1967] 1984: 75). As lay actors, participants conduct 'fieldwork' of their own in cooperation with other non-experts to foster, disseminate and consolidate knowledge about computational surveillance. They do, in a sense, echo Geertz famous anthropological rallying cry to "[…] hawk the anomalous, peddle the strange" (Geertz 2000: 64), by probing into a world of alien algorithms and corporations like *Facebook* and *Google*.

The notion of collaboration stretches across the themes discussed in this chapter. In the communicative arenas of SNS and face-to-face interaction, participants piece together how surveillance works. And even though news media, as another communicative arena, offer ready-made, top-down interpretations of surveillance, their integration into common-sense reality does not take place without collaborative effort: what the media say about surveillance is replicated, queried, questioned or confirmed in *Facebook* posts, casual face-to-face conversations and folk tales through emerging cultures of mediatisation (Hepp 2013).

This chapter has shown that such collaboration is not a linear trajectory to an all-encompassing, uncontroversial common-sense reality of surveillance. There is no 'Heilsversprechen' (Riesebrodt 2007), a promise of salvation, at the end of a collaborative enterprise where surveillance stands demasked, decoded, and ultimately understood in its operations, motivations, and consequences. Although the common-sense reality of surveillance thickens over time, it does not solidify. In a sense, it is asymptotical: although instances of surveillance knowledge expand over time, a comprehensive reality seems impossible to reach. In another sense, it is dialectical: common-sense knowledge and its dissolution coincide.

Building and deconstructing a reality of computational surveillance in dialogue is a collaborative effort. This includes the foundations upon which such knowledge can be constructed in the first place. Amidst the fragility of computational reality, people collaboratively reconfirm the foundations that make intersubjective common-sense possible in the first place. Through affirmatory tokens, people reproduce truisms about

how computational surveillance works. As a lowest common denominator, these affirmatory tokens ensure that forming an intersubjective consensus remains possible in the light of competing interpretations.

Collaboration between lay actors does not mean that people can systematically challenge the reality of computation and gain access to its enclave of meaning. Yet, the notion of collaboration underscores that dealing with computational surveillance is not an individual and ultimately lonesome affair. The previous chapter, particularly through the notion of unfolding events, has shown how deeply and personally the world of computation impinges on people as individual agents. This chapter has added that querying, contextualising and narrating such encounters is a set of social practices woven into the fabric of everyday life and expression of the computed sociality that Kallinikos and Tempini (2014) have outlined. In combination with concepts from Berger and Luckmann, this empirical analysis has expanded the notion of computed sociality and demonstrated that it includes not just the computational modulation of reality, but also practices of knowledge production by human agents in reference to computation that are enacted outside the computational domain itself. In other words, whereas Bucher (2012c) highlights how computation ‘makes sense’, I have documented empirically how people make sense of computational surveillance that makes sense about them in a collaborative process of social construction. The chapter has shown that a computational logic does not monopolise meaning despite its constitutive role in the social world. Hepp (2013) has criticised traditional notions of a ‘media logic’ and drawn on Berger and Luckmann to show that ascribed meaning and interpretation by human agents towards what the media and hence computation ‘do’ recognises them as subjects and helps understand their role in the production of meaning. The collaborative practices I have shown in this chapter underscore this and highlight people's role as active agents in the context of computed sociality.

Chapter Eight: Negotiating Clashes of Reality With Unknown Interlocutors

This chapter explores participants' capacity to act towards computational surveillance in relation to their own understanding of reality and explores its motivations, modalities, consequences and limits. It constitutes the concluding empirical chapter in this thesis and is based on the groundwork which the preceding empirical analyses have provided. The first empirical chapter (*Chapter Five*) facilitated an understanding of people's complex attitudes and experiences of surveillance between care and control, necessity, risk and avoidance. *Chapter Six* and *Chapter Seven* focussed on the aspect of computation in surveillance, in particular how people encounter generally invisible processes of computational surveillance in everyday life, and their communicative practices of structuring these encounters. One chapter explored this issue from the perspective of individual agents, whereas another detailed the collaborative efforts of decoding the presence and modus operandi of computational surveillance. While these chapters were narratives in their own right, they also were preconditions for understanding the possibility and practice of negotiating clashes between people's own, and the computational interpretation of reality. They provided a wider context of the necessity to act in this manner, and the complications involved. Agency is a broad term. Following the theoretical framework and empirical analysis thus far, this chapter is specifically concerned with people's ability to shape how computational surveillance perceives and calculates them. It remains open to incorporate different modes and motivations of participants' acts, from resistance to complicity in co-engineering of their own exposure. By proxy of this theme, the chapter incorporates broader questions around the general ability to act towards computation and ultimately the role of human agents in a computed world, that initially surfaced in *Chapter Six* around the imperative of reflexivity and rationality. Below, I re-introduce the main theoretical concepts which inform this chapter and outline its argument.

At the heart of the chapter are the concepts of visibility, glitches, and reflexivity. To recall, in the theoretical framework outlined in *Chapter Three*, I identified these concepts as cornerstones for the capacity to act. Firstly, I have used the notion of visibility to denote people's perceptual and cognitive barriers in querying computational surveillance, and to understand agency as making visible the illegible and incomprehensive mechanisms that

underpin a computational logic. I have also stressed that while human agents struggle to render computation visible, computers look back and categorise and calculate them. In this chapter, I use the notion of visibility in these two ways, connected by what Goffman (1971) calls 'relations of visibility'. I am focussing on how people make visible computational interlocutors with the objective to influence how these interlocutors 'see' them, and how they mould their appearance accordingly. Secondly, I understand glitches as an updated concept emerging from Berger and Luckmann's ([1966] 1991) notion of dissonances. Berger and Luckmann distinguish between two types of reality, or explanatory frameworks for how the world operates. Subjective reality refers to the world of individual, lived experience. Objective reality has little to do with established notions of objectivity as unbiased or infallible and instead refers to the institutionalised, naturalised world in which people live and which they take for granted. As objective reality is a consequence of the abstraction of human acts over time, subjective and objective reality are interconnected. Usually, they are in tune. However, these worlds can become misaligned, causing clashes, or dissonances, between subjective experience and the institutionalised representation of the world. Objective reality here stands for the computed world, which uses inferences about people to create social facts. Glitches occur when discrepancies between subjective, human logic and a computational logic reveal themselves. They are fissures and cracks in a usually coherent universe of reality. These glitches create a need and space for people to act towards computation. Lastly, reflexivity is a concept from Lash (2005), who argues that in order to challenge computational agents, people must act as if they were like them and hence adopt an ever questioning, rational and reflexive logic.

This chapter embeds these concepts in a symbolic interactionist framework informed by Goffman (1971; [1959] 1990; [1967] 2003) in order to understand how human agents set up a framework to act towards computation by establishing a social situation, how they consider assumptions about computation to characterise their interlocutors, and how differences in power determine whether acts are carried out on the front stage, or the back stage.[41] The notions of interface and infrastructure that further informed the theoretical framework also resurface in this context. In this discussion, a further extension of Kallinikos and Tempini's (2014) discussion of computed sociality becomes possible. In

[41] As I am using 'back stage' in the sense of Goffman's concept, I follow his spelling instead of the common English language spelling 'backstage'.

Chapter Seven, I have shown that computed sociality also encompasses the construction of intersubjective common sense between human agents that is about computation, but negotiated outside of computational operations. Here, I demonstrate that people also interact with computational agents directly, extending the intersubjective construction of meaning from relationships between human agents to human-machine relationships. The case study of individual representation, or how computational processes frame people, provides a contained field for exploring this communicative constellation.

The chapter begins by developing a typology of glitches in participants' lived experience. It argues that people strive to overcome those glitches by negotiating their appearance vis-à-vis computational agents. Drawing on Goffman, it frames computational agents as unknown interlocutors whose unclear shape and motives complicates interaction and defines relations of visibility between interactants. Under these conditions, this chapter documents three types of acts through which participants negotiate their representation by computational interlocutors. Some of these only take place on the interface of the screen and disregard deeper engagement with a computational logic, whereas others delve deeper into the workings of computation. However, despite this plethora of practices, this chapter stresses that people's act towards computation are riddled with failures and omissions. It concludes that participants are far from hyper-rational and ever-reflexive agents, and highlights that the realisation of their fallibility gives rise to a redefined sense of self-worth and aspirations of character in the context of a computed world.

8.1. Understanding Glitches

Pointing to her *Facebook* newsfeed, Laura, a student in London, complained:

> [8, 01] It's always this guy here. I don't even know him that well, but whatever he posts, it always pops up. And like here, when I click on my friends' profile here, what she posts, it's not there [DK: in the newsfeed]. So I have to check her profile, I mean if I want to see...stay up to date."

For Laura, it is evident that *Facebook* curates the activities she gets to see in her newsfeed. But *Facebook*'s filters do not reflect what is important to her. The person who keeps reoccurring in her newsfeed is a far-flung acquaintance that she has only met at a few parties. Her best friend instead hardly features at all in her newsfeed, a situation that she finds unacceptable:

[8, 02] "To be honest, I want to decide for myself how Facebook filters my newsfeed, it's my life after all and I should be the one who decides what I get to see, like what my real friends are up to and also what friends I get to see, and not Facebook."

Facebook's apparent idea of Laura and how she sees herself were out of sync. Laura encountered a dissonance between objective reality, or how inferences from her digital presence have become institutionalised as a social fact by computers, and her subjective experience. This dissonance is a glitch that reveals a flaw in *Facebook*'s logic. In contrast to a software crash or a bug, Laura did not encounter a technical glitch, but a glitch in the production of meaning. As computers increasingly constitute the social world, glitches also refer to slippages, or mistakes, in how computers understand the world. Just as technical glitches often result from human-machine interaction, such as user input that a given software cannot cope with, these social glitches are produced in interaction between a computational and a human logic. These glitches then are not 'hard' operational failures, but 'soft' glitches that are constituted by discrepancies in judgement and interpretation.

Control about what is relevant in her life had been taken from Laura, and there was no straightforward way to reclaim it. Yet Laura had no intention of settling with this situation. Although a computational logic is usually invisible and curtails the ability to act towards it, Laura did not accept simply being at the mercy of flawed inference. Instead, she expressed intention to correct the glitch and impose her subjective experience onto her objective representation. Such glitches are commonplace, and like Laura, participants see themselves as agents who strive to overcome them. While these glitches often are highly specific and personal, they can be categorised into three types; (1) naïve inferences, (2) normative clashes, and (3) computational superiority over subjective experience. Below, I draw on select participants' narratives to illustrate this typology of glitches.

8.1.1. Naïve Inferences

Glitches are particularly pertinent in backlashes against the way information on the web is personalised. In these cases, a computational logic is perceived by participants as naïve and simplistic compared to the complex, multi-faceted and rich subjective experience. I illustrate this with the help of Dennis, a student from Germany, and Stuart from London. When I joined Dennis in front of his computer, he pointed to his *Facebook* newsfeed and complained:

[8, 03] "Well, how this is selected, always, like this friend, as if it's stuff you have to see and the other stuff is being left out – that doesn't make any sense. They select it; well, I mean they don't show everything that everybody says, that would be too much with – how many do I have – well, 328 friends." [DK: translation from German]

Such disagreements are not confined to *Facebook*. They also occur other SNS, on retail sites like *Amazon*, on music streaming services. Many participants also bemoan the naïve inferences which targeted advertising makes about them, such as adverts reappearing for a product they have already bought. Instead of resisting being tracked at all, many participants suggest that computers should 'listen in' better. Stuart, whom I interviewed in his student flat in London says:

[8, 04] "Sometimes I am on Amazon, and I think - really? Is that what you are recommending me? You don't know me at all, do you? Ok, sometimes it is really useful, I have it mostly with books. But I bought some DVDs. And the movies Amazon tells me to buy are usually pretty shit. So thanks for that. I could pick better movies myself without these recommendations. I mean, some websites now ask you whether it was helpful, a recommendation. And you can click yes or now, so have your say in a way. Like everyone should be able to have a say. So yes, what they think I like, it's just bollocks really."

The world of computation is opaque to most people. This is reflected in how Laura, Dennis and Stuart cope with dissonances. They acknowledge that computational forces are at work beneath the interface. But clashes between objective and subjective reality entail an asymmetry of power. While a computational logic can transgress into the realm of lived experience, participants struggle to systematically dismantle the computational logic. Laura, Dennis and Stuart circumvent this asymmetry by choosing a language of personal experience over technological concepts. While they are unable to criticise lines of code or algorithmic processes, they can challenge computed outcomes directed at themselves by proxy of their self-knowledge. By asserting their subjectivity, they convert the computational logic into an object of mockery. Other participants have shared similar experiences. They show that computation is not necessarily a mystical, or scary phenomenon due to its impenetrability. While participants may be upset by the outcomes of wrong, simplistic calculations, the fallibility of computation and their ability to call out computational flaws equips them with a comfort of power amidst a computed world.

Arguably, challenging inferences in this way says little about participants' power of agency towards computational forces. Poking fun at hilarious book suggestions on *Amazon* is not a form of code literacy (Hayles 2005). It remains open whether computation really works in the way that participants observe through being obviously

misrepresented. Nevertheless, these examples underscore that people as lay actors have the possibility in principle to dissent from computed outcomes.

8.1.2. Normative Clashes

The glitches that Laura, Dennis and Stuart encountered refer to a specific manifestation of a computational logic. In their accounts, *Facebook*'s and *Amazon*'s curation mechanisms do something rare: they unfold into the realm of human experience where they can be grasped. In this state, they seem to stand still and appear limited in scope and fixed in time and space. This allows participants to identify a specific disagreement. They relate a snapshot of the computational logic to the full richness of their own, subjective experience. But there is a much wider, more diffuse sense of disagreement based on general suspicion instead of actuality. Participants have a general risk awareness associated with surveillance and computation that stretches from the loss of privacy, social stigmatisation by peers, disadvantages in future employment, general fears of social consequences to inaccurate representation. Attached to those concerns are expectations of how computation should interpret their personal data and represent them as data subjects. Glitches emerge when these expectations clash with how participants believe they are de facto computed. These glitches are situated everywhere and nowhere. Participants have a diffuse sense that they exist, but struggle to pinpoint them. James the barista highlights:

[8, 05] "Everybody is after your data, and if you don't stop using the internet, they will get it. But it is not really clear what happens once they got that data and that really worries me like what that says about you, and you don't even know that, and it's going to hit you years later."

Similarly, Paula from Germany has a general sense of disagreement with computational surveillance that like Laura, she intends to overcome:

[8, 06] "You can't really know who has what data about me, I think. Either you adapt and say, 'screw it', or you do something and try to protect yourself, so you'll be seen as whom you want to be seen yourself. Just name, or also address, or some random clicks you have made or some bullshit to fake everything." [DK: translation from German]

Paula finds it impossible to know exactly how society is computed. Yet she still thinks that people can co-shape their computational representation and thereby overcome glitches as normative discords between subjective experience and objective reality. This can either be through reconciling subjective experience and computational reality by explicitly disseminating specific information about oneself to set the agenda of

calculation, or to prevent glitches from happening in the first place by starving the computational logic of meaningful input.

8.1.3. Computational Superiority

In a cafe in Erfurt, Germany, history student Enrico is after something different. Balancing his laptop on his knees, he is logged into *last.fm*, an online recommendation service for music. In front of him, he sees the result of a surveillance architecture he has helped create. Enrico listens to nearly all of his music on his PC, which boasts a collection of thousands of songs. *Winamp*, the media player he uses to play his mp3 files, is equipped with a plug-in which Enrico has deliberately installed. It sends information about whichever song he is currently playing to his *last.fm* account. With a sense of pride Enrico showed me that this 'scrobbler' had already recorded a history of 8,654 listening events:

> [8, 07] "So here you can see what I've been listening to. Really amazing. Here you have listed all the songs and the top bands. I always like to think of myself as an indie guy; my favourite artist is Bon Iver. But the coolest thing is, here I can see from the listening statistics that recently I've been listening to Mumford & Sons much more often. So actually, that would be my favourite band. That's pretty heavy, you think, ah, yes, last.fm knows me better than I do myself somehow. And as I said, here you can see what kind of recommendations they give, like similar to Bon Iver, or here, also cool, The National." [DK: translation from German]

When Enrico lets *last.fm* measure and quantify his everyday music consumption and tastes, he engages in 'everyday metering' (Pantzar & Shove 2005), a practice that is commonly understood as "collecting, collating and analysing minute data and providing feedback on how to better care for one's self" (Whitson 2013: 167). While Enrico finds *Amazon*'s purchase recommendations simplistic, there is nothing naïve about *last.fm*'s inferences. They provide Enrico with information about his listening patterns and make recommendations he had not thought of himself. Enrico's case is unlike the other stories from participants discussed so far, where purpose and meaning of surveillance were not evident. For Enrico, it is entirely clear what data *last.fm*'s algorithms are processing and how they are generating outcomes. *Last.fm*'s surveillance infrastructure is laid open in front of him, from the scrobbler that collects data, its aggregation and analysis on *last.fm*'s servers, to the cross-referencing with data from other users, to ultimately curated list of recommendations. *Last.fm* describes itself as a system and Enrico can validate its operation and logic. Computation ceases to be a mysterious force and becomes a trusted tool for self-discovery.

Enrico's story is a special case. He does not encounter a glitch where computational inferences fail to accurately represent him. On the contrary, in the particular *last.fm* context, the idea of a glitch itself is categorically impossible for Enrico. In his mind, *last.fm* is infallible because it knows his music tastes better than he does. Enrico does not want to influence *last.fm* to better reflect his own subjective experience. On the contrary, he feeds *last.fm* ever more data about himself so that he can adjust his own behaviour. Glitches also are not an unintended consequence of exposure to surveillance. Enrico is deliberately exposing himself to *last.fm*. He wants to revise his perception of self as proposed by *last.fm*, and not impose his perception of self on the logic of computation. Such self-exposure to computational analysis echoes the concept of 'quantified self', fuelled by the proliferation of consumer devices such as fitness trackers (Wolf 2010). Enrico sees an absolute techno-truth in *last.fm* and glitches cannot come up because he does not take his own, subjective reality for valid faced with the power he ascribes to *last.fm*.

But Enrico's perceived gains from *last.fm*'s computational authority also suggest that glitches are not necessarily limited to negative consequences of surveillance and computation. For instance, Laura's criticism of the *Facebook* newsfeed was neither sparked by privacy concerns, nor by another negative sentiment towards surveillance at large. Her motivation was much more mundane: addressing a personal inconvenience. Laura just wanted to be up-to-date on her friend's whereabouts. The relationship between people and computational surveillance then is not always about grand narratives of privacy, intrusion and threat, but much more nuanced.

8.2. Interacting with Computation

Noticing glitches usually coincides with the ambition to overcome them. Participants consider themselves as interactants who actively negotiate their computational representation, either by intervening in the objective reality of computation or by letting such objective reality alter their subjective experience. As I have highlighted in the introduction to this chapter, this further expands the notion of computed sociality. While Kallinikos (2009) has outlined how computational processes render social reality, people's practices of interacting with computation show that reality is also co-rendered between human and computational agents. Human agents actively and consciously contribute to the construction of reality not just between peers as shown in *Chapter Seven*,

but within the computational domain and in relation to computational agents as well. However, their expressed intention to intervene in glitches alone says little about participants' actual influence on computation, and about specific practices of intervention. In order to explore this, some conceptual groundwork is required which I attempt in this section by drawing on frameworks of interaction proposed by Goffman. I illustrate my argument with the help of two participants, Laura and Freddy, and only occasionally make references to others. This choice is based on practical reasons for the sake of a coherent narrative and also to illustrate that patterns of interaction are complex within, and not just between participants.

8.2.1. The Possibility of Interaction

During our conversation, Laura stressed that *Facebook*'s decision to prominently insert a remote acquaintance into her newsfeed was not arbitrary. She remembered how she had previously clicked on some of the *YouTube* videos her acquaintance had been posting. Her own actions, that much she knew, must have triggered *Facebook*'s selection mechanism. This gave Laura an idea how she could possibly intervene:

> [8, 08] "For a while, I just clicked on my friend's profile all the time. Like, here [DK: Laura points on her friend's profile which is now on her screen], I went to her profile all the time, I mean not really to see what's new, just so Facebook knows I go there. And I clicked on tons of posts and pictures, and clicked 'like', I mean it was a bit stupid because there was no point really because the pics were all quite old and she probably thought 'what the hell', why is she liking random pictures all of a sudden."

Laura had no means to rewrite the newsfeed algorithm, to give it specific instructions, or to ask *Facebook* to change it to a more accurate representation of who she is. Instead, she believed to have found an angle to interact with *Facebook* by connecting the curation of her newsfeed to her own behaviour. To influence *Facebook*, she emulated the behaviour which she considered to have led to its assumptions in the first place. By clicking on her real friend's profile, Laura assumed that she would establish a connection with *Facebook*'s logic. She expected *Facebook* to recognise her clicks as a signal to make her real friend more prominent on the newsfeed. Without altering the computational logic as such, Laura hoped to teach it. She assumes that the computational logic is already present, perpetually analysing her clicks and feeding back curated visual information to her on that basis. Laura considers herself as making contact, and as initiating a negotiation. *Facebook* is always already looking at her, but she has to actively change focus to look back. When in front of a computer, her attention usually is focussed on what is going on

right on the interface of the screen. Now, her attention moves behind the interface of the screen and the computational logic becomes her primary interlocutor. Her actions may still take place on the screen, but it is not the buttons and photos on which she clicks on that matter. These are just acts to reach the computational logic behind it.

Freddy, a young teacher, wants to intervene in his computational representation more widely. He has a diffuse sense of disagreement between his own privacy concerns and the data analysis practices by online companies. I sat next to next to Freddy in his flat in Germany, which he shares with his girlfriend. Freddy booted up his computer and showed me various online profiles, from *Facebook* and *StudiVZ* to a discussion forum for metal music. Freddy has a strict regime about his account names:

[8, 09] "Well, so here on Facebook, that's not my real name. My first name is correct, but the rest is fake; and religion, Buddha and stuff and hobbies, that's all bullshit. And here, at StudiVZ, one sec… [DK: Freddy logs out of his Facebook account, closes Internet Explorer and opens StudiVZ in Firefox] well, here I also have the same first name, but the last name isn't completely fake. See, the first letters are correct. And on the metal messaging board I have a metal nickname, that has nothing to do with reality." [DK: translation from German]

For each online service, Freddy uses a different username. He also alternates web browsers and assigns a different one to each SNS. Several participants pursue similar practices, but Freddy is particularly meticulous. When I inquired about his social media use after the think-aloud protocol, Freddy did not refer to *Internet Explorer* or *Mozilla Firefox*. Instead, he calls them the '*Facebook*-Browser' and the '*StudiVZ*-Browser'. Each SNS account is also associated with a distinct email address, although he uses the same email address for *StudiVZ* and the online music forum. Using more addresses would just not be practical, he claimed and continued to highlight that neither email address contained his real name. As our conversation continued, Freddy moved effortlessly between browsers, underscoring the apparent ease by which he keeps the contexts of his online activities apart:

[8, 10] "I don't want to be tracked by everyone everywhere; if I can't completely avoid it, well, like this I can at least contain it, and they can't infer so much about my personality, and the information is all wrong anyways. So I make extra sure this way because I'm feeding the companies that do stuff like this with crap." [DK: translation from German]

Freddy does not see himself merely subjected to the invisible forces of online surveillance, but as an active agent who can at least co-shape and negotiate his online representation. Both Laura's and Freddy's example show that participants believe that they can gain access to a computational logic without coding or other expert skills. Such

interactions do not happen in isolation. Laura probed into *Facebook* in the context of her desire to see more of her friend, and Freddy's interactions are embedded in his wider internet use. Both examples also shed light on the dynamics of interaction. Laura's case highlights that participants' see the computational logic as a particular kind of interlocutor. Freddy's defensive acts illustrate that relations of power are part of these interactions.

8.2.2. Unknown Interlocutors

At its most basic, participants' interventions in glitches can be understood as practices of impression management (Goffman [1959] 1990). Participants want to establish and maintain impressions that are congruent with how they intend to be perceived. But this impression management faces complications. In a previous chapter, I have highlighted that an asymmetry of expressive information between participants and computational practices is a key factor behind the perception of surveillance as risk. This asymmetry also structures participants' interaction. A far cry from the 'special mutuality' that characterises face-to-face interaction for Goffman, participants struggle to identify their interaction partner in the first place. In face-to-face interaction, interactants have the same amount of expressive tokens available about each other. Yet while a computational logic can analyse the world that participants inhabit, participants themselves struggle to grasp their computational interlocutors - are they present at all in a given moment, what is their aim, how do they perceive participants, how does the computational logic react to participants' attempts of interaction?

Participants engage in interactions in darkness. Occasions in which a computational logic reveals at least some expressive information and provides communicative feedback are scarce. In most cases, participants are left to speculate about their interlocutors. 'Discrepant roles' (Goffman [1959] 1990) become a structural feature of the interaction. These discrepancies denote aspects that interactants consciously or unconsciously hide from others, be it as a normative feature of their role or by virtue of personal decision. For instance, in theatre, performers have access to both frontstage and backstage areas, while members of the audience can only see the front stage. This means that some possess special information and knowledge about a social situation that is not shared with others. Goffman sees discrepant roles as potential threats to an interaction because they can cause breaks in its order, or challenge it entirely. In the case of computational interactants, role

discrepancies are so prominent that participants are unable to define the social situation at hand in the first place. According to Goffman, a social situation is characterised by interaction rules. But how to define interaction rules for a social situation in which one interactant is conceptually unknown and which may not even have a precedent that participants can use as a template? Negotiating glitches are not normatively defined situations such as two people meeting for a coffee.

In the absence of guidelines, participants look to establish interaction rules on their own initiative. For instance, when Laura repeatedly clicked on her friend's *Facebook* profile, she did not merely attempt to influence how *Facebook* perceives her. It also was a proposition: 'if I do this, you acknowledge my action and revise what you show me in the newsfeed'. Participants also try to glean such rules from their computational interlocutors. When participants speculate how a computational logic works, they also hypothesise which rules govern them, and how they themselves could communicate within these rules.

But participants do not know whether their proposed interaction rules are accepted, or whether they have correctly inferred their interactants' logic. In the absence of a feedback loop, Laura cannot be sure that clicking on her friend's *Facebook* profile had any effect:

[8, 11] "Not sure if it did anything. I think I see her more often now in the newsfeed, so yes. I think it must have had an effect. Yes, clearly. But I can't really measure it and also, I think I now see everyone more often, so maybe Facebook made some changes as well?"

Similarly, Freddy intersperses his narrative with qualifying statements, such as 'hoffentlich [I hope]' and 'eventuell [maybe]'. I hence propose the term 'unknown interlocutors' for computational agents. These are interlocutors that neither reveal themselves, nor provide feedback throughout an interaction about its rules, its trajectory and its consequences.

8.2.3. Relations of Visibility

These obstacles lead to the question how participants are positioning themselves towards unknown interlocutors when they seek to establish an interaction. Goffman's ([1959] 1990) notion of 'protective practices' provides a starting point. These are practices of impression management emerging from perceived differences in power. In an omniscient gaze, computational surveillance has already established a connection to human agents. But participants still need to creatively find a way to establish a relationship in the first place, either at a given moment in time like Laura, perpetually like Freddy, or in a specific

context like Enrico. Protective practices thus are launched from a position of inferiority and recall de Certeau's (1984) notion of tactics. De Certeau opposed tactics and strategies, whereby strategies are linked to structures and institutions of power that define the context in which people live. This applies to the realm of objective reality computed by institutional agents of surveillance like *Google* or *Facebook*. Tactics are responses to these strategies by those who are subjugated to them, such as the walker in the city or users of online services.

Yet the notion of tactics alone is too limited to frame participants' practices. Participants differ in the knowledge of tools and practices that can help understand computational agents. For instance, Laura relies on her common sense, whereas Freddy draws on software. Some participants are also more systematic than others: Freddy has a meticulous plan that spans across all his online activities, whereas Laura's practices are focussed on a single situation. Participants are located across a spectrum of practices, where some exhibit traits of strategies rather than tactics. This requires a concept that recognises but does not confine itself to the dualistic nature and prescriptive politics of tactics and strategies.

The notion of tactics is also too constricted in its motivations. De Certeau sees tactics as defensive acts, directed against strategies of power. But for participants, tactics towards surveillance are not necessarily about resistance. As Lyon (2007) has posited, surveillance is neither inherently good nor bad, and participants' acts reflect this. Some practices are geared towards escaping the gaze of surveillance, such as Freddy's elaborate web browsing routines. Other practices aim at enhancing exposure and making sure that computational agents can capture as much personal data as possible. Again others are a hybrid. While Laura wants to resist *Facebook*'s specific curation of her newsfeed, she is not opposed to curation on the *Facebook* newsfeed per se. Participants' attitudes to computational agents escape a binary of good and evil. While this becomes most apparent in Laura's example, other practices also are structured by similar tensions. At face value, Enrico's voluntary exposure to surveillance may be considered as an endorsement of surveillance. Yet for him, matters are more complicated. He chose to open up to surveillance because he considers a full dataset about himself less biased than a selective one, where the scarcity of data would lead to false conclusions about him. Surveillance

remains to have negative connotations for him, and the attempt to fully expose himself is a means to mitigate them:

> [8, 12] "I tell you, before I get wrong recommendations, because they don't have enough data about me and make the wrong conclusions about who I am, I rather tell myself, I let everything be recorded 100%. This is all accurate then, because that is 100% me. So I prefer 100% instead of 50% or 60% [...]." [DK: translation from German]

A concept that captures participants' complex relationship to unknown interlocutors then also needs to move beyond a simple dichotomy of resistance and complicity. The notion of visibility is able to accommodate these concerns. It remains open to both enhancing or reducing exposure to surveillance, as well as to resisting or complying with computation. It also encapsulates both the human senses through which people act in the world, and the operational mode of computation as 'seeing without eyes'. The concept of visibility echoes participants' own terminology, who are concerned about 'being seen' by computational agents. Lastly, the notion of visibility fits into Goffman's framework of interaction, who considers interactions as relations of visibility (Goffman 1971).

In the remainder of this chapter, I will systematically analyse participants' relationship to unknown interlocutors as relations of visibility. The following sections will map relations of visibility on a spectrum that defines where participants address computational agents - in the realm of participants' sensory experience at one end, and in the realm of computation at the other. In analogy to the theoretical framework of this thesis, I call these endpoints interface and infrastructure. 'Interface' denotes practices that take place on the front stage in Goffman's ([1959] 1990) sense. They are enacted and geared towards the visible layer of the computer screen with no specific consideration of what is going on behind it. 'Infrastructure' refers to backstage practices that attempt to lift the curtain behind the interface. While they may still be enacted on the interface of the screen, in their focus, infrastructure practices leave the realm of human sensory experience behind to tap directly into the invisible logic of computation. This spectrum then provides an understanding of how far people's acts extend into the computational domain. It also documents the patterning of computed sociality between highly computational and non-computational aspects of active human involvement.

For reasons of legibility and clarity, I use the term 'appearances' when it comes to people's management of their own representation towards computation. I use the term

'visibility' to denote practices and mechanism of interrogating interlocutors, both human agents interrogating computational agents, and vice versa.

8.3. Negotiating Appearances

In order to explore practices on the spectrum of interface and infrastructure, I use three broad categories that represent different bands of practice in this spectrum: (1) data scarcity, (2) obfuscation, and (3) modification. These bands refer to modulations of interface and infrastructure and progressively move from practices on the interface to those leaning more towards infrastructure.

8.3.1. Data Scarcity

Practices of data scarcity are about limiting the personal footprint on the internet to starve computational interlocutors of useful information that they can use to compute human agents. They are protective measures to shield subjective experience against being translated into the objective reality of computation. These practices come in various forms. They range from practices which only take place on the interface, over attempts to interact with the infrastructure of computation directly, to measures of using software proxies to handle the interaction.

Interface Practices

When I asked Rebecca about the lack of information on her *Facebook* profile, she responded:

> [8, 13] "No data for me is better than wrong data, or like data where you don't know what's happening with it. So I rather have as little as possible about me on the internet." [DK: translation from German]

Her presence on *Facebook* only contains a few travel images, a tightly regulated friend list, and lacks information on hobbies, family members, schools or university, and even status updates. Like many participants, Rebecca is concerned about leaving traces that can be analysed. The only way that the politics student can think of avoiding the grasp of surveillance is to reveal as little information as possible:

> [8, 14] "Well, I don't know….as soon as the data is out there on the internet, you can't do anything about it anymore. Whom should I call to ask 'hey, delete this please' […] and then who knows what is happening with my data and it goes to Google, or the BKA [DK: Federal Criminal Police Office] and will be manipulated, I don't know. And I do not have any picture of me, on Facebook at least. On StudiVZ I have a photo album about New York. But this does not really bother me because StudiVZ can sell this on to whomever, they will not

> learn anything about me personally, it is just buildings, Ground Zero and stuff." [DK: translation from German]

In Rebecca's mind, glitches between her subjective experience and inferences by computational agents cannot be corrected, only avoided. Her approach represents a strand of practices focussed on data scarcity that is geared at producing as little data as possible for computational analysis. Such tactics are commonplace. Sarah, who is Rebecca's fellow student from Erfurt, follows a similar approach. She calls it a 'profile diet':

> [8, 15] "Yes, there actually is quite a lot what you cannot see. I am doing a profile diet so to speak. My contact details are limited anyways. Yes, what do Apps and Services learn about me? I don't really have any Apps or stuff like that, well I really want to limit what I feed Facebook with, that's the only way for me." [DK: translation from German]

Both students feel unable to negotiate their appearances. They lack a hypothesis about how computational agents operate and hence are unable to establish a conscious interaction. To overcome this interactional barrier, they treat *Facebook*'s computational logic as if it was just another *Facebook* user in flesh and bone. They reduce personal information, limit the volume of photos and if they upload photos at all, ensure that they are as non-descript and impersonal as possible. This echoes the measures that users take to curtail what human interlocutors can discover about them online. Sarah and Rebecca try to humanise computational agents and assume that their ability to 'see' is impaired in the same way as that of human agents.

Sarah's and Rebecca's approaches to *Facebook* are examples of interface practices. Negotiating appearances takes place in a framework that begins and ends on the visual layer of the *Facebook* user interface. It does so in a double sense, which situates their practices at the far end of interface practices. Firstly, interactions with algorithms are confined to the affordances that the *Facebook* user interface offers, such as making clicks, sharing pictures and other content. The location of interaction is the interface. Secondly, Sarah and Rebecca equip their computational interlocutor with the same abilities and constraints as human interlocutors. They do not lift the veil of the interface to peek into the algorithmic logic. The conceptual framework of interaction then also is located on the interface.

Thinking About Infrastructure

For Mark, data scarcity comes with behavioural constraints. As much as he would like to, he simply does not use the 'like' button on *Facebook* and refrains from commenting on friends' posts:

> [8, 16] "Well, it may sound awkward...how do say...I just don't want Facebook to assume that when I like a post, I also like that person, and they get recommended as a close friend or something that's always popping up. Or that, like, I have over 300 friends, and I also do not want Facebook to know my best mates, like the 5 to 10 people I really care about because they can track that who I communicate with. So I make a note in my head 'like'. And sometimes in the pub, I say: 'nice picture' or something and we talk about it."

While Mark compensates for his constrained use of *Facebook* through face-to-face interaction with peers, others do not have such alternatives. In London, Katy told me that she avoids certain websites altogether. She would just not be able to control how data on her is collected:

> [8, 17] "I mean I do avoid dodgy websites. [...] My friends are on these file sharing sites, but I went on their once with my old computer. You really feel with all the pop-ups and the general look and feel that they snoop you out. Like this video player wanted to install itself and I could somehow not cancel it. So you kinda know that they want to suck your data and enter your system when you are on there, so I do not go there at all anymore."

Mark and Katy make parts of their online behaviour dependent what they believe goes on behind the interface. Like Sarah and Rebecca, they struggle to establish communicative access to negotiate how they appear to an unknown interlocutor. But their rationale is different. In a basic way, they anticipate and conceptualise unknown interlocutors and account for the invisible logic behind the interface in their tactics.

Software Proxies

In the examples so far data scarcity meant that participants limited particular online activities. Yet once participants engage more deeply with the infrastructure of computation, behavioural limitations are replaced by other approaches to data scarcity. Carrying his laptop everywhere he goes, Dave rarely misses a chance of being online. He may not have a smartphone, but when he leaves his home in the morning after checking the online news over breakfast, he flips shut his laptop, puts it in his bag and heads to university or the gym where he works. In the lecture hall, he reopens it and starts it up yet again in the library, before finally continuing to work and surf the internet at home. These intervals inform Dave's practices of disappearance. When Dave opens his laptop at a new location, his first destination is the preferences menu in his web browser:

[8, 18] “Well from home I go to the library and start up the laptop and before I go online, I first of all delete all cookies, and when I wrap up, so when I go home and start up the computer again, then I delete all the cookies from the session in the library. Always remove the accumulated waste from before so to speak. Yes why, to start again, a new sheet of paper, so that my entire history will not be scanned.” [DK: translation from German]

Similarly, Amanda clears her browser cache after every browsing session, and she even resets her entire browser to default. Every time she shuts down her computer, saved passwords and custom configurations are lost again. But re-entering the internet every time as an apparently blank slate outweighs these hassles:

[8, 19] “I don't have any fancy settings, I am a pretty basic user really. I just want to make sure all data in Safari is gone so it’s all clean for next time, and nothing spyware style stuff is on my computer and does some bad shit, like that. Does that sound weird? I also am a clean freak generally so maybe that's also why.”

Both Dave and Amanda stand for a strand of participants who are convinced that they inevitably create data trails. Instead of trying to prevent the impossible, they want to remove the footprints that they have involuntarily created. These participants forego practices of self-limitation that curtail the range of online activities in favour of practices that address the consequences of their behaviour. The spatial and temporal boundaries of their internet sessions act as intervals in which they intend to reset their data trail. According to their rationale, computational surveillance interprets them with growing ease the longer they surf the web, melting away their anonymity until the next cookie sweep or browser reset. For them, data scarcity is not a fixed status that can be maintained, but a condition that must be continually restored. In contrast to those participants who refrain from online activities, these participants directly intervene in the computational infrastructure by limiting its ability to calculate them.

More technologically savvy participants draw on software to maintain a constant level of data scarcity through interventions on the infrastructure level. In a previous chapter, I already introduced Richard. He uses *Ghostery* to identify occurrences of surveillance through a pop-up window which lists all advertising trackers and other monitoring tools on a website and blocks all tracking cookies. Other participants draw on a whole range of tools. When I leant over Andre’s computer in his Aachen apartment, he proudly explained his setup:

[8, 20] “Here I have Norton, Ghostery as well, and wait, here is AdBlock. Once I had Avira but I now deactivated that because of Norton, which is supposed to be better in the end [...]” [DK: translation from German]

Andre wanted to take every chance he could to protect his data from being scrutinised. Software was the best way to prevent surveillance:

[8, 21] "By yourself, you can't do anything. I am not a programmer and even if I was, what Google or others do, and you don't even know those others, that wouldn't help anyways. I think even programmers use such tools." [DK: translation from German]

Both Richard and Andre do not consider themselves as technical experts, which they feel that limits their ability to act. While some academics might consider Rushkoff's (2011) *Program or Be Programmed* as polemic, Richard and Andre subscribe to this logic. Limited in skills, they still think that they need to intervene on the level of infrastructure. Unable to establish a direct interaction with computational agents, they rely on software as a proxy. When we sat down to navigate to his favourite websites, a *Norton* pop-up window appeared on Andre's screen:

[8, 22] "Yeah, yes, I click yes, or no. So here it's yes, but I might also say no, usually depends on trust really. When I don't know, like what the site is... Norton does it, I trust it." [DK: translation from German]

Andre assumes that the software will act in accordance with his own values. This is echoed by Christina who uses *AdBlock* at work as a magazine journalist:

[8, 23] "AdBlock, like the name suggests it. It does good things, blocking ads and that's what I want. It is how I feel about ads."

In these cases, participants use software as advocates of their subjectivity. They may not know exactly how these tools function, but they believe that the software acts on their behalf. Participants may not be able to read the logic of computational surveillance, so they use software as 'envoys' that can relate to otherwise unknown interlocutors and take over the task of establishing a social situation. In their minds, these software tools place them on an equal footing with a logic they do not understand. Software then is a way to overcome discrepant roles between interactants by proxy.

Synthesis: Data Scarcity

As this section has shown, practices of data scarcity can be structured on a spectrum of interface and infrastructure. It began with behavioural limitations at the far end of interface practices. Further examples moved progressively towards a stronger consideration of infrastructure. But there is no simple dualism between interface and infrastructure. Interface practices can be further differentiated by considering the *location of interaction* and the *participant framework of interaction.* Whereas the location of

interaction in all examples was the interface, the participant framework of interaction, how each participant imagines the interaction, varies. It can exclusively relate to the interface, but it can also consider infrastructure. Practices that consider infrastructure are marked by a struggle to establish an interactional relationship with computation.

Participants' experiences contain a sense of tactical play with unknown interlocutors. This tactical play echoes the idea of role discrepancy in two ways. Firstly, hiding from computational agents is a token of power for participants. By withholding their data, participants strive to become unknown interlocutors themselves. Being unknown can only be an incomplete enterprise. Participants realise that they cannot transgress into the world of computation, whereas computational agents allow inferences about participants. Participants strive to be unknown in the sense of removing individual attributes from computational grasp. Secondly, participants seek to overcome role discrepancies through the use of software. Tools such as *Ghostery* and others are proxies through which participants gain access to a computational logic, counteracting code with other code. Through data scarcity, participants try to overcome discrepant roles by making computational agents as weak as they are themselves in understanding their interlocutor. In contrast, the use of software is an attempt to equip participants with the same attributes of power that they bestow on computational surveillance. In both cases, practices of data scarcity then are attempts to change the power balance in interactions towards interactional equivalence between human and non-human agents.

8.3.2. Obfuscation

During the First World War, the British Admiralty and US Navy were alert about the deadly capabilities of German submarines. The clear silhouettes of their ships on the horizon presented ideal targets for these submerged hunters. Struggling to protect their vessels from enemy view, they adopted an unconventional measure. Instead of painting ships in particularly unobtrusive ways, visually strong, highly abstract schemes that were often in bold colours and reminded of cubist paintings, were placed on their hulls. Concealment was replaced by confusion in what came to be known as 'dazzle' camouflage. The dazzle pattern broke the regularity of a ship's outline, making it difficult for the enemy to determine its type, size, speed and direction. While this pattern could already confuse bare eyes, it was specifically designed to disrupt mediated observation through optical rangefinders, which determined an object by pairing two half images into

a single view. The dazzle patterns impeded the alignment of these two halves.[42] In order to interact with computational agents, participants engage in practices that resemble these wartime tools. Below I outline these modes of obscuring digital traces.

Software Hacks

Lars has a *Mozilla* browser plug-in that is unlike *Ghostery* or the other tools discussed so far. Instead of shielding his data and blocking cookie intrusions, it produces even more data. It constantly emits a stream of arbitrary search terms including, to Lars's bemusement, 'Britney Spears'. On the bottom of his browser, I saw a list of terms:

> [8, 24] "That's so funny, Britney Spears, here it is. Of course, I am not her fan, that's clear. I am not a little girl, but that's what you will think. Only data waste, nobody can figure out who I really am, because this is mixed with what I really do into some kind of broth and then Google probably asks itself what's going on there. " [DK: translation from German]

Lars believes that he can mask his intentions by producing data noise. Akin to a dazzle ship camouflage, he hides in the open and uses the additional data to confuse unknown interlocutors like *Google*. Such attempts to perplex computational surveillance are common. Luise, who shares a flat with several other students, pretends to be someone else on the internet every week. Compared to her flatmates, Luise claims to know fairly little about computers. Yet she speaks in a confident tone when she explains how Susanne, her flatmate responsible for all internet matters, tampers with their collective internet account:

> [8, 25] "Well, Google, they are known for collecting search queries and compile statistics on that and so forth, but I can…Even if they know it's me, via the IP-address... But at home, we have configured the IP-address in such a way that it always changes, so they cannot find it out ultimately." [DK: translation from German]

Susanne has edited the settings on the flat's internet router so that it changes a unique identifier, the IP address, on a regular basis, apparently making it impossible for unknown interlocutors to build a long-term profile of the flat's internet use. Luise trusts Susanne. She neither deletes any cookies nor tries to limit her data footprint. If anything, she feels more carefree because she believes that she is not traceable anymore.

Fake Clicks

In a Canary Wharf office, Joanna takes a different approach. Joanna is unhappy in her job as a legal secretary and just wants to get through the day. The location of her desk helps.

[42] See e.g. Behrens (1999) for a history of the dazzle camouflage and the role of artists in conceiving them.

It is in an isolated corner, shielding her computer screen from passers-by. Throughout the day, she has a *Facebook* tab open in her browser, and unless there is an urgent task that cannot be postponed, she checks the newsfeed, news websites or fashion blogs. Yet although she can hide her procrastination from colleagues, she is less sure about the IT department. There are rumours that her company scans employees' internet traffic. While Joanna does not know how this scanning process works exactly, she suspects that her procrastination could raise a red flag and has developed a way to trick the system:

[8, 26] "Facebook, when I am there I change tabs, and then I go to Google, and I type in some law terms...so I pretend that I'm googling work stuff, like I'm doing research. And then Facebook is still open, so I did not go to www.facebook.com again. Or like my fashion blogs. So I can just go back there and I guess it won't register."

At the other end of London, in a construction planning office, Jack has reserved such an approach for what he calls 'emergencies'. Referencing the famous Police song 'Every Breath You Take', he expects to be tracked continuously. While he is generally not concerned, his attitude changes in some situations:

[8, 27] "So embarrassing, but ok. One time you know, growing old and all that so I was looking at some anti-aging stuff, like on cosmetics websites and stuff. And I am a guy, and my colleagues always joke about this, like it's totally girly. And I was, searching, searching so that's basically all I did for a good two hours or so. And I did not want to get those ads for that later of course... And there's the whole thing about personal advertising now, and then when they come to my desk ask me a question and see the ad."

Jack felt trapped in gender stereotypes emerging from his behavioural data. Whether surveillance algorithms take him for a woman is of little concern to him. Rather, he worries that the consequences of calculation will surface to his co-workers. 27-year-old Jack works in an open-plan office and his colleagues frequently stop by for a chat, so any advertising would be for everyone to see. His concerns are not related to computation itself but arise from human peers who judge him based on computational inferences. To avoid being exposed, Jack randomly surfs to websites and arbitrarily clicks on adverts. He wants to dilute the analytical weight that an advertising algorithm would place on anti-aging products. Jack's example illustrates that practices of negotiating appearance extend beyond the realm of computation itself, and are intertwined with role maintenance towards other human agents.

Synthesis: Obfuscation

Probing into the computational logic is a core aspect of all practices of obfuscation. Participants formulate specific hypotheses about computational interlocutors and seek to

exert influence on an infrastructural level. This is different from the bulk of data scarcity practices, where computational principles largely remain abstract. In data scarcity practices, withholding data usually is associated with a feeling of being unable to intervene, and participants refrain from attempts of interaction. In contrast, practices of obfuscation demonstrate a much more intimate relationship with computation, where involved participants recognise and embrace its perceived logic. Participants proactively engineer possibilities for interaction. However, practices of obfuscation are also much narrower. They refer to specific instances and are not extended to surveillance across temporal and spatial contexts.

The difference between data scarcity and obfuscation becomes even clearer through the prism of interface and infrastructure. In the case of data scarcity, practices that consider infrastructure are often outsourced to software. But how *Ghostery*, *AdBlock* and other tools identify and block surveillance is not evident to participants. These tools are black boxes, and their use is fuelled by mere hope of success. Participants believe the software to be inherently good and to act in their interest. Software also features in attempts to obscure traces. But its use differs from tools for data scarcity. Consider Lars's software tool which emits false search terms. Like in Enrico's case of *last.fm*, where the computational logic explains itself, Lars can see how his software operates. By emitting random search terms that are visible in Lars's browser bar, the software unveils its logic of operation. It is a rather simple logic, where the software does in automated form what participants can conceptually understand and at least in theory, replicate manually.

Practices of obfuscation show how participants engage with computational infrastructure through their own acts. Prerequisite is a specific hypothesis about the logic that underpins unknown interlocutor's. Just as dazzle ship paintings were literally a surface measure directed at an underlying technology of interpreting visual information (the rangefinder), participants' practices of obscuring information target the computational logic that transforms data into information. In both cases, overstimulating the mechanism of interpretation shall transform it into a blunt tool by turning it against itself. The dazzle ship camouflage was an initially tactical consideration that turned into a minutely planned and exercised operation, and itself into a tool of power. As it was employed, it acquired more and more strategic, rather than tactical properties. The same is the case with participants' acts of obscuring information. These practices demonstrate a much deeper

engagement and reflection over specific instances of computation. They are meticulously prepared, and participants can provide sound justifications for their approaches. Whereas participants' acts often are tactical in de Certeau's sense, practices of obfuscation exhibit strategic characteristics.

8.3.3. Modification

Relating to unknown interlocutors also forms the basis for another set of tactics. Instead of acting on what computers supposedly 'think' in order to render their inferences useless, some participants also take advantage of a computational logic in order to construct a subjectively more meaningful representation of themselves. These practices of modifying appearances take two forms.

Teaching Computational Agents

Let's recall Laura, who believes to have figured out how *Facebook* curates her newsfeed. While she cannot change how *Facebook* makes inferences, she thinks that she can change the outcome of *Facebook*'s curation by supplying subjectively meaningful information. Laura does not want to hide from computational surveillance, but to challenge 'naïve inferences'. Like Laura, many participants recognise a clash between the complexity of their subjectivity and the apparently simplistic assumptions of computational agents. They want to teach computers to capture them as they see themselves.

In Fateha's eyes, social networks 'sometimes need a bit of help' to understand their users. Fateha works in a London advertising agency but wants to change jobs. *LinkedIn* is her main tool, but the automatic recommendations she gets do not met her criteria. She receives weekly emails about vacant positions:

[8, 28] "It was terrible, it was all sales jobs. Horrible jobs. I guess they must think, LinkedIn thought I want to be in sales because well, yes I am in sales. But I want to go into design and I studied it, and it did not list it here. So it must think because I am in ad sales, I also want my next job to be sales. It's a bit better now, but here - this is another ad agency, but this is a pharma company, for sales - I mean that's still totally not what I want."

Fateha tried to reconstruct *LinkedIn*'s logic of inference and concluded that it is overly simplistic. In an attempt to enhance its understanding of her preferences, she tweaked her profile information, adding keywords such as 'graphic design' wherever she could:

[8, 29] "I also, well, that's not true really, well a bit at least. My internship, it was not about design really, but I made it sound like a design thing. I hope that LinkedIn have picked that up

somehow and yes it's not true. In case when I get questions, when someone asks me I can say what I did, I mean I can always explain it."

But she was not certain that her intervention had worked. After all, she could only speculate how *LinkedIn*'s logic operates. In an attempt to increase her chances to trigger a behaviour that resonated with her unknown interlocutor, she also sent out *LinkedIn* invitations to strangers who work in graphic design, hoping that at least one of these tactics worked.

Frank in Germany, who I introduced earlier as a clerk for the public transport company, had a different problem. Whatever music he listens to is captured by *last.fm*, where his friends can see a list of all his songs. One day, a friend poked fun at him for having listened to a German pop song:

[8, 30] "It was 'Tausendmal berührt' [DK: 'Touched a thousand times'], you probably know it, right? I was really like, shit, what's going on here, that's not possible, that can't be. But then it was clear: shit, I was writing [DK: an essay for university] and needed something to keep me going. Usually, I don't listen to folk music at all, more house music, but I probably just craved it, I had the song on my computer somehow and well, it just did fit and I had it on repeat all the time, it was just an embarrassing tune. An accident so to speak and he just discovered it. But crazy, last.fm just uses it, well their results are not that accurate then." [DK: translation from German]

An embarrassing folk song had put Frank's musical reputation in jeopardy. He did not want to be caught dead listening to the song, but *last.fm* had exposed him. But according to Frank, *last.fm* should have distinguished between his usual songs and this exceptional incident. Although Frank had undoubtedly listened to the song, it did not reflect how he wanted to be seen. Frank had assumed a more sophisticated logic behind *last.fm*'s algorithms, and was disappointed as the site overstated the song's subjective importance. Recognising that he had to prevent further embarrassment, Frank put together a playlist of his favourite songs and let his music player repeat these tunes for hours at a time over several days until he had successfully overwritten *last.fm*'s mention of the embarrassing song.

Entering the Computational Gaze

In the examples so far, tinkering with one's appearance was rooted in an assumption of the superiority of subjective experience over computed reality. But just as in the case of Enrico, who thought that *last.fm* knows him better that he does himself, some participants intentionally submit to surveillance. Lars has a problem with procrastination and has

installed *RescueTime*, an application that tracks his internet use and provides statistics in the form of charts, percentages and minutes spent per website:

[8, 31] "This tool allows me to discover things about me that I would not realise otherwise, that only becomes clear when it is analysed and presented to me. Sometimes you think you are only away from your work for a couple of minutes, but if I look at RescueTime, it tells me that it can well have been an hour." [DK: translation from German]

The idea that computers know better also determines other practices of appearance. Several participants were not concerned about targeted advertising and instead voluntarily increased their exposure. Tim made sure that when given the option, he preferred to log onto a third party website with his *Facebook* credentials:

[8, 32] "I don't care about privacy, actually, it's better this way. I rather have personalised ads that are interesting, than random stuff. [...] What I have on Facebook is all true and I have nothing to hide, so if it can help to get better ads and if I can discover new things that are recommended to me, so if this is the case, I am happy to give other websites my data as well."

Submitting oneself fully to the computational gaze is less common than other forms of engaging with computational agents. They stand for a particular view of unknown interlocutors, where specific hypotheses about how exactly a computational logic operates make way to generic assumptions about their infallibility. While other practices seek to reduce the gap between discrepant roles and strive for interactional equivalence, submission to surveillance is about the very opposite: cultivating the power differential.

Synthesis: Computational Interlocutors as Significant Others

Practices of modification can be best understood by juxtaposing them with the types of practices discussed previously. Both data scarcity and obfuscation establish a firm boundary between the world of subjective experience and its computational representation. This is reflected in the construction of social situations. Speculating about the logic and motives of their unknown interlocutors, participants intend to avoid meaningful communication through withdrawal and deception, undermining the collaborative constitution and development of social situations between interactants as much as possible. Participants engage with the world of computation so that computers cannot enter their subjective experience. They attempt to decipher the logic of computation to outwit and circumvent it. This limits interaction to a struggle for access to the self and sovereignty over its interpretation between human interlocutors on the one hand, and computational interlocutors on the other.

In contrast, practices of modification performatively modulate computational inferences by bringing subjective experience into the computational realm. Of all practices, modification is most deeply situated on the level of infrastructure. Instead of avoiding the social situation with a computational interlocutor, modification embraces and develops it. Participants tinker with calculations so that their interlocutor can get a better grasp of them. These processes of tinkering are acts of translation that break a dualism between human and computational logics and see them as mutually co-constitutive. Participants teach computational interlocutors how to 'see' them, and acknowledge their interlocutors' view of themselves as meaningful inputs in constructing their own subjectivity. This reflects the basic tenet of symbolic interactionism that the self is not a solitary project and always constituted in interaction, as already expressed in Mead's ([1934] 2015) concepts of 'I' and 'me'.

Yet only in practices of modification, participants accept their interlocutor as co-constituting the self, and not as misrepresenting it. Goffman (1971) has argued that the self is coined by significant others who treat her or him as a being. Re-reading the term 'significant others' in the context of computation reveals a nuance. When human and computational logics intersect, participants chose whether they want to accept computational interlocutors as significant others, and thereby whether to be influenced by them. This does not mean that people can eliminate the consequences of computation through the denial of computational interlocutors - people live in a world that is already computed, irrespective of their personal preferences. However, it illustrates how perceptions of unknown interlocutors as meaningful influence the relationship between human and computational logics. Once interlocutors are identified as meaningful, participants welcome the influence of a computational logic on their self-perception. For instance, Laura was not against being interpreted by *Facebook* per se and merely wanted to be seen in a more nuanced manner. Once she corrected *Facebook*'s perception of herself, she did not mind being under computational scrutiny. In this context, glitches appear from a new perspective. They can be reconciled or avoided if the computational interlocutor is being perceived as a significant other who makes a meaningful contribution to the sense of self. Unlike in cases of data scarcity and obfuscation, glitches then become issues that can be resolved through more, not less interaction.

8.4. Failures: Re-Inventing Reflexive Agents

The plethora of practices discussed so far may spark assumptions that participants act towards surveillance as hyper-rational, ever-reflexive agents, transfixed on ducking and diving from the gaze of computation, calculatingly outplaying surveillance, gaming the system, and perpetually engineering their computational exposure. A Goffmanian framework may further stimulate such perceptions, as some interpret his portrayal of individuals in interaction as overly rational, and manipulative (Petras & Meltzer 2003). Indeed, in their acts towards surveillance, people seem to operate in a way that the logic of computation had originally foreclosed despite their ambitions. As I discussed in a previous chapter, being rational, reflexive and calculative are attributes that people ascribe to computational agents. In order to understand how computation operates, they feel that they need to adopt a maxim of rationality and reflexivity themselves, but ultimately realise that the differences between human and computational logics make this unattainable. Computation is pervasive and largely invisible, defining what I have called the conditions of possibility that people find themselves in. Yet acts towards surveillance are specific instances that are bound in space and purpose, and which involve overcoming these conditions by imagining unknown interlocutors. Indeed, participants' acts towards surveillance bear traits of rational and reflexive agents.

However, in this section, I document that participants cannot be reduced to such labels. Acts towards computational interlocutors stand within a broader context of participants as fallible agents that are complex and contradictory beings between rational and affectual tendencies. At the same time, I show that being rational and ever-reflexive is a state that participants strive towards in their acts, resurrecting the same principles they struggle to apply in the broader context of understanding surveillance. This tension ultimately underscores participants' struggles of participation in computed sociality.

8.4.1. Failures

Practices of appearance are riddled with accidents, disappointments and failures. Attempts to accumulate knowledge about computational surveillance and endeavours to negotiate appearances are also personal histories of regrets. Many realise later that they should have behaved differently in a past situation, and that they were not tactical, focused, and rational where they now think they should have been. Fateha, who now actively manipulates *LinkedIn*, regretfully looks at her past behaviour:

[8, 33] "I was so stupid that when I think now, I am like 'oh my God', I probably ruined it for me already because I was so stupid."

Others struggle with the demands of pervasive awareness. Many participants translate a general attitude to surveillance into principles of appearance, or how they want to render themselves visible to computational interlocutors. I call these 'regimes of appearance'. Yet applying such a regime in a consistent manner is an entirely different affair. I have previously introduced Freddy who meticulously tries to split his online activities across different web browsers. This is a calculated attempt to obscure algorithmic inferences. But in shock, Freddy once realised how he absent-mindedly surfed from his metal music forum to *Facebook* without having changed browsers:

[8, 34] "It really was 'ooooh shit', 'fuuuuck'. Once I did not pay attention and all is lost, how could I be so stupid. You just don't think, let's check Facebook, la la la, no attention to what's happening with the surveillance stuff."

Freddy had inadvertently let his mask down. He had invested labour and discipline into negotiating his appearance and a brief moment of negligence threatened to nullify all his efforts. A wrong mouse-click meant that previously separate online contexts were now connected. Ann-Kathrin was less agitated but recalls a similar situation. She had forgotten to switch off her laptop one night and inadvertently remained signed in to *Facebook* and *Skype*:

[8, 35] "Well, I would not like to appear as if I hadn't anything else to do, that I would just be glued in front of the screen. Because that's not the case often, really. For example, yesterday I forgot to switch off the laptop and then it was all the time, it was online all the time. This is probably also the image that's being portrayed about me, that's being matched with me. 'She is online, she is a junkie', and that goes into some database which puts me in a bad light." [DK: translation from German]

In Goffman's ([1959] 1990) terms, participants struggle to maintain their communicative front towards unknown interlocutors. The roles they try to play require discipline and an overarching principle of rationality which can easily get undermined by a quick affectual glance on *Facebook*, a wrong assumption about *LinkedIn*'s logic, or another negligence. Yet no matter how reflexive, controlled and diligent participants are about maintaining regimes of appearance, they also realise that interactions with unknown interlocutors inevitably involve a third party – other human agents. Previously, I introduced a number of participants who tightly control what information is available about them on *Facebook*. But tactics like Sarah's 'profile diet' are difficult to execute on a daily basis. She recounts numerous occasions where friends have uploaded and tagged pictures of her that clash with her idea of making herself visible to computation. Sometimes, people have even

posted personal details on her *Facebook* wall. She did not want *Facebook* to 'see' her in these ways:

[8, 36] "Come on people, I then think, if someone has no pictures of themselves, you gotta realise that you can't just post like crazy like on your own profile. And this really happened to me, like after the skiing vacation, where they tagged me, and then I also had some winter holiday ads, I am not sure if that was on Facebook or somewhere else on the internet, but it was there. Really, come on." [DK: translation from German]

Like Sarah, many participants realise time and again that even as they emulate computational approaches, they are not acting as lone agents, but are dependent on others who co-constitute their appearance. Suddenly, being impulsive, irrational, or at least not calculative, emerge as bad behavioural traits that people see in their peers.

8.4.2. The Limits of Reflexivity

Participants have developed ancillary tactics that focus on repairing or preventing the failures and mishaps that come with attempts to manage one's appearance. Once participants realise how careless they have been with their personal data in the past, many try to erase traces and undo their unwanted exposure. When Freddy realised that he had not changed browsers before he accessed *Facebook*, he did the following:

[8, 37] "When I realised, I immediately logged out of Facebook and deleted my history, and just to be on the safe side, I also restarted my computer and reinstalled Firefox and I hope that helped." [DK: translation from German]

Others embark on a deletion frenzy when they realise that their past behaviour was threatening their current idea of appearance, getting rid of all old accounts and registration data. Again others rely on policing their appearance. Tim from London highlights:

[8, 38] "I'm just monitoring what's out there, what information exists on me and what Google says when I google my name."

Sarah applies such policing tactics to her peers on *Facebook*. When a *Facebook* alert tells her that she has been tagged in a post or a photo, she is quick to undo this:

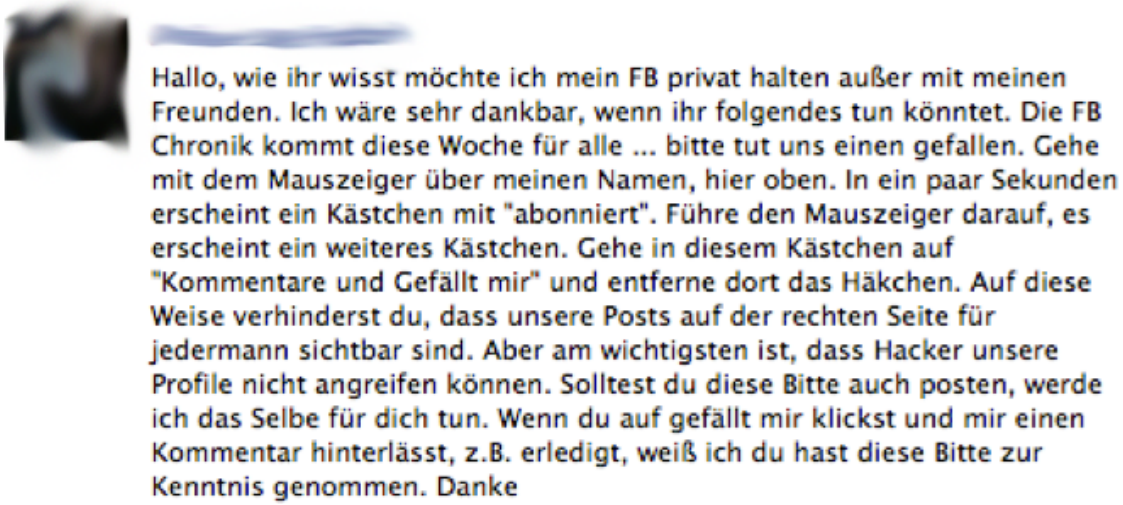
[8, 39] "I admit it is annoying because you can't always be that fast, so that the photo keeps being visible. But after I have untagged myself, I cannot be recognised [DK: by Facebook's algorithms] at least." [DK: translation from German]

Realising that their appearance to computation is co-dependent on others, some participants try to maintain their regime through dialogue. Anna, my first participant, observed that their peers took to public discussion after a recent change in *Facebook*'s privacy settings:

[8, 40] "This was, well Facebook changed its terms and conditions and there were also your activities, your likes, visible for everyone in the world. And there were discussions then, that you could not control that anymore and hackers and others could mine all that data. And then some people made some posts to warn about this." [DK: translation from German]

When we sat in front of my computer, she navigated to her friend's *Facebook* page and pointed towards a post. Her friend had published a post declaring that she wanted to keep her profile private despite recent changes in *Facebook*'s logic. She urged everyone to deactivate an option in their own account settings that made comments available to an extended circle of people beyond immediate contacts and asked for confirmation that her friends had acknowledged her message and taken action.

Figure 6: Facebook Post Acknowledging Co-Dependency



Source: Screenshot from participant's Facebook account

Such attempts to prevent or fix collapses in regimes of appearance debunk the idea of participants as hyper-rational, ever-reflexive agents, and show them as people that struggle for control, torn between an imperative of becoming like computers, scrambling to prevent their peers from undermining their efforts and fixing their own omissions. But these attempts also establish reflexivity and rationality as attributes that underpin people's intentions. When they engage with computational interlocutors, many try to mirror their modus operandi as rational, reflexive, planned and calculated. Participants want to act as agents who grasp the modalities of computation. This entails being reflexive in the sense that participants probe and question their interlocutors and become 'rule finders' (Lash 2007) that spot patterns and regularities, similar to the generative rules that underpin the computational logic itself. Yet in contrast to Lash, they do not act 'as if' they were

algorithms and instead are modelling their behaviour on how they interpret computation through their human senses and social experiences.

Yet conversely, failures of maintaining regimes of appearance can be understood as unsuccessful approximations to a computational logic. When such regimes collapse, it becomes apparent to participants that they are indeed unable to permanently impose principles they see in computational interlocutors onto themselves. Participants know that they are not pervasively rational and reflexive, but want to be, and condemn their own affectual nature. Their struggle and determination to keep up with the rational and reflexive paradigm of computation shows how a computational logic creeps into and alters a human logic. It changes how people want to think, how they want to understand themselves and engage with the world, defining desirable attributes of character.

8.5. Chapter Conclusion

This chapter explored participants' practices towards computational surveillance. After previous chapters had documented how human agents encounter and construct knowledge about computational surveillance, this chapter focussed on their capacity to intervene in and interact with the computational rendition of reality (Kallinikos 2009), and how these acts are themselves expression of computed sociality (Kallinikos & Tempini 2014). My argument demonstrated the motivations, modalities, consequences, and limits of relating to computational interlocutors. It approached agency towards computation through the concept of glitches, a reformulation of Berger and Luckmann's notion of dissonances. Glitches occur when subjective experience and meaning are misaligned with objective reality, expressed through the logic of computation.

The chapter outlined three types of glitches - naïve inferences, normative clashes and the superiority of computational inference. Participants strive to resolve these glitches, and through a Goffmanian framework of symbolic interaction, this chapter illustrated how participants act on them. Computational interactants are unknown interlocutors whose shape, motivations and logic are hard to grasp, challenging participants to establish a social situation through which to interact. Computational agents can see and read human agents, but such insights are not mutual, leading to skewed relations of visibility in favour of computational interlocutors. Engaging in interaction from a disadvantaged position, participants apply assumptions, they look and learn and probe in order to tease out their

interlocutors' characteristics. On this basis, they negotiate their appearance, or how their subjective experience is reflected and acknowledged in computational principles, through three types of practices – data scarcity, obfuscation, and modification. Each of these types of practices takes place on a spectrum that signifies the depth of encroachment into the computational logic. Interface practices both take place on the screen and only consider what is on the screen, whereas infrastructure practices delve into the underbelly of computation. Yet participants are not hyper-rational and ever-reflexive agents.

The chapter concludes that people's practices are riddled with omissions, misconceptions and failures. Participants are torn between their rational, reflexive and their affectual selves. Yet they also realise that computational interlocutors are cold, calculating, rational and reflexive, and that agency towards them demands such qualities to a grade and with a consistency that is unattainable for them. Acting towards computational surveillance alters the perception of an ideal self, and rationality and reflexivity emerge as desirable attributes for self-optimisation vis-à-vis computational forces.

These findings stand in a broader context. The practices towards computational surveillance discussed here shed further light on the social construction of reality against the background computed sociality, the central paradigm of this study. In *Chapter Seven*, I have shown how people intersubjectively construct knowledge about a computational world and establish a common-sense reality between them. This chapter has shown that the intersubjective constitution of reality does not just take place between people, but also between human and computational agents. As people seek to repair the glitches between their subjective experience and the computational world, they reconcile different views of reality and either mould computation to their perspective or let their view be modified by a computational logic. People's attempts to incorporate computational characteristics into their own ways of thinking about and acting towards the world show that the coordinates of the social construction of reality have changed since Berger & Luckmann's original analysis. The empirical analysis of social construction within computed sociality in this chapter has provided evidence that people routinely direct their everyday practices of negotiating and reaffirming reality towards computational agents, thereby recognising them as agents that co-shape the world and normalising them as common interlocutors.

Chapter Nine: Conclusion

In this dissertation, I have offered a perspective for understanding human agency towards computational surveillance. I have formulated a theoretical approach rooted in and expanding on the sociology of knowledge and have mapped out empirically how young adults in Germany and the UK make sense of, and interact with computational interlocutors to shape their lived experience with surveillance. The thesis was motivated by an intersecting set of shortcomings in the academic debate to provide such a perspective; from the prioritisation in surveillance studies of systems and processes of surveillance over its lived experience to the implication of surveillance as a mere feature in the much broader role of computation in making up the social world. This dissertation has followed Lyon's (2007) call to extend the focus of surveillance research to incorporate the perspective of human agents while recognising the changing socio-technical coordinates of computation in which surveillance itself takes place. These shortcomings in the academic debate were magnified by a growing social urgency to address issues of agency amidst the rapid proliferation of computational surveillance and ensuing public debate, from tactics to evade the gaze of *Facebook* in the news media to recommendations for self-tracking through digital devices in everyday discourse.

This motivation has been detailed in *Chapter One* through a brief survey of the state of academic debate and references to popular culture. The next two chapters progressively developed a theoretical framework. While *Chapter Two* reviewed theories of surveillance, *Chapter Three* shifted focus away from a surveillance-centric approach and developed an alternative perspective on agency through the social construction of reality, theories of algorithms, big data, infrastructure, visibility and communications.

The methodology to transport this framework into the empirical domain has been outlined in *Chapter Four*. It specified three research questions concerning (1) *the role of online surveillance in everyday life*, (2) *how people develop knowledge about the computational mechanisms that underpin computational surveillance*, as well as (3) *the practices that people employ to act towards such forms of surveillance and their underlying intentions*. These research questions were operationalised through a range of methods that include sensitising concepts, in-depth interviews, think-aloud protocols, participant observation and live interviews.

The empirical material has been explored across the next four chapters, which progressively addressed these research questions. *Chapter Five* drew on concepts developed in the theoretical discussion of surveillance, whereas *Chapter Six* to *Chapter Eight* have been supported by the theory of agency developed in *Chapter Three*. Concerned with the role of computational surveillance in everyday life, *Chapter Five* discussed people's relationship towards surveillance through the naturalisation of the surveillance experience, its entanglement with wider everyday online practices and its manifestation as a pervasive sense of risk. The next two chapters explored how participants query the computational mechanisms that structure their everyday life. *Chapter Six* discussed the general conditions under which the construction of knowledge about computational surveillance takes place and how participants as individuals generate such knowledge. *Chapter Seven* documented the collaborative, social practices of constructing knowledge about computation and social mechanisms of manufacturing a common-sense reality in and of a computational world. *Chapter Eight*, the last empirical chapter, investigated participants' communicative acts towards computational surveillance as interlocutors in everyday online life, and how modes of negotiating their appearance towards these interlocutors are expressions of the social construction of reality. While the empirical chapters were analyses in their own right, they also built on each other as each provided groundwork for the next to interrogate different aspects of agency, which is most explicit in the last empirical chapter.

In this final *Chapter Nine*, I synthesise the findings and highlight noteworthy implications. I also discuss the study's limitations and avenues for future research.

9.1. De-Centring Surveillance: A New Perspective for Agency

Framing agency towards computational surveillance required altering the coordinates of debate. I have argued in a review of surveillance literature (*Chapter Two*) to decentre surveillance in lieu of approaches embedded in broader social theory. Surveillance studies themselves provide the basis for this argument through their reflexive criticism of the panopticon as a master concept and departures from grand theories towards situated approaches that focus on particular configurations of surveillance. The argument I have outlined follows these debates, yet also departs from them. While surveillance theory committed to situated approaches incorporates aspects of wider social theory into a surveillance framework, such as Haggerty and Ericsson's (2000) use of Beck's risk

society, I have done the contrary by bringing surveillance into a framework of social theory that is not primarily concerned with surveillance itself. In doing so, I have proposed to disregard surveillance as a phenomenon sui generis, and to consider it instead as a manifestation of much wider social transformations. Surveillance studies have legitimised this approach. As they have described the pervasive spread of surveillance through its computerisation into nearly all aspects of everyday life, my approach has built on and reflected this diagnosis by changing the parameters of inquiry. These parameters have been consolidated in *Chapter Three*, which was developed on the premise that the prison guard, the physical architecture of the panopticon and the CCTV operator have been supplanted or replaced by computing powers as agents of surveillance. This is not merely a change of guards, literally and metaphorically, but expression of a fundamental change of the role of surveillance in society. As algorithms, big data, software and related concepts have come to mediate and constitute lived reality, contemporary surveillance merely is a manifestation of the remaking of the world brought about by computation as a social force. As a consequence, the question of agency is recast into a broader discussion on the ability to act within the reified outcomes of computation.

De-centring surveillance was not merely a theoretical exercise. *Chapter Five* has shown that participants associate surveillance primarily with the state and not with the computational practices of monitoring that they encounter in their everyday lives online. I have documented that the pervasive spread of computational surveillance has paradoxically contributed to its *dissolution* as a distinct category of lived experience and that it is intertwined with and indistinguishable from wider everyday online practices.

For instance, participants consider the collection and processing of their personal data as part and parcel of being online and have forged an *implicit deal* where they exchange access and participation online for being monitored. Furthermore, participants shape, relate to and communicate through their *data doubles*, appropriating categories of surveillance imposed on them as regular and mundane frames through which they navigate online life and nurture their self-understanding. Snooping and spying on friends, while associated with complex social norms, is commonplace among them. This *peer-to-peer surveillance* erodes role distinctions between watching and being watched, complicating moral judgement and normalising surveillance as a playful occurrence.

However, *Chapter Five* has also shown that the dissolution of surveillance coincides with the experience of a *new landscape of risk*, where participants struggle to grasp the intentions and consequences of computational processes they are surrounded by online. This feeling of risk refers to online practices and computational encounters in which surveillance plays a part, but which participants do not regard as surveillance-specific practices. Risk is framed towards computation as an elusive phenomenon, and not towards surveillance as a part of computation.

9.2. The Changing Parameters of Social Construction

To provide a framework for understanding agency (*Chapter Three*), I have combined Kallinikos' diagnosis of the computational rendition of reality (2009) with a reinterpretation of Berger and Luckmann's ([1966] 1991) social construction of reality. While Kallinikos emphasises the computational parameters that constitute reality, Berger and Luckmann offer a theory about how people create and reproduce reality within the bounds of a social world they inhabit. Both approaches stress the engineering of reality, which served as a bridging concept to implement the notion of computation into a theory of agency on the one hand, and to situate questions of agency within a framework of computation on the other. I have summarised the intersection of these perspectives by expanding on the concept of computed sociality (Kallinikos & Tempini 2014).

Agency in a surveillance context is commonly understood in the binaries of resistance and complicity. Within the changed coordinates of debate summarised above, the theoretical framework I have employed has instead specified agency as the general capacity to query and interact with the computational operations that people are embedded in to arrive at an understanding of reality and to shape it. This problematises the conditions of knowledge, or how people can make sense of a world governed by computation. I have introduced a computational logic as a particular way of operating in the world and rendering it. I have also outlined that this logic is categorically inaccessible to human agents. The capacity to act then is hampered by a communication problem in that human agents struggle to relate to computational forces. I have used the notion of invisibility, and the dualism of interface and infrastructure to specify the parameters of this communication problem.

Berger and Luckmann's social construction of reality has helped to theorise how, despite this communication problem, social practices become possible through which human agents can interrogate and reclaim the conditions under which knowledge is produced. This required revisiting their account of social construction, as the authors could not have considered the proliferation of computation at their time of writing. I have shown that the introduction of computation as an additional type of agent involved in the creation and maintenance of social order reconfigures how human agents can manufacture intersubjective common-sense knowledge, which for Berger and Luckmann is the foundation for reality. As a consequence, I have proposed that a theory of social construction needs to consider not merely communicative acts between human agents that render reality, but also acts towards, and involving computational interlocutors.

While Berger and Luckmann's theory does not offer such a perspective directly, I have demonstrated its adaptability and extensibility by reformulating two of its concepts - *dissonances* and *universe maintenance*. This demanded a recourse to wider social theory, as well as to concepts from other debates. I have specified dissonances, or clashes between narratives of reality, through the notion of glitches, a concept predominantly used in new media and computer art. Glitches make a computational logic visible to human agents, revealing discrepancies in judgement and interpretation of the world. Mechanisms of universe maintenance are shared narratives about the world that legitimise and reaffirm reality, such as myths, legends and other stories. While Berger and Luckmann reference religion as their case study, I have shown that sharing narratives of encounters with computation, for instance through glitches, are contemporary expressions of universe maintenance. Through Lash's concept of generative rules and Beck's notion of risk, I have mapped out how the nature of universe maintenance changes in the context of computation from the preservation of a given conception of reality, to everyday collective practices of updating, changing and reconciling knowledge about computation.

My reformulation of dissonances and universe maintenance coincided with a change in focus for theorising social construction. Dissonances were of marginal concern to Berger and Luckmann. As their theory focusses on the maintenance of social stability in mid-twentieth century Western societies, they saw dissonances as exceptional events in an otherwise pervasive and unproblematic social consensus. However, they recognised that such a consensus is historically specific and that the make-up of future societies may

require a stronger emphasis on dissonances in theories of social construction. The introduction of computation as a social force represents such a transformation. By ascribing dissonances an instrumental role in the possibility of agency, I have reconfigured Berger and Luckmann's original framework. I have shifted focus on the complications inherent in creating consensus knowledge about the world and have framed these complications as a default condition, rather than an exception. This new default is also apparent in my take on universe maintenance. Consisting of practices to flexibly update and recalibrate common-sense knowledge, in my interpretation, universe maintenance alludes to a different social disposition than the one Berger and Luckmann had in mind. In Berger and Luckmann's original framework, universe maintenance is enacted from a position of social stability where established myths and other narratives are merely carried forward. I have instead presented universe maintenance as an everyday struggle to prevent a consensus from falling apart, and as the need to continually re-establish this consensus anew.

This reformulation of dissonances and universe maintenance exhibits attributes of a society where certainties are merely temporal. Such are the characteristics of late-modern, or reflexive-modern societies that Beck and other authors have described. In reformulating Berger and Luckmann's theory, I have provided evidence that their approach to the social construction of reality is applicable to and relevant for other iterations of modern societies beyond the confines of the particular socio-historical conditions they were writing in.

More widely, updating their approach took place in a paradigmatically fluid environment where analytical templates for the particular problem of agency I outlined were absent. At the outset of this thesis, I justified my choice for an approach informed by sociology in the broadest sense with Joas' (1996) assertion that part of the discipline's value lies in its paradigmatic instability, making it self-reflexive and adaptive to external debates and concepts. The integration of computational issues into Berger and Luckmann's framework of social construction is testament to this claim. It supports criticism (boyd & Crawford 2012) against pundits (e.g. Anderson 2008) who suggest the demise of theory in an age of computation and big data, and instead helps to demonstrate that established theoretical frameworks and intellectual traditions are equipped to cope with social change and to provide a perspective on computational phenomena.

While the notions of a computational rendition of reality (Kallinikos 2009) and computed sociality (Kallinikos & Tempini 2014) underpinned this reformulation of Berger and Luckmann's theory, throughout the empirical analysis I have also documented how the interplay between these concepts has allowed to expand the idea of computed sociality. In *Chapter Six* I have shown that the computational rendition of reality is already part of participants' everyday lived experience, and that this experience itself is further expression of computed sociality. *Chapter Seven* has demonstrated that the problems of knowledge associated with living under conditions of pervasive computation are expressed in everyday interaction between people. Reflections about computation and the construction of meaning in relation to it establish computed sociality as a general social phenomenon that is also negotiated outside of the domain of computation. Lastly, *Chapter Eight* has provided evidence that people themselves consciously establish interactions with computational interlocutors and that these intentional interactions produce sociality. In this updated sense, this thesis has considered computed sociality as the engineering of the social through computation, the embedding of computation into people's lived experience, and the interdependent process of social construction between human and computational interlocutors.

9.3. Approximating a Computational Logic

Far from imposed by academic diagnoses through abstraction from people's own practice, problems associated with the conditions of knowledge are part of everyday life. Participants recognise that they are living in a world governed by computers that produces knowledge about them, but which is not accessible as an object of knowledge to them in the same way. The computational rendition of reality (Kallinikos 2009) then is problematised in the domain of everyday experience. In *Chapter Six*, I have summarised the experience of these problems as *conditions of possibility.* Most notably, participants connect the ability to interact with and intervene in a computational world with the capacity to emulate a computational logic by adopting a paradigm of perpetual rationality and reflexivity. In this process, these computational attributes are recast as desirable character traits that remain unattainable as participants acknowledge their limits in aspiring to such a computational ideal. The particular rationality and reflexivity of computational agents also remain opaque to participants as the invisibility of computation prevents them from a precise understanding of its modus operandi, and limits ways to think about and express computational principles in language. The computational

rendition of reality then is both present and absent at the same time in people's lives. Participants' attempts of constructing knowledge and acting towards computation take place within these conditions of possibility as constraining factors and are attempts to compensate for them creatively. I have argued that the experience of computation as an agential force and people's own limitations and attempts of querying it are themselves part of computed sociality.

A critical theme that emerged throughout *Chapter Six* and *Chapter Eight* is how this unattainable maxim of rationality and reflexivity manifests itself in participants' attempts to appropriate a computational paradigm in their everyday practices despite such adversity. While *Chapter Six* shed light on the role of emulating computation to shape the conditions of knowledge, *Chapter Eight* showed how such principles translate into situated acts to negotiate particular interpretations and judgements of the world with computational interlocutors. Douglas Rushkoff (2011) once polemically proposed *Program or Be Programmed* as a narrow dualism for agency in a computational world, but participants' narratives have revealed more complex, nuanced and conflicted approaches.

9.3.1. Exosomatic Organs and Limits of Computational Approximation

In *Chapter Six*, I have shown how participants rely on technological tools as *exosomatic organs* that modulate computational forces on their behalf. Recognising their limits in understanding how tracking, monitoring and data collection work online, participants draw on these tools to compensate for the limits of their human senses and cognitive means to remain perpetually vigilant towards computational surveillance. However, I have also shown how participants are inherently frustrated by such exosomatic organs, and that the technological promise they convey is a broken one. During many interviews, participants were worried that the tools they use to stay on top of computational surveillance are themselves opaque and inaccessible to human scrutiny, leading them to question their merits, and sparking concerns about a power differential between those tools on the one hand, and the capabilities of the computational forces they seek to affect, on the other. Enthusiasm and disappointment about technological fixes often coincide, revealing deeply conflicted attitudes within participants. Although some participants rely more on such tools than others, there is a general sense that outsourcing the need to deal with computation to technology is a dead end. As participants employ such tools, they

become aware that their own, human logic remains a vital component in constructing knowledge about computational principles affecting their lives.

9.3.2. Practices and Failures of Adaptation

In *Chapter Eight*, I have shown how the computational maxim of rationality and reflexivity translates into everyday acts of engaging with computational interlocutors. I have documented participants' attempts to gauge how computation 'thinks' and how they adjust their communicative acts to these assumptions to mirror what they perceive as rational, reflexive, planned and calculated acts. Participants query their computational interlocutors and become 'rule finders' (Lash 2007) that spot patterns and regularities, adopting principles of making sense of the world akin to the principles of a computational logic itself, but through their human senses, cognitive means and social experiences. At the same time, participants' narratives regularly showed failures and shortcomings of adopting these principles. Participants expressed awareness that they are not pervasively rational and reflexive. Yet many aspire to be so, and condemn their affectual acts as a flaw of character, for instance when they forget to imagine the role of computation in a given online practice. Through these issues, I have shown how participants' struggle to keep up with the rational and reflexive paradigm of computation is evidence of a computational logic creeping into their modes of making sense of the world and how people want to understand themselves.

9.4. Unfolding and Collaboration as Construction of Knowledge

Despite obstacles of generating knowledge about a computational world, this thesis has demonstrated that attempts to reclaim the conditions of knowledge and probe into the workings of computation are an intrinsic part of participants' everyday activities, both online and offline. This construction of knowledge is carried out both as individual practices, as well as through communicative acts in collaboration with others.

9.4.1. Unfolding Events

In *Chapter Six*, I have shown how the construction of knowledge is both serendipitous and reactive, as well as initiated by participants themselves. Participants often obtain new insights into the workings of computation through a computational logic that reveals itself in *unfolding events* by converting its processes and assumptions onto the interface of the screen where they become accessible to human understanding. Such unfolding events are

ruptures of experience by foregrounding issues of computational surveillance into consciousness, transforming an ordinary situation into one defined by computation.

Most participants attempt to gain additional control over the occurrence of these unexpected encounters and trigger unfolding events themselves. Throughout my interviews, and irrespective of their technological proficiency, participants highlighted how they engage in restorative acts to provoke a computational logic to reveal itself. I have demonstrated that such unfolding events are bittersweet. On the one hand, they create a sense of unease for participants because they defy their stock of existing knowledge about the way computation operates and remind them of the limits and the fallibility of their knowledge. On the other hand, participants have emphasised how they welcome unfolding events as sources of knowledge. Participants live in a constant state of coming-to-consciousness, where new unfolding events reveal additional information, momentarily enabling a grasp on an otherwise elusive computational logic, yet confronting them with the realisation that their knowledge is perpetually incomplete and fragile. The experience of unfolding events specifies and deepens participants' recognition that they live within the computational environment that (Kallinikos and Tempini (2014) have outlined, and that it consists of 'discrepant worlds' (Berger & Luckmann ([1966] 1991) that they struggle to reconcile.

9.4.2. Collective Practices

In contrast to assertions that the social implications of a computational world are largely absent from the public agenda and confined to expert circles (Meckel 2011), I have shown in *Chapter Seven* that a wider collective inquiry into the role of computation and its logic is taking place. For instance, news media provide templates for interpretation and blueprints for acting towards computational surveillance, offering *recipe knowledge*. The complexity of social construction became particularly evident during the discussion of SNS. I have shown how a recurring stream of social media posts on surveillance incidents *legitimises inquiry* into the world of computation by affirming social acceptability and social norms around the construction of knowledge. I have also shown how conversations about computational surveillance on SNS and face-to-face are acts of *meaningful reciprocity* that help consolidate common-sense knowledge. Taken together, I have proposed that collective acts in such communicative areas stand for an emerging culture of mediatisation (Hepp 2013).

Yet participants' narratives have revealed that intersubjective common-sense knowledge about computational surveillance is inherently unstable and does not translate into a coherent picture of social reality at the end of a collaborative enterprise that is solidified and finite. Participants have likened attempts to interrogate computational processes to a 'puzzle' and continuously assemble reality as an ongoing construction. This differs from Berger and Luckmann's original theoretical description, who see the social construction of reality as an analytical concept and claim that people do not actually experience their own reality as constructed. In contrast, I have shown that the experience of construction is an intrinsic feature of the computational world that participants live in. The scaffold of construction remains visible as people accept reality as a given.

Reality as an ongoing construction coincides with conflicts of interpretation, where multiple truths become available at the same time, leading both to confirmations and disconfirmations about assumptions of reality. Participants showed that generating social consensus entails reconciling such competing interpretations and to individually find out around which interpretation a social consensus is forming, a process that I have called *the hard work of common-sense*.

Given the unstable nature of common-sense knowledge, my interviews showed how participants employ tactics to maintain and solidify a social consensus. *Affirmatory tokens* and *folk tales* allow participants to assess whether their knowledge is congruent with that of their peers. They are also a form of social grooming, and participants use them to confirm that they believe in a common set of assumptions about the computational world as their peers. This analysis has shown that computed sociality extends beyond the realm of computation and is also expressed through intersubjective acts of meaning-making between human agents about the role and nature of computation as a constituent part of the social world.

9.5. Imagining and Interacting with Computational Interlocutors

The intersubjective construction of reality does not just take place between human agents that are coming to terms with a reality co-shaped by computation, but also manifests itself directly in acts between human and computational agents. I have argued that these human-machine interactions are themselves part of computed sociality. Attempts to tease out the computational logic through provoked unfolding in *Chapter Six* has already suggested

this. This dynamic became more explicit in *Chapter Eight*, where I documented how participants engage in practices to repair glitches between how they see themselves, and how computational agents perceive them. I have shown how participants routinely reconcile different views of reality through *impression management*, and either mould computation to their perspective or let a computational logic modify their sense of reality.

I have offered a taxonomy of glitches entailing *naïve inferences*, *normative clashes*, and *computational superiority*. Drawing on Goffman's symbolic interaction (Goffman 1971; [1959] 1990; [1967] 2003), I have highlighted that participants strive to overcome glitches by establishing a social situation with computational forces as *unknown interlocutors*, whose motives are unclear and where interaction rules are absent. I have shown how participants develop assumptions about their computational interlocutors and infer a social situation on this basis.

Participants provided individual narratives on how they create and act in social situations with computational interlocutors. Specific tactics were recurring across participants' accounts, but combinations of tactics and how they are enacted are highly personal and lack a normative framework. Nevertheless, patterns emerged, and I have grouped participants' practices to repair glitches in three categories called *data scarcity*, *obfuscation*, and *modification*. I also introduced a second layer of categorisation as a spectrum which enabled a view in how far these practices take place on the interface of the screen, or on the level of the computational infrastructure itself. This analysis revealed that some participants confine themselves to the interface of the screen and have a rudimentary imagination of computation as an interlocutor, whereas at the other extreme, participants both take into account the infrastructure in which computation operates and even attune their own communicative acts to how they imagine that a computational logic works.

9.6. Defining Agency Towards Computational Surveillance

In *Chapter Three*, I have argued that a theoretical understanding of agency towards computational surveillance can only outline how agency is possible in principle and that it cannot capture all actual manifestations of agency in their nuances and variety. As Jonathan Crary (2014) has reminded us, the notion of agency also is subject to historically specific interpretations, and as Emirbayer & Mische (1998) have stressed, the term

'agency' itself is often not sufficiently problematised and specified. I proposed to leave the closer delineation of what actually constitutes agency in the context of this study to the empirical domain. Abstracting from the specific themes outlined in this concluding chapter, participants' narratives have shown that agency in the context of computed sociality is possible despite the constraints I described in *Chapter Six* as *conditions of possibility*. I have shown this by updating Berger and Luckmann's framework to incorporate the specific conditions of computation through Kallinikos' work, and by locating this agency within an expanded notion of computed sociality. Such agency is not monolithic, but has multiple facets:

At the most fundamental level, agency manifests itself in the ability to reclaim the conditions of knowledge. This is a much broader sense of agency than studies focussing on resistance towards surveillance (e.g. Toon 2000) or online activism (e.g. Karpf 2010) convey. Agency is not steeped in an us-versus-them rhetoric that follows political motives or seeks to overturn a regime of surveillance power. It also does not mean that human agents 'win' over the forces of computation and restore a pre-computational reality that they are masters of. Far from such Hollywood dramaturgy, agency emerged as the ability to create the conditions to negotiate social order and the common-sense reality of the world in accordance with others, including both human and computational agents. I have shown that while a computational logic modulates and constitutes the social world, people's interactions with each other about this world establish and consolidate common-sense knowledge about computation. I have also demonstrated that agency is enacted in relationships between human agents and computational interlocutors, and that negotiations of reality in direct interactions with such interlocutors is commonplace.

Agency then also entails the acknowledgement of computational interlocutors as an additional type of social agent. This scenario neither appeared to people as a radical rupture that uproots them nor did it spark feelings of fear that a cyborg dystopia has finally arrived. Despite different degrees of technical expertise and ability to engage with computational interlocutors, participants generally recognised and accepted computation as an agential force. The intention to overcome glitches helps explain this. As participants seek to repair these glitches, they draw on mechanisms of universe maintenance that fix and retune, rather than uproot social order. Despite occasional shocking revelations through unfolding events, agency towards computational surveillance, therefore, is not a

narrative of revolution, but expression of everyday, hardly noticeable, recalibrations of social reality.

Stories of resistance or compliance with computational surveillance persist, but not in a binary form. These narratives themselves are rooted in, and extensions of the process of constructing knowledge and such acts of recalibration. They are so in a double sense. When participants act towards computational agents, they establish a social situation that entails assumptions and inferences about them as interlocutors, which are themselves expressions of knowledge construction. I have also shown how practices of resistance and compliance are linked to glitches between how participants see themselves and the world on the one hand, and the perspective of computation on the other. Resistance and compliance with computation then are communicative acts of negotiating a shared reality between human and computational interlocutors and bringing discrepant ideas about reality in tune.

All these acts take place under the absence of established normative templates that participants can draw on. Participants encounter a reality of computation constantly in flux, iteratively and collaboratively establish perpetually changing conceptions of reality and reflexively seek to approximate the logic(s) of computational interlocutors. While I have steered away from a meta-discussion that problematises the concept of agency as such due to a matter of focus, the empirical manifestations of agency I have documented highlight the merits of framing agency beyond prevalent rational or normative dimensions as containing a creative strand (Emirbayer & Mische 1998; Joas 1996).

9.7. Limitations and Tangents

While focus enables a manageable scope, it comes with limitations. Below, I outline the limitations of this thesis to aid the interpretation of results and place signposts for the range of inferences that can and cannot be made. I also highlight areas for future research that emerge out of these limitations.

9.7.1. Socio-Demographics and the Construction of Knowledge

By focussing on young adults aged between 18 and 29 years old, other age groups have been precluded in this study. This choice was made to engage with a set of participants who see the internet as an integral part of their everyday life and exhibit a broad range of online activities across different contexts from school and university to work and leisure

to provide sufficiently rich and diverse narratives about encounters with computational surveillance. Despite including participants with a maximum age difference of eleven years, this study found no evidence of age-related differences in between them regarding narratives or terminology. However, the results do not necessarily translate to other age groups. For instance, the *Pew Research Center* (2015) found demographic differences between social media users both concerning presence on SNS and frequency of use that may shape exposure and hence perceptions of computation. The engineering of social consensus about computational surveillance is heavily informed by exposure to communicative areas such as SNS, but also by talk within peer groups, such as anecdotes about online failures which presuppose that online and offline cultures are intertwined. It must be cautioned that the shared stock of knowledge and social practices of generating consensus could be influenced by age. For instance, older demographics might not have access to, nor replicate the collaborative practices I outlined in their peer groups. People younger than my participants, especially those who do not remember a life before the internet, may grow up with a different set of risk assessments and attitudes towards computational agents.

Issues of age also translate to other socio-demographic limitations inherent in this thesis. For instance, in a study on marketer's use of personal data, Turow et al. (2015) found statistically significant differences for the variables 'race' and 'education' concerning people's willingness to give up their data for supermarket discounts. In this thesis, I have not considered race and have only peripherally considered education. While the sampling method ensured that participants were recruited from a variety of social backgrounds and occupations, it did not afford a systematic analysis of how such differences influence the social construction of knowledge.

In a critique of the notion of 'digital natives', Helsper and Eynon (2010) have argued that generational differences are overemphasised as determinants of internet literacy and that variables such as education, experience and breadth of use are at least equally important. In this thesis, I have provided a perspective on the differences between participants when it comes to engaging with computational interlocutors through a spectrum that ranges from practices on the interface to infrastructure practices. Further research is necessary to relate these differences both to age, as well as to other variables such as those that Helsper and Eynon have identified.

This study has included participants both in the UK and Germany. Differences between countries centred around the definition of surveillance which is partly influenced by historical experience. The only other observed difference between countries emerged in the use of privacy advocacy groups on SNS. While these results offer indications for a transnational set of practices, this study has not considered the social construction of knowledge in other national contexts, in particular in Non-Western societies. Further evidence is required to understand transnational practices and to investigate possible national, or historical and cultural differences more widely that may have a larger impact on the construction of knowledge than the sample from Germany and the UK that I drew on in this thesis.

9.7.2. Communities of Practice

This thesis has considered participants both as individuals and as social beings embedded in particular social groups. Evidence provided sees them engaged with computed sociality alone in front of their computer screens, and as social agents in collaborative exchange with others in a range of communicative arenas. Participants' narratives provided a glimpse into their peer groups, and into the social construction of knowledge within those peer groups. This became particularly evident in *Chapter Seven*, where stories of *universe maintenance* showed that some narratives spread over the wider internet (e.g. 'pig story'), whereas others are localised narratives confined to a circle of cohabitating friends (e.g. 'pornography failure').

It was beyond the scope of this study to systematically explore different practices and regimes of knowledge construction specific to such peer groups, and ultimately how different social groups live in computed sociality. There are merits for a future study that uses a different set of methods, such as ethnography, and other sampling techniques, to specifically explore the structure of knowledge production within and between social groups. The notion of 'communities of practice' (Wenger [1998] 2000) for instance would enable such a perspective beyond conventional socio-demographic coordinates.

An approach rooted in a communities of practice paradigm that builds on the social construction of knowledge outlined in this thesis would also create inroads to other issues and debates within the wider field of computation and society:

Just as Gitelman (2013) has highlighted in the aptly titled *Raw Data is an Oxymoron* that data are always a product of bias, in *Chapter Three*, I have suggested that a computational logic is also informed by human practices. These include values, experiences, lay-psychological and lay-sociological assumptions encoded by programmers and data practitioners into software. A perspective informed by communities of practice could shed further light on the social construction of knowledge within those professional circles.

Similarly, such an approach could link the perspective developed in this thesis to debates around digital labour in a platform economy. The *Financial Times* recently headlined an article 'When your boss is an algorithm' (O'Connor 2016), outlining the struggle of drivers for taxi services such as *Uber*, or delivery services like *Deliveroo* or *Amazon*, with their algorithmically engineered schedules. Analysing how these workers imagine, interrogate and challenge the computational systems they are embedded in would provide a timely study within the context of the social construction of knowledge that I outlined.

9.7.3. Technological and Political Change

The pace of technological change means that since the fieldwork for this study largely in 2010, the repertoire of communication tools, both regarding software and hardware, as well as the practices they afford, has already expanded and changed.

While many German participants discussed at length their activities on *StudiVZ*, this German SNS has since fallen into disregard and German media liken it to a 'ghost town' (Dörner 2015). Similarly, *Instagram*, which at the time of writing attracts 500 million monthly active users (Instagram 2016), had just been launched and *Snapchat* had not yet seen the light of day. Think-aloud protocols and probing interviews took place in front of personal computers. While many participants possessed smartphones, mobile devices constituted an alternative form of being online that was peripheral to their overall use. Conversely, in its earnings report for the quarter ending 30 June 2016, *Facebook* highlighted that 88% of users access *Facebook* on mobile devices, with 56% using only mobile devices (Facebook 2016).

The proliferation of smartphones has coincided with the rise of an app environment in which media experiences are contained that has also colonised tablets and connected TVs. Apps are self-contained information appliances (Zittrain 2008) designed for specific

devices that are often not open to modifications. However, modifications like ad-blockers installed onto a web browser were part of the tools that participants in this study used to probe into the workings of computation. At the same time, the introduction of virtual personal assistants such as *Apple*'s *Siri* or *Amazon*'s *Echo* permits a more intimate, and immediate communication with computational interlocutors. These applications and devices are controlled by the user's voice. They react to natural language and respond in a human-like voice which the user can select from a set of options, such as whether the voice is male or female.

A common concern when conducting research about everyday practices that are embedded in a particular socio-technical configuration is the applicability of findings over time. While this study offered a snapshot of the practices that inform the social construction of computational reality around the year 2010, it was, at the most fundamental level, also technology-agnostic and provided an analytical template for the incorporation of future technologies. Many of the practices and narratives that I discussed were not dependent on one particular technology. Participants probe into the workings of computation in an environment of perpetual change, where confirmations and disconfirmations of reality alternate, and where they are regularly exposed to new encounters with computation. They explore creative practices to establish a relationship with computational interlocutors and renegotiate the common stock of knowledge about a computed world. Further research is required into how the proliferation of mobile devices and artificial intelligence like voice-controlled virtual assistants alters and supplements the practices around the construction of knowledge and relationships to computational interlocutors that I have outlined here. But such research can draw on and extend the analysis provided in this thesis.

In the case of surveillance, political change is as prominent as technological transformation. When I conducted fieldwork for this thesis, Edward Snowden had not yet disclosed the depth and interconnections of a global surveillance infrastructure which was previously inconceivable for many people. The magnitude of his ongoing revelations that began in 2013 also had academic implications, prompting leading surveillance scholar David Lyon (2015) to write a book probing into *Surveillance After Snowden*. While this thesis could not incorporate these phenomena into the empirical work which predated the disclosures, further research is required to understand whether Snowden's revelations

have led to a changed cultural climate, to new perceptions of surveillance, and whether these revelations have given rise to new practices. At large, however, the Snowden revelations underscore the relevance of this research rather than undermine it, in particular as the empirical part of this thesis has been concerned with the role of computation in everyday life over the focus on surveillance per se.

9.7.4. Enlightenment and Computational Providence

Beyond the empirical limitations and areas for future research, there are much broader theoretical implications for the proliferation of computation as a social force that exceeded the scope of this thesis.

Computed sociality presents an obstacle to human agency that society has manufactured itself, paradoxically by following the Enlightenment principle of rationality to its ultimate conclusion. Max Weber wrote about the disenchantment of the world, where the rule of science usurped a worldview steeped in myth and blind belief. He stressed that through the rationality of science, in principle, human agents have become able to explain the workings of the world:

> "The increasing intellectualization and rationalization do not, therefore, indicate an increased and general knowledge of the conditions under which one lives. It means something else, namely, the knowledge or belief that if one but wished one could learn it at any time. Hence, it means that principally there are no mysterious incalculable forces that come into play, but rather that one can, in principle, master all things by calculation. This means that the world is disenchanted. One need no longer have recourse to magical means in order to master or implore the spirits, as did the savage, for whom such mysterious powers existed. Technical means and calculations perform the service." (Weber 1946: 139)

It is the ultimate continuation of these technical means and calculations in the form of computation which turns the disenchantment of the world into its opposite. While, as Hepp suggests "there is no sense that in the everyday world media technologies appear to be the product of 'divine intervention'" (2013: 59), computation is developing into its own, 'mysterious and incalculable force' in Weber's sense that erodes the ability to know the conditions under which one lives. Giddens has connected this disenchantment, understood as Enlightenment, with trust in human senses:

> "One type of certainty (divine law) was replaced by another (the certainty of our senses, of empirical observation), and divine providence was replaced by providential progress." (Giddens 1991: 48)

But if Enlightenment stands for replacing divine providence with providential progress, providential progress is being superseded by computational providence. I have alluded to this issue in my discussion of the communication problem inherent in the conditions of knowledge in *Chapter Three*. Beyond the analysis that I could provide in the limited space of this thesis, a much broader theoretical discussion is however necessary on the interplay between a logic of modern progress and the resurgence of faith and fate as social paradigms. This requires a critical review of the explanatory potential of theories of modernity and a reading of their existing critiques in a new light.

This dissertation could already offer a small step in this direction by showing how people's struggles to relate to a computational world spark explanatory frameworks and intersubjective narratives which are not technically correct assumptions about computation, but practices of meaning-making to facilitate social order. Berger and Luckmann's original case study for their account of social construction was religion, and amidst the denigration of human senses through the computational rendition of reality, future analysis of life in computed sociality may revert to that theme. The findings shown in this thesis also imply that future theoretical work under such a paradigm can benefit from avoiding the conceptual trap of 'docile bodies' (Foucault 1977) by taking serious from the outset the role of people as creative agents that find possibilities, whatever the conditions of reality.

References

Acquisti, Alessandro, and Ralph Gross. 2006. 'Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook'. In *Privacy Enhancing Technologies*, edited by George Danezis and Philippe Golle, 36–58. Lecture Notes in Computer Science 4258. Berlin: Springer.

Ailon, Nir, Bernard Chazelle, Kenneth L. Clarkson, Ding Liu, Wolfgang Mulzer, and C. Seshadhri. 2011. 'Self-Improving Algorithms'. *SIAM Journal on Computing* 40 (2): 350–75.

Alaimo, Cristina. 2014. 'Computational Consumption: Social Media and the Construction of Digital Consumers'. Phd, The London School of Economics and Political Science (LSE). http://etheses.lse.ac.uk/975/ (last accessed September 15, 2016).

Alaimo, Cristina, and Jannis Kallinikos. 2016. 'Encoding the Everyday: The Infrastructural Apparatus of Social Data'. In *Big Data Is Not a Monolith: Policies, Practices, and Problems*, edited by Cassidy R. Sugimoto, Hamid R. Ekbia, and Michael Mattioli, 77–90. Cambridge, MA: MIT Press.

Albrechtslund, Anders. 2008. 'Online Social Networking as Participatory Surveillance'. *First Monday* 13 (3).

Albro, Ed, Steve Fox, Steven Gray, Mark Sullivan, and Elsa Wenzel. 2011. 'Privacy Lost: The Amazing Benefits of the Completely Examined Life'. *PCWorld*, April 30. http://www.pcworld.com/article/226667/privacy_lost_the_amazing_benefits_of_the_completely_examined_life.html (last accessed September 15, 2016).

Aldridge, Irene. 2013. *High-Frequency Trading: A Practical Guide to Algorithmic Strategies and Trading Systems*. 2nd ed. Hoboken: John Wiley & Sons.

Allen, Mark 1994. '"See You in the City!" Perth's Citiplace and the Space of Surveillance'. In *Metropolis Now: Planning and the Urban in Contemporary Australia*, edited by Katherine Gibson and Sophie Watson, 137–47. Sydney: Pluto.

Andersen, Chris. 2008. 'The End of Theory: The Data Deluge Makes the Scientific Method Obsolete'. *WIRED*, June 23. http://archive.wired.com/science/discoveries/magazine/16-07/pb_theory# (accessed September 15, 2016).

Andreas Blass, and Yuri Gurevich. 2003. 'Algorithms: A Quest for Absolute Definitions'. *Bulletin of the EATCS* 81: 195–225.

Andreessen, Marc. 2009. 'Why Software Is Eating The World'. *Wall Street Journal*. http://www.wsj.com/articles/SB10001424053111903480904576512250915629460 (last accessed September 15, 2016).

Andrejevic, Mark. 2005. 'The Work of Watching One Another: Lateral Surveillance, Risk, and Governance'. *Surveillance & Society* 2 (4): 479–97.

———. 2007. *iSpy: Surveillance and Power in the Interactive Era*. Lawrence, KS: University Press of Kansas.

Aschermann, Tim. 2015. ‘Datenspuren Im Internet Löschen: So Geht’s’. *Chip*, October 4. http://praxistipps.chip.de/datenspuren-im-internet-loeschen-so-gehts_12369 (last accessed September 15, 2016).

Ayres, Ian. 2008. *Super Crunchers: How Anything Can Be Predicted*. London: John Murray.

Aytes, Ayhan. 2013. ‘Return of the Crowds: Mechanical Turk and Neoliberal States of Exception’. In *Digital Labour*, edited by Trebor Scholz, 79–97. New York, NY: Routledge.

Back, Les, and Nirmal Puwar. 2012. ‘A Manifesto for Live Methods: Provocations and Capacities’. *The Sociological Review* 60 (June): 6–17.

Ball, Kirstie, and Kevin D Haggerty. 2005. ‘Doing Surveillance Studies’. *Surveillance & Society* 3 (2/3): 129–38.

Barker, Timothy. 2011. ‘Aesthetics of the Error: Media Art, the Machine, the Unforeseen and the Errant.’ In *Error: Glitch, Noise, and Jam in New Media Cultures*, edited by Mark Nunes, 42–58. New York, NY: Continuum.

Barnard-Wills, David. 2011. ‘UK News Media Discourses of Surveillance’. *The Sociological Quarterly* 52 (4): 548–67.

Barnes, Susan B. 2006. ‘A Privacy Paradox: Social Networking in the United States’. *First Monday* 11 (9).

Barocas, Solon, Sophie Hood, and Malte Ziewitz. 2013. ‘Governing Algorithms: A Provocation Piece’. SSRN Scholarly Paper ID 2245322. Rochester, NY: Social Science Research Network. http://papers.ssrn.com/abstract=2245322 (last accessed September 15, 2016).

Barry, Andrew, Thomas Osborne, and Nikolas Rose. 1996. ‘Introduction’. In *Foucault and Political Reason: Liberalism, Neo-Liberalism, and Rationalities of Government*, edited by Andrew Barry, Thomas Osborne, and Nikolas Rose, 1–18. Chicago, IL: University of Chicago Press.

Baudrillard, Jean. 1998. *The Consumer Society: Myths and Structures*. 1st ed. London: SAGE.

Bauman, Zygmunt. 1988. *Freedom*. 1st ed. Minneapolis, MN: Open University Press.

———. 2000. *Liquid Modernity*. Chichester: John Wiley and Sons Ltd.

———. 2001. ‘Consuming Life’. *Journal of Consumer Culture* 1 (1): 9–29.

———. 2005. *Work, Consumerism and the New Poor*. Maidenhead: Open University Press.

Beck, Ulrich. 1992. *Risk Society: Towards a New Modernity*. London: SAGE.

Beck, Ulrich, and Wolfgang Bonß, eds. 2001. *Die Modernisierung der Moderne*. Frankfurt a. M.: Suhrkamp.

Beck, Ulrich, Wolfgang Bonß, and Christoph Lau. 2001. ‘Theorie Reflexiver Modernisierung – Fragestellungen, Hypothesen, Forschungsprogramme’. In *Die Modernisierung Der Moderne*, edited by Ulrich Beck and Wolfgang Bonß. Frankfurt a.M.: Suhrkamp.

Beck, Ulrich, Anthony Giddens, and Scott Lash. 1996. *Reflexive Modernisierung: Eine Kontroverse*. 6th ed. Frankfurt a.M.: Suhrkamp.

Beer, David. 2009. 'Power through the Algorithm? Participatory Web Cultures and the Technological Unconscious'. *New Media & Society* 11 (6): 985–1002.

———. 2014. *Punk Sociology*. Houndmills: Palgrave MacMillan.

Behrens, Roy R. 1999. 'The Role of Artists in Ship Camouflage During World War I'. *Leonardo* 32 (1): 53–59.

Bell, Daniel. 1976. *The Coming of Post-Industrial Society: A Venture in Social Forecasting*. Reissue. New York, NY: Basic Books.

Bell, Genevieve, and Paul Dourish. 2007. 'Yesterday's Tomorrows: Notes on Ubiquitous Computing's Dominant Vision'. *Personal Ubiquitous Computing* 11 (2): 133–143.

Benn, Gottfried. 1991. 'Der Radardenker'. In *Sämtliche Werke: Prosa 3* edited by Gerhard Schuster. Stuttgart: Klett.

Bentham, Jeremy. 2010. *The Panopticon Writings*. Edited by Miran Bozovic. London: Verso.

Berg, Bruce L. 2006. *Qualitative Research Methods for the Social Sciences*. 6th ed. Boston, MA: Allyn & Bacon.

Berger, Peter L., and Thomas Luckmann. (1966) 1991. *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*. London: Penguin.

Berlinski, David. 2000. *The Advent of the Algorithm: The Idea That Rules the World*. 1st ed. New York, NY: Houghton Mifflin Harcourt.

Berry, David M. 2011. 'The Computational Turn: Thinking About the Digital Humanities'. *Culture Machine* 12 (0).

Bhagwati, Sandeep. 2015. 'Musicking Beyond Algorithms'. In *Patterns of Intuition*, edited by Gerhard Nierhaus, 359–77. Dordrecht: Springer.

Blumer, Herbert. 1992. *Symbolic Interactionism: Perspective and Method*. Berkeley, CA: University of California Press.

Boase, Jeffrey. 2013. 'Implications of Software-Based Mobile Media for Social Research'. *Mobile Media & Communication* 1 (1): 57–62.

Bogard, William. 1996. *The Simulation of Surveillance: Hyper-Control in Telematic Societies*. Cambridge: Cambridge University Press.

———. 2006. 'Welcome to the Society of Control: The Simulation of Surveillance Revisited'. In *The New Politics of Surveillance and Visibility*, edited by Kevin D. Haggerty and Richard V. Ericson, 55–78. Toronto: Toronto University Press.

Bostrom, Nick. 2014. *Superintelligence: Paths, Dangers, Strategies*. Oxford: Oxford University Press.

Bousquet, G. 1998. 'Space, Power, Globalization: The Internet Symptom'. *Societies* 4: 105–13.

Bowker, Geoffrey C., Karen Baker, Florence Millerand, and David Ribes. 2010. 'Toward Information Infrastructure Studies: Ways of Knowing in a Networked

Environment'. In *International Handbook of Internet Research*, edited by Jeremy Hunsinger, Lisbeth Klastrup, and Matthew M. Allen, 97–117. Dordrecht: Springer.

Bowker, Geoffrey C., and Susan Leigh Star. 1999. *Sorting Things Out: Classification and Its Consequences*. Cambridge, MA: MIT Press.

boyd, danah. 2008. 'Taken Out of Context: American Teen Sociality in Networked Publics. PhD Dissertation'. University of California-Berkeley, School of Information.

boyd, danah, and Kate Crawford. 2012. 'Critical Questions for Big Data'. *Information, Communication & Society* 15 (5): 662–79.

boyd, danah, and Nicole B. Ellison. 2007. 'Social Network Sites: Definition, History, and Scholarship'. *Journal of Computer-Mediated Communication* 13 (1): 210–30.

Boyne, Richard. 2000. 'Post-Panopticism'. *Economy and Society* 29 (2): 285–307.

Brighenti, Andrea. 2007. 'Visibility A Category for the Social Sciences'. *Current Sociology* 55 (3): 323–42.

Bruns, Axel. 2013. 'Faster than the Speed of Print: Reconciling "big Data" Social Media Analysis and Academic Scholarship'. *First Monday* 18 (10).

Bryman, Alan. 1988. *Quantity and Quality in Social Research*. London: Routledge.

———. 2008. *Social Research Methods*. 3rd ed. Oxford: Oxford University Press.

Brynjolfsson, Erik, and Andrew Mcafee. 2014. *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*. New York, NY: W. W. Norton & Company.

Buchanan, Elizabeth A., and Michael Zimmer. 2015. 'Internet Research Ethics'. Edited by Edward N. Zalta. *The Stanford Encyclopedia of Philosophy*. http://plato.stanford.edu/archives/spr2015/entries/ethics-internet-research/ (last accessed September 15, 2016).

Bucher, Taina. 2012a. 'Want to Be on the Top? Algorithmic Power and the Threat of Invisibility on Facebook'. *New Media & Society* 14(7): 1164–1180.

———. 2012b. 'The Friendship Assemblage: Investigating Programmed Sociality on Facebook'. *Television & New Media*, 14 (6): 495-509.

———. 2012c. 'A Technicity of Attention: How Software "Makes Sense"'. *Culture Machine* 13: 1–23.

———. 2017 (forthcoming). 'The Algorithmic Imaginary: Exploring the Ordinary Affects of Facebook Algorithms'. *Information, Communication & Society* 20 (1): 30–44.

Burrell, Jenna. 2009. 'The Field Site as a Network: A Strategy for Locating Ethnographic Research'. *Field Methods* 21 (2): 181–99.

Bush, Vannevar. 1945. 'As We May Think'. *The Atlantic Monthly*. http://www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/303881/ (last accessed September 15, 2016).

Castells, Manuel. 2010. *The Rise of the Network Society: Information Age: Economy, Society, and Culture v. 1*. 2nd ed. Chichester: Wiley-Blackwell.

Charters, Elizabeth. 2003. ‘The Use of Think-Aloud Methods in Qualitative Research An Introduction to Think-Aloud Methods’. *Brock Education Journal* 12 (2): 68–82.

Cheal, David. 2005. *Dimensions of Sociological Theory*. Houndmills - Basingstoke: Palgrave Macmillan.

Clarke, Roger. 1988. ‘Information Technology and Dataveillance’. *Commun. ACM* 31 (5): 498–512.

———. 1994. ‘The Digital Persona and Its Application to Data Surveillance’. *The Information Society* 10 (2).

Cortesi, Aldo. 2010. *Sortvis: Sorting Algorithm Visualization*. http://sortvis.org.

Couldry, Nick. 2003. *Media Rituals*. London: Routledge.

Couldry, Nick, and Andreas Hepp. 2013. ‘Conceptualizing Mediatization: Contexts, Traditions, Arguments’. *Communication Theory* 23 (3): 191–202.

Couldry, Nick, and Alison Powell. 2014. ‘Big Data from the Bottom up’. *Big Data & Society* 1 (2).

Couldry, Nick, and Joseph Turow. 2014. ‘Advertising, Big Data, and the Clearance of the Public Realm: Marketers’ New Approaches to the Content Subsidy’. *International Journal of Communication* 8: 1710–26.

‘Council Orders Banksy Art Removal’. *BBC News* 2008, October 24. http://news.bbc.co.uk/1/hi/england/london/7688251.stm (last accessed September 15, 2016).

Crary, Jonathan. 2014. *24/7: Late Capitalism and the Ends of Sleep*. London: Verso.

Crawford, Kate. 2016. ‘Can an Algorithm Be Agonistic? Ten Scenes from Life in Calculated Publics’. *Science, Technology & Human Values*, 41(1), 77-92.

Crellin, Jonathan, T. Horn, and J. Preece. 1990. ‘Evaluating Evaluation: An Empirical Examination of Novel and Conventional Usability Evaluation Methods’. Conference paper. https://researchportal.port.ac.uk/portal/en/publications/evaluating-evaluation-an-empirical-examination-of-novel-and-conventional-usability-evaluation-methods(d5e4444f-5f32-4b82-8368-618aa33e1f01)/export.html (last accessed September 15, 2016).

Dandecker. 1994. *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day*. Cambridge: Polity.

Daston, Lorraine. 2013. ‘How Reason Became Rationality’. Max Planck Institute for the History of Science. http://www.mpiwg-berlin.mpg.de/en/research/projects/DeptII_Daston_Reason/index_html (last accessed September 15, 2016).

De Certeau, Michel. 1984. *The Practice of Everyday Life*. Berkeley, CA: University of California Press.

De Kerckhove, Derrick. 1997. *Connected Intelligence: The Arrival of the Web Society*. Toronto: Somerville House.

Deleuze, Gilles. 1992. ‘Postscript on the Societies of Control’. *October* 59: 3–7.

Deuze, Mark. 2012. *Media Life*. 1st ed. Cambridge: Polity.

Diebold, Francis X. 2012. ‘A Personal Perspective on the Origin(s) and Development of “Big Data”: The Phenomenon, the Term, and the Discipline, Second Version’. PIER Working Paper No. 13-003 ID 2202843. Rochester, NY: Social Science Research Network. http://papers.ssrn.com/abstract=2202843 (last accessed September 15, 2016).

Dijck, Jose Van. 2013. *The Culture of Connectivity: A Critical History Of Social Media*. Oxford: Oxford University Press.

Dörner, Stephan. 2015. ‘Gruscheln Vorbei Bei StudiVZ: Nach Zehn Jahren Wirkt Lea Verzweifelt - WELT’. *DIE WELT*, November 12. https://www.welt.de/wirtschaft/article148741374/Nach-zehn-Jahren-StudiVZ-wirkt-Lea-verzweifelt.html (last accessed September 15, 2016).

Drucker, Peter. 1969. ‘Knowledge Society’. *New Society* 13 (343): 629–31.

Dubrofsky, Rachel E. 2007. ‘Therapeutics of the Self Surveillance in the Service of the Therapeutic’. *Television & New Media* 8 (4): 263–84.

Dubrofsky, Rachel E., and Shoshana Amielle Magnet, eds. 2015. *Feminist Surveillance Studies*. Durham, NC: Duke University Press Books.

Duggan, Maeve. 2015. ‘The Demographics of Social Media Users’. *Pew Research Center: Internet, Science & Tech*. August 19. http://www.pewinternet.org/2015/08/19/the-demographics-of-social-media-users/ (last accessed September 15, 2016).

Durkheim, Emile. (1912) 1995. *The Elementary Forms of Religious Life*. Translated by Karen E. Fields. Reprint. New York, NY: Free Press.

Edwards, Paul N., Steven J. Jackson, Geoffrey C. Bowker, and Cory P. Knobel. 2007. ‘Understanding Infrastructure: Dynamics, Tensions, and Design’. Working Paper. http://deepblue.lib.umich.edu/handle/2027.42/49353 (last accessed September 15, 2016).

Eggers, Dave. 2014. *The Circle*. New York, NY: Vintage.

Ellul, Jacques. (1954) 1964. *The Technological Society*. Translated by John Wilkinson. New York, NY: Vintage.

Emirbayer, Mustafa, and Ann Mische. 1998. ‘What is Agency? *American Journal of Sociology* 103 (4): 962-1023.

Ericson, Richard V., and Kevin D. Haggerty. 2006. ‘The New Politics of Surveillance and Visibility’. In *The New Politics of Surveillance and Visibility*, edited by Richard V Ericson and Kevin D Haggerty, 3–33. Toronto: University of Toronto Press.

Ericsson, K. Anders, and Herbert A. Simon. 1980. ‘Verbal Reports as Data’. *Psychological Review* 87 (3): 215–51.

———. 1984. *Protocol Analysis: Verbal Reports as Data*. Cambridge, MA: MIT Press.

Eslami, Motahhare, Aimee Rickman, Kristen Vaccaro, Amirhossein Aleyasen, Andy Vuong, Karrie Karahalios, Kevin Hamilton, and Christian Sandvig. 2015. ‘“I Always Assumed That I Wasn’t Really That Close to [Her]”: Reasoning About Invisible Algorithms in News Feeds’. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 153–162. CHI ’15. New York, NY: ACM.

Facebook. 2015. ‘Facebook Q3 2015 Results’. Financial Earnings Report, Menlo Park, CA. http://files.shareholder.com/downloads/AMDA-NJ5DZ/1034414376x0x859098/DC6C9112-AFF6-4E76-9168-7DBA0D5FFDAB/FB_Q3_15_Earnings_Slides_FINAL.pdf (last accessed September 15, 2016).

———. 2016. ‘Facebook Q2 2016 Results’. Financial Earnings Report, Menlo Park, CA. https://s21.q4cdn.com/399680738/files/doc_presentations/FB-Q216-Earnings-Slides.pdf (last accessed September 15, 2016).

Flyvbjerg, Bent. 2006. ‘Five Misunderstandings about Case-Study Research’. In *Qualitative Research Practice*, edited by Clive Seale, Giampietro Gobo, Jaber F. Gubrium, and David Silverman, 390–404. London: SAGE.

Foth, Marcus, and Roger Burrows, eds. 2009. ‘Afterword: Urban Informatics and Social Ontology’. In *Handbook of Research on Urban Informatics: The Practice and Promise of the Real-Time City*, 450–54. Hershey, PA: IGI Global.

Foucault, Michel. 1976. *The History of Sexuality, Volume 1*. Harmondsworth: Penguin.

———. 1977. *Discipline and Punish: The Birth of the Prison*. New York, NY: Vintage.

———. 1984. ‘What is Enlightenment?’ In *The Foucault Reader*, edited by Paul Rabinow, 32–50. New York, NY: Pantheon Books. Cited in Hacking, Ian. 2002. *Historical Ontology*. Cambridge, MA: Harvard University Press.

———. 1991. ‘Governmentality’. In *The Foucault Effect: Studies in Governmentality*, edited by Graham Burchell, Colin Gordon, and Peter Miller, 87–104. Chicago, IL: University of Chicago Press.

Franklin, Ursula. 1996. ‘Stormy Weather: Conflicting Forces in the Information Society’. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/media/sp-d/archive/02_05_a_960918_05_e.asp (last accessed September 15, 2016).

Frith, Jordan. 2015. *Smartphones as Locative Media*. 1st ed. Cambridge: Polity.

Fuchs, Christian. 2013. ‘Political Economy and Surveillance Theory’. *Critical Sociology* 39 (5): 671–87.

Fulmer, Jeffrey. 2009. ‘What in the World Is Infrastructure?’ *PEI Infrastructure Investor*, no. July/August: 30–32.

Furlong, Kathryn. 2010. ‘Small Technologies, Big Change: Rethinking Infrastructure through STS and Geography’. *Progress in Human Geography* 34 (3).

Galloway, Alexander R. 2004. *Protocol: How Control Exists after Decentralization*. Cambridge, MA: MIT Press.

———. 2006. *Gaming: Essays on Algorithmic Culture*. Minneapolis, MN: University of Minnesota Press.

———. 2012. *The Interface Effect*. Cambridge: Polity.

Gandy, Oscar H. 1989. ‘The Surveillance Society: Information Technology and Bureaucratic Social Control’. *Journal of Communication* 39 (3): 61–76.

———. 1993. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview.

———. 2003. ‘Data Mining and Surveillance in the Post 9/11 Envrionment’. In *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age*, edited by Kirstie Ball and Frank Webster, 26–41. London: Pluto.

Gane, Nicholas, Couze Venn, Martin Hand, and Katherine Hayles. 2007. ‘Ubiquitous Surveillance: Interview with Katherine Hayles’. *Theory, Culture & Society* 24 (7–8): 349–58.

Gantz, John, and David Reinsel. 2011. ‘Extracting Value from Chaos’. Framingham, MA. http://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf (last accessed September 15, 2016).

Gardiner, Eileen. 2015. *The Digital Humanities*. New York, NY: Cambridge University Press.

Garfinkel, Harold. (1967) 1984. *Studies in Ethnomethodology*. 2nd rev. ed. Cambridge: Polity.

Geertz, Clifford. 2000. *Available Light: Anthropological Reflections on Philosophical Topics*. Princeton, NJ: Princeton University Press.

Giddens, Anthony. 1985. *The Nation-State and Violence*. Cambridge: Polity.

———. 1990. *The Consequences of Modernity*. Cambridge: Polity.

———. 1991. *Modernity and Self-Identity: Self and Society in the Late Modern Age*. Cambridge: Polity.

Gilbert, Brendan James. 2009. ‘Getting to Conscionable: Negotiating Virtual Worlds’ End User License Agreements without Getting Externally Regulated’. *Journal of International Commercial Law and Technology* 4 (4): 238–51.

Gill, Stephen. 1995. ‘The Global Panopticon? The Neoliberal State, Economic Life, and Democratic Surveillance’. *Alternatives: Global, Local, Political* 20 (1): 1–49.

Gillespie, Tarleton. 2014. ‘The Relevance of Algorithms’. In *Media Technologies: Essays on Communication, Materiality, and Society*, edited by Tarleton Gillespie, Pablo J. Boczkowski, and Kirsten A. Foot, 167–94. Cambridge, MA: MIT Press.

Gilroy, Paul. 1993. *The Black Atlantic - Modernity and Double Consciousness*. London: Verso.

Gitelman, Lisa, and Virginia Jackson. 2013. ‘Introduction’. In *‘Raw Data’ is an Oxymoron*, edited by Lisa Gitelman, 1–14. Cambridge, MA: MIT Press.

Glaser, Barney G., and Anselm L. Strauss. 1967. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Chicago, IL: Transaction.

Glickman, Seth W., Sam Galhenage, Lindsay McNair, Zachry Barber, Keyur Patel, Kevin A. Schulman, and John G. McHutchison. 2012. ‘The Potential Influence of Internet-Based Social Networking on the Conduct of Clinical Research Studies’. *Journal of Empirical Research on Human Research Ethics: JERHRE* 7 (1): 71–80.

Goffman, Erving. (1959) 1990. *The Presentation of Self in Everyday Life*. New edition. London: Penguin.

———. 1961. *Asylums: Essays on the Social Situation of Mental Patients and Other Inmates*. 1st ed. Garden City, NY: Anchor Books.

———. (1967) 2003. *Interaction Ritual: Essays on Face-to-Face Behavior*. New York, NY: Pantheon.

———. 1971. *Relations in Public*. New York, NY: Basic.

Gooding, Paul. 2012. 'Mass Digitization and the Garbage Dump: The Conflicting Needs of Quantitative and Qualitative Methods'. *Literary and Linguistic Computing* 28 (3): 425-431.

Goriunova, Olga, and Alexei Shulgin. 2008. 'Glitch'. In *Software Studies: A Lexicon*, edited by Matthew Fuller, 110–18. Cambridge, MA: MIT Press.

Graham, Stephen, and Simon Marvin. 2001. *Splintering Urbanism: Networked Infrastructures, Technological Mobilities and the Urban Condition*. New York, NY: Routledge.

Groombridge, Nic. 2002. 'Crime Control or Crime Culture TV?' *Surveillance & Society* 1 (1): 30–46.

Hacking, Ian. 1990. *The Taming of Chance*. Cambridge: Cambridge University Press.

———. 2002. *Historical Ontology*. Cambridge, MA: Harvard University Press.

———. 2004. 'Between Michel Foucault and Erving Goffman: Between Discourse in the Abstract and Face-to-Face Interaction'. *Economy and Society* 33 (3): 277–302.

Haggerty, Kevin D. 2006. 'Tear down the Walls! On Demolishing the Panopticon'. In *Theorizing Surveillance: The Panopticon and Beyond*, edited by David Lyon, 23–45. Cullompton: Willan.

Haggerty, Kevin D., and Richard V. Ericson. 2000. 'The Surveillant Assemblage'. *The British Journal of Sociology* 51 (4): 605–22.

Halavais, Alexander. 2009. *Search Engine Society*. Cambridge: Polity Press.

Hammersley, Martyn. 1992. *What's Wrong With Ethnography?: Methodological Explorations*. 1st ed. London: Routledge.

Hammersley, Martyn, and Paul Atkinson. 2007. *Ethnography: Principles in Practice*. 3rd rev. ed. London: Routledge.

Hayles, N. Katherine. 2005. *My Mother Was a Computer: Digital Subjects and Literary Texts*. Chicago, IL: University of Chicago Press.

———. 2006. 'Unfinished Work: From Cyborg to Cognisphere'. *Theory, Culture & Society* 23 (7–8): 159–66.

'Hello, Larry! Google's Page on Negativity, Laws, and Competitors'. 2013. *PCWorld*. May 15. http://www.pcworld.com/article/2038841/hello-larry-googles-page-on-negativity-laws-and-competitors.html (last accessed September 15, 2016).

Helsper, Ellen Johanna, and Rebecca Eynon. 2010. 'Digital Natives: Where Is the Evidence?' *British Educational Research Journal* 36 (3): 503–20.

Hepp, Andreas. 2013. *Cultures of Mediatization*. 1st ed. Cambridge: Polity.

Hier, Sean P., and Josh Greenberg. 2009. 'The Politics of Surveillance: Power, Paradigms, and the Field of Visibility'. In *Surveillance: Power, Problems, and Politics*, edited by Sean P. Hier and Josh Greenberg, 14–29. Vancouver: University of British Columbia Press.

Hilbert, Martin, and Priscila López. 2011. ‘The World’s Technological Capacity to Store, Communicate, and Compute Information’. *Science* 332 (6025): 60–65.

Hine, Christine, ed. 2005. *Virtual Methods: Issues in Social Research on the Internet*. New York, NY: Berg.

Holstein, James A., and Jaber F. Gubrium. 1994. ‘Phenomenology, Ethnomethodology, and Interpretative Practice’. In *Handbook of Qualitative Research*, edited by Norman K. Denzin and Yvonna S. Lincoln, 262–72. Thousand Oaks, CA: SAGE.

———. 2004. ‘The Active Interview’. In *Qualitative Research: Theory, Method and Practice*, edited by David Silverman, 2nd ed., 140–61. London: SAGE.

Horst, Heather A., and Daniel Miller. 2012. ‘The Digital and the Human: A Prospectus for Digital Anthropology’. In *Digital Anthropology*, edited by Heather A. Horst and Daniel Miller, 3–35. London: Berg.

‘How to Stop LinkedIn from Using YOUR Name & Photo to Advertise’. 2011. *LIFE, TIPS ... and Interesting News*. September 28. http://tempguest.blogspot.it/2011/09/how-to-stop-linkedin-from-using-your.html (last accessed September 15, 2016).

Ignatieff, Michael. 1978. *A Just Measure of Pain: The Penitentiary in the Industrial Revolution 1750-1850*. New York, NY: Pantheon.

Innis, Robert E. 1984. ‘Technics and the Bias of Perception’. *Philosophy & Social Criticism* 10 (1): 67–89.

Instagram. 2016. ‘Instagram Today: 500 Million Windows to the World’. 2016. *Instagram Blog*. June 21. http://blog.instagram.com/post/146255204757/160621-news (last accessed September 15, 2016).

Introna, Lucas D., and Amy Gibbons. 2009. ‘Networks and Resistance: Investigating Online Advocacy Networks as a Modality for Resisting State Surveillance’. *Surveillance & Society* 6 (3): 233–58.

Isin, Engin F., and Greg M. Nielsen, eds. 2008. *Acts of Citizenship*. London: Zed.

Jaeger, Paul T., Jimmy Lin, Justin M. Grimes, and Shannon N. Simmons. 2009. ‘Where Is the Cloud? Geography, Economics, Environment, and Jurisdiction in Cloud Computing’. *First Monday* 14 (5).

Jay, Martin. 1994. *Downcast Eyes: The Denigration of Vision in Twentieth-Century French Thought*. Berkeley, CA.: University of California Press.

Joas, Hans. 1996. *Creativity of Action*. Cambridge: Polity.

Jones, Sydney, and Susannah Fox. 2015. ‘Generations Online in 2009’. Pew Research Center. http://www.pewinternet.org/2009/01/28/generations-online-in-2009/ (last accessed September 15, 2016).

Josselson, Ruthellen H., and Amia Lieblich. 2003. ‘A Framework for Narrative Research Proposals in Psychology’. In *Up Close and Personal: The Teaching and Learning of Narrative Research*, edited by Ruthellen H. Josselson, Amia Lieblich, and Dan P. McAdams, 259–74. Washington, DC: American Psychological Association.

Juvenal. 1998. *The Sixteen Satires*. Edited by Peter Green. 3rd rev. ed. London: Penguin Classics.

Kallinikos, Jannis. 2009. ‘On the Computational Rendition of Reality: Artefacts and Human Agency’. *Organization* 16 (2): 183–202.

Kallinikos, Jannis, and Niccolò Tempini. 2014. ‘Patient Data as Medical Facts: Social Media Practices as a Foundation for Medical Knowledge Creation’. *Information Systems Research* 25 (4): 817–33.

Karpf, David. 2010. ‘Online Political Mobilization from the Advocacy Group’s Perspective: Looking Beyond Clicktivism’. *Policy & Internet* 2 (4): 7–41.

Katz, Randy H. 2009. ‘Tech Titans Building Boom’. February 1. http://spectrum.ieee.org/green-tech/buildings/tech-titans-building-boom (last accessed September 15, 2016).

Kemple, Thomas, and Laura Huey. 2005. ‘Observing the Observers: Researching Surveillance and Counter-Surveillance on “Skid Row”’. *Surveillance & Society* 3 (2/3): 139–57.

Kennedy, Helen, Thomas Poell, and Jose van Dijck. 2015. ‘Data and Agency’. *Big Data & Society* 2 (2).

Khunkham, Kritsanarat. 2014. ‘Hilfe, Ich Bin Aus Dem Newsfeed Gefallen!’ *Die Welt*, January 20. http://www.welt.de/debatte/kolumnen/der-onliner/article124029185/Hilfe-ich-bin-aus-dem-Newsfeed-gefallen.html (last accessed September 15, 2016).

King, Gary, Robert O. Keohane, and Sidney Verba. 1994. *Designing Social Inquiry: Scientific Inference in Qualitative Research*. Princeton, NJ: Princeton University Press.

King, Storm A. 1996. ‘Researching Internet Communities: Proposed Ethical Guidelines for the Reporting of Results’. *The Information Society* 12 (2): 119–28.

Kiousis, Spiro. 2002. ‘Interactivity: A Concept Explication’. *New Media & Society* 4 (3): 355–83.

Kitchin, Rob. 2014. *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*. Thousand Oaks, CA: SAGE.

Knapp, Daniel. 2009. ‘Limits of Big Brother in the online data industry’. *Screen Digest*, September Issue: last page.

Knapp, Daniel, and Eleni Marouli. 2015. ‘Video Advertising in Europe: The Road to Programmatic Ubiquity’. Industry White Paper. London: SpotX & IHS. https://www.spotxchange.com/resources/downloads/research/ihs-report-video-advertising-in-europe-the-road-to-programmatic-ubiquity/ (last accessed September 15, 2016).

Koskela, Hille. 2003. ‘’Cam Era’ - The Contemporary Urban Panopticon’. *Surveillance & Society* 1 (3): 292–313.

Kraut, Robert, Judith Olson, Mahzarin Banaji, Amy Bruckman, Jeffrey Cohen, and Mick Couper. 2004. ‘Psychological Research Online: Report of Board of Scientific Affairs’ Advisory Group on the Conduct of Research on the Internet’. *American Psychologist* 59 (2): 105–17.

Kuechemann, Fridtjof. 2012. ‘Ist Etwas Umsonst, Sind Deine Daten Der Preis’. *Frankfurter Allgemeine Zeitung*, March 28. http://www.faz.net/aktuell/feuilleton/medien/online-spiel-data-dealer-ist-etwas-

umsonst-sind-deine-daten-der-preis-11699515.html (last accessed September 15, 2016).

Lace, Susanne. 2005a. ‘Introduction’. In *The Glass Consumer: Life in a Surveillance Society*, edited by Susanne Lace, 1–16. Bristol: Policy.

———. 2005b. ‘The New Personal Information Agenda’. In *The Glass Consumer: Life in a Surveillance Society*, edited by Susanne Lace, 207–46. Bristol: Policy.

Lash, Scott. 2005. ‘Intensive Media - Modernity and Algorithm (Draft)’. In *Roundable, Research Architecture*. London: Centre for Research Architecture, Goldsmiths’ College, University of London. http://roundtable.kein.org/node/125 (last accessed September 15, 2016).

———. 2007. ‘Power after Hegemony Cultural Studies in Mutation?’ *Theory, Culture & Society* 24 (3): 55–78.

Latour, Bruno. 2015. *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford: Oxford University Press.

Latour, Bruno, Pablo Jensen, Tommaso Venturini, Sébastian Grauwin, and Dominique Boullier. 2012. ‘“The Whole Is Always Smaller than Its Parts” – a Digital Test of Gabriel Tardes’ Monads’. *The British Journal of Sociology* 63 (4): 590–615.

Laurent, Samuel. 2009. ‘Un internaute mis à nu à partir de ses traces sur le web’. *Le Figaro*, January 15, sec. High-Tech. http://www.lefigaro.fr/secteur/high-tech/2009/01/15/01007-20090115ARTFIG00625-un-internaute-mis-a-nu-a-partir-de-ses-traces-sur-le-web-.php (last accessed September 15, 2016).

Levin, Thomas Y. 2002. ‘Rhetoric of the Temporal Index: Surveillant Narration and the Cinema of “real Time”’. In *CTRL [SPACE]: Rhetorics of Surveillance from Bentham to Big Brother*, edited by Thomas Y. Levin, Ursula Frohne, and Peter Weibel, 1st ed., 578–93. Karlsruhe: MIT Press.

Lewis, Clayton H. 1982. ‘Using the “Thinking Aloud” Method In Cognitive Interface Design’. IBM Research Report RC 9265, Yorktown Heights, NY: IBM.

Lewis, Michael. 2014. *Flash Boys: Cracking the Money Code*. New York, NY: Allen Lane.

Lischka, Konrad. 2010. ‘Street-View-Debatte: Brüllen Gegen Google’. *Spiegel Online*, August 2. http://www.spiegel.de/netzwelt/netzpolitik/street-view-debatte-bruellen-gegen-google-a-676609.html (last accessed September 15, 2016).

Lischka, Konrad, Ole Reissman, and Matthias Kremp. 2011. ‘Datensammler Apple: Your iPhone Is Watching You’. *Spiegel Online*, April 20. http://www.spiegel.de/netzwelt/web/datensammler-apple-your-iphone-is-watching-you-a-758320.html (last accessed September 15, 2016).

Livingstone, Sonia. 2008. ‘Taking Risky Opportunities in Youthful Content Creation: Teenagers’ Use of Social Networking Sites for Intimacy, Privacy and Self-Expression’. *New Media & Society* 10 (3): 393–411.

Lobe, Adrian. 2015. ‘Für Computer Sind Menschen Wie Gorillas’. *Frankfurter Allgemeine Zeitung*, September 19. http://www.faz.net/aktuell/feuilleton/algorithmen-praegen-alltag-und-verstaerken-klischees-13805022.html (last accessed September 15, 2016).

Loewenstein, George F., Christopher K. Hsee, Elke U. Weber, and Ned Welch. 2001. 'Risk as Feelings'. *Psychological Bulletin* 127: 267-86.

Lovink, Geert. 2010. Interview by Victoria Lynn. *Broadsheet Magazine* February 2010. http://networkcultures.org/geert/interview-with-geert-lovink-by-victoria-lynn/ (last accessed September 15, 2016).

Lupton, Deborah. 2015. *Digital Sociology*. Abingdon: Routledge.

Lyon, David. 1988. *The Information Society: Issues and Illusions*. Cambridge: Polity.

———. 1994. *The Electronic Eye: The Rise of Surveillance Society: Computers and Social Control in Context*. Cambridge: Polity.

———. 2001. *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.

———. 2002. 'Surveillance Studies: Understanding Visibility, Mobility and the Phenetic Fix'. *Surveillance & Society* 1 (1): 1–7.

———. 2003. 'Surveillance as Social Sorting: Computer Codes and Mobile Bodies'. In *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, edited by David Lyon, 11–30. New York, NY: Routledge.

———. 2006. 'The Search for Surveillance Theories'. In *Theorizing Surveillance – The Panopticon and Beyond*, edited by David Lyon, 3–20. Cullompton: Willan.

———. 2007. *Surveillance Studies: An Overview*. 1st ed. Cambridge: Polity.

———. 2015. *Surveillance After Snowden*. 1st ed. Cambridge: Polity.

Mackenzie, Adrian, and Ruth McNally. 2013. 'Living Multiples: How Large-Scale Scientific Data-Mining Pursues Identity and Differences'. *Theory, Culture & Society* 30 (4): 72–91.

Macpherson, C. B. (1962) 2011. *The Political Theory of Possessive Individualism: Hobbes to Locke*. Reprint. Don Mills: OUP Canada.

Mahrt, Merja, and Michael Scharkow. 2013. 'The Value of Big Data in Digital Media Research'. *Journal of Broadcasting & Electronic Media* 57 (1): 20–33.

Mann, Steve, Jason Nolan, and Barry Wellman. 2003. 'Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments.' *Surveillance & Society* 1 (3): 331–55.

Manon, Hugh S., and Daniel Temkin. 2011. 'Notes on Glitch'. *World Picture* 6.

Manovich, Lev. 2012. 'Trending: The Promises and the Challenges of Big Social Data'. In *Debates in the Digital Humanities*, edited by Matthew K. Gold, 460–75. Minneapolis, MN: University of Minnesota Press.

———. 2013. *Software Takes Command*. Int. ed. New York, NY: Bloomsbury Academic.

Mansell, Robin. 2009. *The Information Society, Vol. 1*. Milton Park: Routledge.

Marcus, George E., and Erkan Saka. 2006. 'Assemblage'. *Theory, Culture & Society* 23 (2–3): 101–6.

Marcus, George E. 1997. 'The Uses of Complicity in the Changing Mise-En-Scène of Anthropological Fieldwork'. *Representations*, no. 59: 85–108.

Marichal, José. 2012. *Facebook Democracy: The Architecture of Disclosure and the Threat to Public Life*. Abingdon, Oxon: Routledge.

Markoff, John. 2015. *Machines of Loving Grace: The Quest for Common Ground Between Humans and Robots*. 1st ed. New York, NY: HarperCollins.

Marks, Laura. 2003. 'Invisible Media'. In *New Media: Theories and Practices of Digitextuality*, edited by Anna Everett and John T Caldwell, 33–46. New York, NY: Routledge.

———. 2010. *Enfoldment and Infinity: An Islamic Genealogy of New Media Art*. Cambridge, MA: MIT Press.

Marks, Peter. 2005. 'Imagining Surveillance: Utopian Visions and Surveillance Studies'. *Surveillance & Society* 3 (2/3).

Marx, Gary T. 1985. 'The Surveillance Society: The Threat of 1984-Style Techniques'. *The Futurist* 21 (6).

———. 2002. 'What's New About the "New Surveillance"? Classifying for Change and Continuity'. *Surveillance & Society* 1 (1): 9–29.

———. 2003. 'A Tack in the Shoe: Neutralizing and Resisting the New Surveillance'. *Journal of Social Issue* 59 (2): 369–90.

———. 2009. 'Soul Train: The New Surveillance in Popular Music'. In *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, edited by Ian Kerr, Valerie Steeves, and Carole Lucock, 1st ed. Oxford: Oxford University Press.

Mason, Jennifer. 2002. *Qualitative Researching*. 2nd rev. ed. London: SAGE.

Mathiesen, Thomas. 1997. 'The Viewer Society Michel Foucault's `Panopticon' Revisited'. *Theoretical Criminology* 1 (2): 215–34.

Mayer-Schönberger, Viktor, and Kenneth Cukier. 2013. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. 1st ed. Boston, MA: Houghton Mifflin Harcourt.

McKie, Linda, and Louise Ryan. 2012. 'Exploring Trends and Challenges in Sociological Research'. *Sociology* 46 (6): 1–7.

McNay, Lois. 1994. *Foucault: A Critical Introduction*. New York, NY: Continuum.

Mead, George Herbert. (1934) 2015. *Mind, Self, and Society*. Edited by Charles W. Morris. Chicago, IL: University of Chicago Press.

Meckel, Miriam. 2011a. *NEXT: Erinnerungen an eine Zukunft ohne uns*. Reinbek: rororo.

———. 2011b. Im Gespräch: Miriam Meckel: Werden wir alle zu Algorithmen? Interview by Christian Geyer and Daniel Haas. http://www.faz.net/aktuell/feuilleton/debatten/digitales-denken/im-gespraech-miriam-meckel-werden-wir-alle-zu-algorithmen-11228310.html?printPagedArticle=true#pageIndex_2 (last accessed September 15, 2016).

Meyrowitz, Joshua. 1985. *No Sense of Place: The Impact of Electronic Media on Social Behavior*. Oxford: Oxford University Press.

Miller, Daniel. 2011. *Tales from Facebook*. 1st ed. Cambridge: Polity.

Moor, James H. 1985. 'What Is Computer Ethics?' *Metaphilosophy* 16 (4): 266–75.

Moretti, Franco. 2013. *Distant Reading*. London: Verso.

Morley, David. 1980. *The 'Nationwide' Audience: Structure and Decoding*. London: British Film Institute.

———. 1992. *Television, Audiences and Cultural Studies*. 1st ed. London: Routledge.

Morozov, Evgeny. 2011. *The Net Delusion: The Dark Side of Internet Freedom*. New York, NY: Perseus.

———. 2013a. 'The Perils of Perfection'. *New York Times*, March 3.

———. 2013b. *To Save Everything, Click Here: The Folly of Technological Solutionism*. New York, NY: PublicAffairs.

———. 2015. 'Europe Is Wrong to Take a Sledgehammer to Big Google'. *Financial Times*, January 11. http://www.ft.com/cms/s/0/0b758868-86e5-11e4-8a51-00144feabdc0.html?siteedition=uk#axzz3foF9B0Mp (last accessed September 15, 2016).

Mosco, Vincent. 1989. *The Pay-Per Society: Computers and Communication in the Information Age*. Norwood, NJ: Praeger.

Nassehi, Armin. 1997. 'Risikogesellschaft'. In *Soziologische Gesellschaftsbegriffe. Konzepte Moderner Zeitdiagnosen*, edited by Georg Kneer, Armin Nassehi, and Markus Schroer, 252. München: W. Fink.

Nissenbaum, Helen. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law Books.

Noble, David F. 1986. *Forces of Production: A Social History of Industrial Automation*. New York, NY: Oxford University Press.

Norris, Clive, and Gary Armstrong. 1999. *The Maximum Surveillance Society: The Rise of CCTV*. Oxford: Bloomsbury Academic.

O'Connor, Sarah. 2016. 'When Your Boss Is an Algorithm'. *Financial Times*, September 8. https://www.ft.com/content/88fdc58e-754f-11e6-b60a-de4532d5ea35 (last accessed September 15, 2016).

Ouellette, Laurie, and James Hay. 2008. *Better Living Through Reality TV: Television and Post-Welfare Citizenship*. Malden, MA: Wiley-Blackwell.

Ovide, Shira, and Mark Peters. 2014. 'Why Data Centers Collect Big Tax Breaks'. *Wall Street Journal*, November 14, sec. Tech. http://www.wsj.com/articles/why-data-centers-collect-big-tax-breaks-1416000057 (last accessed September 15, 2016).

Pantzar, Mika, and Elizabeth Shove. 2005. 'Metering Everyday Life.' *17th Annual SASE Meeting*. Budapest.

Page, Larry. 2013. 'Google I/O 2013 Keynote Q&A'. presented at the Google I/O 2013, Moscone West Convention Center, San Francisco, May 15. https://www.youtube.com/watch?v=AfK8h73bb-o&feature=youtu.be&t=48 (last accessed September 15, 2016).

Palfrey, John, and Urs Gasser. 2008. *Born Digital: Understanding the First Generation of Digital Natives*. New York, NY: Basic Books.

Palmer, Gareth. 2002. ‘Big Brother An Experiment in Governance’. *Television & New Media* 3 (3): 295–310.

Pariser, Eli. 2011. *The Filter Bubble: What the Internet Is Hiding from You*. Penguin Press.

Parks, Lisa. 2012. ‘Technostruggles and the Satellite Dish: A Populist Approach to Infrastructure’. In *Cultural Technologies: The Shaping of Culture in Media and Society*, edited by Göran Bolin. New York, NY: Routledge.

Parsons, Talcott. 2012. *The Social System*. New York, NY: Free Press.

Pasquale, Frank. 2015. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press.

Patane, Matthew, and Timothy Meinch. 2015. ‘Register Exclusive: Microsoft Apparently behind Data Center’. *Des Moines Register*. http://www.desmoinesregister.com/story/news/2014/04/13/microsoft-apparently-behind-west-des-moines-data-center/7662083/ (last accessed September 15, 2016).

Patton, Michael Quinn. 2015. *Qualitative Research & Evaluation Methods: Integrating Theory and Practice*. 4th ed. Thousand Oaks, CA: SAGE.

Patton, Paul. 1994. ‘Metamorpho-Logic: Bodies and Powers in A Thousand Plateaus’. *Journal of the British Society for Phenomenology* 25 (2): 157–69.

Petras, John W., and Bernard N. Meltzer. 2003. ‘Theoretical and Ideological Variations in Contemporary Interactionism’. In *Symbolic Interaction: An Introduction to Social Psychology*, edited by Larry T. Reynolds and Nancy J. Herman, 55–63. Walnut Creek, CA: AltaMira.

Pink, Sarah. 2009. *Doing Sensory Ethnography*. London: SAGE.

Poggi, Jeanine. 2014. ‘The CMO’s Guide to Addressable TV Advertising’. *Advertising Age*, February 19. http://adage.com/article/cmo-strategy/cmo-s-guide-addressable-tv-advertising/291728/ (last accessed September 15, 2016).

Pool, Ithiel de Sola. (1983) 1984. *Technologies of Freedom*. Reprint. Cambridge, MA.: Belknap.

Poster, Mark. 1990. *The Mode of Information: Poststructuralism and Social Context*. Chicago, IL: University of Chicago Press.

———. 1996. ‘Databases as Discourse, Or, Electronic Interpellations’. In *Computers, Surveillance, and Privacy*, edited by David Lyon and Elia Zureik, 175–92. Minneapolis, MN: University of Minnesota Press.

Prensky, Marc. 2001. ‘Digital Natives, Digital Immigrants Part 1’. *On the Horizon* 9 (5): 1–6.

Pridmore, James. 2013. ‘Collaborative Surveillance: Configuring Contemporary Marketing Practice’. In *The Surveillance-Industrial Complex: A Political Economy of Surveillance*, edited by Kirstie Ball and Laureen Snider, 107–21. London: Routledge.

‘Privatsphäre: Magazin Veröffentlicht Profil von Ahnungslosem Web-Nutzer’, *Spiegel Online* 2009, January 15. http://www.spiegel.de/netzwelt/web/privatsphaere-magazin-veroeffentlicht-profil-von-ahnungslosem-web-nutzer-a-601559.html (last accessed September 15, 2016).

Rankin, J. Mark. 1988. ‘Designing Thinking-Aloud Studies in ESL Reading’. *Reading in a Foreign Language* 4: 119–32.

Rappaport, Stephen D. 2011. *Listen First!: Turning Social Media Conversations Into Business Advantage*. Hoboken, NJ: Wiley.

Repstad, Pål, and Inger Furseth. 2013. *An Introduction to the Sociology of Religion: Classical and Contemporary Perspectives*. Aldershot: Ashgate.

Rheingold, Howard. 2000. *The Virtual Community: Homesteadning on the Electronic Frontier*. Cambridge, MA: MIT Press.

Riesebrodt, Martin. 2007. *Cultus und Heilsversprechen: Eine Theorie der Religionen*. 1st ed. München: C.H.Beck.

Ritchie, Jane, Jane Lewis, Carol McNaughton Nicholls, and Rachel Ormston, eds. 2014. *Qualitative Research Practice: A Guide for Social Science Students and Researchers*. 2nd ed. London: SAGE.

Ritzer, George. 2010. *Sociological Theory*. 8th ed. New York, NY: McGraw-Hill Higher Education.

Ritzer, George, and Nathan Jurgenson. 2010. ‘Production, Consumption, Prosumption: The Nature of Capitalism in the Age of the Digital “prosumer”’. *Journal of Consumer Culture* 10 (1): 13–36.

Rogers, Richard. 2013. *Digital Methods*. Cambridge, MA: MIT Press.

Rohbeck, Johannes. 1993. *Technologische Urteilskraft. Zu Einer Ethik Technischen Handelns.* Frankfurt a.M.: Suhrkamp.

Röhle, Theo. 2010. *Der Google-Komplex: Über Macht Im Zeitalter Des Internets*. Bielefeld: transcript Verlag.

Rose, Nikolas. 1999. *Powers of Freedom: Reframing Political Thought*. Cambridge: Cambridge University Press.

Roth, Anne. 2011. ‘Bitte Recht Freundlich’. *Der Freitag*, October 21. https://www.freitag.de/autoren/der-freitag/bitte-recht-freundlich (last accessed September 15, 2016).

Ruhleder, Karen, and Susan Leigh Star. 1996. ‘Steps towards an Ecology of Infrastructure: Design and Access for Large-Scale Collaborative Systems’. *Information Systems Research* 7 (1): 111–34.

Rule, James B. 2009. *Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience*. 1st ed. Oxford: Oxford University Press.

Ruppert, Evelyn, John Law, and Mike Savage. 2013. ‘Reassembling Social Science Methods: The Challenge of Digital Devices’. *Theory, Culture & Society* 30 (4): 22–46.

Rushkoff, Douglas. 2011. *Program or Be Programmed: Ten Commands for a Digital Age*. Berkeley, CA: Soft Skull.

Sanchez, Andrés. 2009. ‘Facebook Feeding Frenzy: Resistance-through-Distance and Resistance-through-Persistence in the Societied Network’. *Surveillance & Society* 6 (3): 275–93.

Sartre, Jean-Paul. (1943) 1993. *Being and Nothingness*. Translated by Hazel E. Barnes. Reprint. New York, NY: Washington Square Press.

Sassen, Saskia. 2005. 'The Global City: Introducing a Concept'. *Brown Journal of World Affairs* XI (2): 27–43.

Savage, Mike. 2013. 'The "Social Life of Methods": A Critical Introduction'. *Theory, Culture & Society* 30 (4): 3–21.

Savage, Mike, and Roger Burrows. 2007. 'The Coming Crisis of Empirical Sociology'. *Sociology* 41 (5): 885–99.

———. 2009. 'Some Further Reflections on the Coming Crisis of Empirical Sociology'. *Sociology* 43 (4): 762–72.

Schelsky, Helmut. 1965. 'Die Paradoxien Des Alters in Der Modernen Gesellschaft'. In *Auf Der Suche Nach Der Wirklichkeit*, edited by Helmut Schelsky, 198–221. Düsseldorf: Diedrichs.

Schirrmacher, Frank. 2009. *Payback: Warum wir im Informationszeitalter gezwungen sind zu tun, was wir nicht tun wollen, und wie wir die Kontrolle über unser Denken zurückgewinnen*. 2nd ed. München: Karl Blessing Verlag.

Schmidt, Jan-Hinrik. 2009. 'Tagung zur Medienethik im Web 2.0'. Academic Blog. *Schmidt mit Dete*. December 2. http://www.schmidtmitdete.de/archives/416 (last accessed September 15, 2016).

Schneier, Bruce. 2015. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. 1st ed. New York, NY: W. W. Norton & Company.

Scholz, Trebor. 2008. 'Market Ideology and the Myths of Web 2.0'. *First Monday* 13 (3). http://firstmonday.org/ojs/index.php/fm/article/view/2138 (last accessed September 15, 2016).

———. 2013. *Digital Labor: The Internet as Playground and Factory*. 1st ed. New York, NY: Routledge.

Schutt, Russel K. 2014. *Investigating the Social World: The Process and Practice of Research*. 8th ed. Los Angeles, CA: SAGE.

Selwyn, Neil. 2009. 'The Digital Native – Myth and Reality'. *Aslib Proceedings* 61 (4): 364–79.

Sennett, Richard. 1998. *The Corrosion of Character: The Personal Consequences of Work in the New Capitalism*. New York, NY: W. W. Norton & Company.

Serres, Michel. 1989. 'Panoptic Theory'. In *The Limits of Theory*, edited by Thomas M. Kavanagh, 25–50. Stanford, CA: Stanford University Press.

Sewell, Jr., William H. 1992. 'A Theory of Structure: Duality, Agency, and Transformation'. *American Journal of Sociology* 98 (1): 1–29.

———. 2005. *Logics of History: Social Theory and Social Transformation*. Chicago: University of Chicago Press.

Silverman, David. 2006. *Interpreting Qualitative Data: Methods for Analyzing Talk, Text and Interaction*. 3rd ed. London: SAGE.

Simmel, Georg. 1971. ‘The Stranger’. In *Georg Simmel on Individuality and Social Forms*, edited by Donald N Levine, 143–50. Chicago, IL: University of Chicago Press.

‘SimpleWash’. 2016. *SimpleWash*. http://www.simplewa.sh/ (last accessed September 15, 2016).

Slezak, Peter. 1989. ‘Scientific Discovery by Computer as Empirical Refutation of the Strong Programme’. *Social Studies of Science* 19 (4): 563–600.

Slovic, Paul. 1999. ‘Trust, Emotion, Sex, Politics, and Science: Surveying the Risk-Assessment Battlefield’. *Risk Analysis* 19 (4): 689–701.

Solove, Daniel J. 2004. *The Digital Person: Technology And Privacy In The Information Age*. New York, NY: NYU Press.

———. 2011. *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven, CT: Yale University Press.

Stake, Robert. 1994. ‘Case Studies’. In *Handbook of Qualitative Research*, edited by Norman K. Denzin and Yvonna S. Lincoln, 236–47. Thousand Oaks, CA: SAGE.

Staples, William G. (2000) 2013. *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*. 2nd ed. Lanham: Rowman & Littlefield.

Steiner, Christopher. 2012. *Automate This: How Algorithms Came to Rule Our World*. New York, NY: Portfolio.

Tabor, Philip. 2000. ‘I Am a Videocam’. In *The Unknown City: Contesting Architecture and Social Space*, edited by Iain Borden, Joe Kerr, and Jane Rendell, 122–37. Cambridge, MA: MIT Press.

Tempini, Niccolò. 2014. ‘Governing Social Media: Organising Information Production and Sociality through Open, Distributed and Data-Based Systems’. Phd, The London School of Economics and Political Science (LSE). http://etheses.lse.ac.uk/1026/ (last accessed September 15, 2016).

Thrift, Nigel. 2005a. *Knowing Capitalism*. London: SAGE.

———. 2005b. ‘The Automatic Production of Space’. In *Knowing Capitalism*, edited by Nigel Thrift. London: SAGE.

Thrift, Nigel, and Ash Amin. 2002. *Cities: Reimagining the Urban*. London: Polity Press.

Toon, Ian. 2000. ‘’Finding a Place in the Street’: CCTV Surveillance and Young People’s Use of Urban Spaces’. In *City Visions*, edited by David Bell and Azzedine Haddour, 1st ed, 141–65. Harlow: Routledge.

Touraine, Alain. 1995. *Critique of Modernity*. Cambridge, MA: Blackwell.

Turkle, Sherry. 2011a. *Alone Together*. New York, NY: Basic.

———. 2011b. *Alone Together: Why We Expect More from Technology and Less from Each Other*. New York, NY: Basic.

Turow, Joseph. 2006. *Niche Envy: Marketing Discrimination in the Digital Age*. Cambridge, MA: MIT Press.

———. 2011. *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth*. New Haven, CT: Yale University Press.

Turow, Joseph, Michael Hennessy, and Nora Draper. 2015. 'The Tradeoff Fallacy. How Marketers Are Misrepresenting American Consumers And Opening Them Up to Exploitation'. Report. Annenberg School for Communication, University of Pennsylvania, Philadelphia, PA. https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf (last accessed September 15, 2016).

Tyrell, Hartmann. 2005. 'Singular oder Plural - Einleitende Bemerkungen zu Globalisierung und Weltgesellschaft'. In *Weltgesellschaft: Theoretische Zugänge und empirische Problemlagen*, edited by Bettina Heintz, Richard Münch, and Hartmann Tyrell, 1–50. Stuttgart: Lucius & Lucius.

Uprichard, Emma. 2012. 'Being Stuck in (Live) Time: The Sticky Sociological Imagination'. *The Sociological Review* 60 (June): 124–38.

———. 2013. 'Focus: Big Data, Little Questions?' *Discover Society* 1 (October). http://discoversociety.org/wp-content/uploads/2013/10/DS_Big-Data.pdf (last accessed September 15, 2016)

Vainio-Larsson, Arja. 1990. 'Evaluating the Usability of User Interfaces: Research in Practice'. In *INTERACT 90 - 3rd IFIP International Conference on Human-Computer Interaction*, edited by Dan Diaper, David J. Gilmore, Gilbert Cockton, and Brian Shackel, 323–28. Cambridge.

Van Couvering, Elizabeth. 2007. 'Is Relevance Relevant? Market, Science, and War: Discourses of Search Engine Quality'. *Journal of Computer-Mediated Communication* 12 (3): 866–87.

Van Dijk, Jan. 2012. *The Network Society*. 3rd ed. London: SAGE.

van Someren, Maarten W., Yvonne F. Barnard, and Jacobijn A.C. Sandberg. 1994. *The Think Aloud Method: A Practical Guide to Modelling Cognitive Processes*. London: Academic Press.

Virilio, Paul. 1986. *Speed and Politics: An Essay on Dromology*. New York, NY: Semiotext(e).

———. 2005. *Desert Screen: War at the Speed of Light*. New York, NY: Bloomsbury.

Vollmer, Gerhard. 1992. 'Die Vierte Bis Siebte Kränkung Des Menschen: Gehirn, Evolution Und Menschenbild'. *Philosophia Naturalis* 29 (1): 118–134.

Voruz, Véronique. 2013. 'The Status of the Gaze in Surveillance Societies'. In *Re-Reading Foucault: On Law, Power and Rights*, edited by Ben Golder, 127–50. Abingdon: Routledge.

Walby, Kevin T. 2005. 'Institutional Ethnography and Surveillance Studies: An Outline for Inquiry'. *Surveillance & Society* 3 (2/3).

Weber, Max. 1946. 'Science as a Vocation'. In *From Max Weber: Essays in Sociology*, edited and translated by C. Wright Mills and H. H. Gerth, 129–56. New York, NY: Oxford University Press.

———. (1930) 2001. *The Protestant Ethic and the Spirit of Capitalism*. Translated by Talcott Parsons. 2nd ed. London: Routledge.

Webster, Frank. 2006. *Theories of the Information Society*. 3rd ed. London: Routledge.

Webster, Frank, and Kevin Robins. 1986. *Information Technology: A Luddite Analysis*. Norwood, NJ: Praeger.

Weizenbaum, Joseph. 1977. *Computer Power and Human Reason: From Judgment to Calculation*. San Francisco, CA: W.H. Freeman & Co.

———. 1978. *Die Macht der Computer und die Ohnmacht der Vernunft*. Translated by Udo Rennert. Frankfurt a.M.: Suhrkamp.

Wenger, Etienne. (1998) 2000. *Communities of Practice: Learning, Meaning, And Identity*. New ed. Cambridge: Cambridge University Press.

'What They Know - Wsj.com'. *Wall Street Journal.* 2016 http://www.wsj.com/public/page/what-they-know-digital-privacy.html (last accessed September 15, 2016).

Whitaker, Greg. 1999. *The End of Privacy: How Total Surveillance Is Becoming a Reality*. New York, NY: New Press.

Whitson, Jennifer R. 2013. 'Gaming the Quantified Self'. *Surveillance & Society* 11 (1/2): 163–76.

Wiener, Norbert. 2013. *Cybernetics: Second Edition: Or the Control and Communication in the Animal and the Machine*. 2nd ed. Eastford, CT: Martino Fine.

Wilkinson, Alec. 2007. 'Remember This?' *The New Yorker*, May 28. http://www.newyorker.com/magazine/2007/05/28/remember-this (last accessed September 15, 2016).

Williams, Frederick, Ronald E. Rice, and Everett M. Rogers. 1988. *Research Methods and the New Media*. Series in Communication Technology and Society. New York, NY: Free Press.

Winner, Langdon. 1977. *Autonomous Technology: Technics Out-of-Control as a Theme in Political Thought*. Cambridge, MA: MIT Press.

Wolf, Gary. 2010. 'The Data-Driven Life'. *The New York Times*, April 28. http://www.nytimes.com/2010/05/02/magazine/02self-measurement-t.html.

Wood, David Murakami. 2009. 'The `Surveillance Society' Questions of History, Place and Culture'. *European Journal of Criminology* 6 (2): 179–94.

Yar, Majid. 2003. 'Panoptic Power and the Pathologisation of Vision: Critical Reflections on the Foucauldian Thesis.' *Surveillance & Society* 1 (3): 254–71.

Yekutieli, Yuval. 2006. 'Is Somebody Watching You? – Ancient Surveillance Systems at the Southern Judean Desert'. *Journal of Mediterranean Archaeology* 19 (1): 65–89.

Yin, Robert K. (1984) 214AD. *Case Study Research: Design and Methods*. 5th ed. Los Angeles, CA: SAGE.

Zhou, Larry. 2014. 'EXCLUSIVE: Facebook Plans Event to Recruit Sociologists'. *VentureBeat*, July 6. http://venturebeat.com/2014/06/07/exclusive-to-sell-ads-in-the-developing-world-facebook-is-hiring-sociologists/ (last accessed September 15, 2016).

Zikopoulos, Paul. 2011. *Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data*. 1st ed. New York, NY: McGraw-Hill.

Zimmer, Michael. 2008. ‘The Externalities of Search 2.0: The Emerging Privacy Threats When the Drive for the Perfect Search Engine Meets Web 2.0’. *First Monday* 13 (3).

Zittrain, Jonathan. 2008. *The Future of the Internet and How to Stop It*. London: Penguin.

Zuboff, Shoshana. 1989. *In The Age Of The Smart Machine: The Future Of Work And Power*. Reprinted edition. New York, NY: Basic.

———. 2015. ‘Big Other: Surveillance Capitalism and the Prospects of an Information Civilization’. *Journal of Information Technology*, April 4.

Appendix A

Below are the information sheet providing written context and the consent form that were handed out to participants prior to the interviews.

INFORMATION SHEET: A STUDY ON

PERSONAL DATA ON THE INTERNET AND YOUR LIFE WITH COMPUTERS

About the study

Hello, my name is Daniel Knapp and I am a PhD student in Media & Communications at the University of London. I am doing research on how people deal with personal data on the internet and generally make sense of how the internet and computers works. I would like to ask for your help in this research. The aim is to better understand how people relate to technology. Anyone can participate, you do not need to know anything particular about the internet or computers. It is all about your experience and opinions, so there are no right or wrong answers.

You will receive an incentive of **£25** for your participation.

What does taking part in the study involve?

As part of the study, I am interviewing internet users aged between 18 and 29. You would be asked to participate in two interviews. The first interview would be a conversation between us at a place of your choice or at my office. If you have a place that you like, it just needs to be quiet enough to have a good conversation. After that, we would meet a second time. This second interview would be a bit different and involve you commenting spontaneously what your thoughts and aims are while you are using the internet in my presence. Afterwards, I would ask you some questions based on what you said. This would last about two hours. Again, it can be done at any time place of your convenience where it is not too noisy. We will also need internet access. I am happy to invite you to my office for this. I would like to tape-record our conversations. You do not have to answer any questions you do not wish to and you can stop the interview at any time, without giving reasons.

What will happen to your answers?

All comments you give will be made anonymous and are strictly confidential. You will not be identified in the final research report. Only I will have access to the raw data arising from this research which will be stored in a safe place and all computer-held data will be password-protected. The requirements of the Data Protection Act will be observed.

Further questions and concerns

This study has been approved by the Department for Media & Communications, Goldsmiths College, University of London. If you have any questions about the research, you can contact me at:
Daniel Knapp
Department for Media and Communications, Goldsmiths, University of London
Lewisham Way
London SE 14 6NW
E-Mail: cop01dk@gold.ac.uk
Phone: +44 (0) 794 600 78 13

Should you have any concerns about the conduct of the research, you can contact Professor Nick Couldry, supervisor of this study:
Professor Nick Couldry
Professor of Media and Communications
Department for Media and Communications, Goldsmiths, University of London
Lewisham Way
London SE 14 6NW
E-Mail: n.couldry@gold.ac.uk
Phone: +44 (0) 20 7919 636

CONSENT FORM

A STUDY ON

THE INTERNET AND PERSONAL DATA

Researcher: Daniel Knapp

1.) I confirm that I have read and understood the information sheet for the above study and have had the opportunity to ask questions.

2.) I understand that my participation is voluntary and that I am free to withdraw at any time, without giving any reason.

3.) I confirm that the interview will be recorded with my consent and that in the transcript a pseudonym or alias will be used and reference to me as an individual will be removed. The data will only be used for the stated research purposes.

4.) I understand that any data I provide through taking part in this research will be held in accordance with the Data Protection Act 1998.

Please mark as applicable:

I agree to take part in this research ☐

I do not agree to take part in this research ☐

_____ _____

(Signature of participant) (Date)

_____

(Name of participant PLEASE PRINT)

Appendix B

Participant Chart:

Pseudonym	Gender	Age	Occupation	Location
Adam	Male	22	Student (Art)	UK
Amanda	Female	21	Student (Finance)	UK
Andre	Male	29	Car Body Shop Worker	Germany
Anna	Female	20	Student (Pedagogics)	Germany
Ann-Kathrin	Female	21	Student (Psychology)	Germany
Annegret	Female	19	Apprentice (Optician)	Germany
Bashir	Male	23	Student (Medicine)	UK
Christina	Female	26	Business Journalist	UK
Constanza	Female	29	Artist	UK
Dave	Male	25	Fitness Coach/Marketing Associate	Germany
Dennis	Male	26	Student (Geophysics)	Germany
Enrico	Male	28	Student (History)	Germany
Evelyn	Female	20	Student (Psychology)	Germany
Fateha	Female	22	Event Organiser (Advertising)	UK
Frank	Male	27	Administrator (Public Transport)	Germany
Franzi	Female	24	Physiotherapist	Germany
Freddy	Male	28	Teacher	Germany
Henning	Male	22	Student (Engineering)	Germany
Ian	Male	25	Charity Worker	UK
Jack	Male	27	Planning Officer (Construction Sector)	UK
James	Male	28	Barista	UK
Joanna	Female	26	Legal Secretary	UK
Josephine	Female	21	Hairdresser & Student (Textile Design)	Germany
Karen	Female	27	Dental Hygienist	UK
Katy	Female	23	Student (Translation Studies)	UK
Lars	Male	26	Student (Politics) & Former Police Officer	Germany
Laura	Female	23	Student (Development Studies)	UK
Linda	Female	25	Recent Maths Graduate/Jobseeker	UK
Luise	Female	22	Student (Law)	Germany
Mark	Male	25	Office Clerk	UK
Martin	Male	26	Sales Manager	UK
Mike	Male	27	Graphic Designer	UK
Paula	Female	28	Homemaker & Part-Time Yoga Instructor	Germany
Rebecca	Female	20	Student (Politics)	Germany
Richard	Male	24	Financial Advisor	UK
Sarah	Female	21	Student (Linguistics)	Germany
Simona	Female	26	Business Analyst	UK
Stefan	Male	23	Student (Biology)	Germany
Stuart	Male	26	Loans Advisor	UK
Tim	Male	26	Student (Anthropology)	UK