Big data, microtargeting, and governmentality in cyber-times. The case of the Facebook-Cambridge Analytica data scandal.

Ellen Emilie Henriksen

Master thesis in political science, Department of Political Science

UNIVERSITY OF OSLO

Spring, 2019

Word count: 47756

Big data, microtargeting, and governmentality in cyber-times. The case of the Facebook-Cambridge Analytica data scandal.

2019

Big data, microtargeting, and governmentality in cyber-times

Ellen Emilie Henriksen

http://www.duo.uio.no/

Print: Reprosentralen, Universitetet i Oslo

Word count: 47756

Abstract.

This thesis aims to conceptualise microtargeting a as a security threat. The Facebook-Cambridge Analytica scandal has received substantial media attention, and subsequent proclamations as to how the use of microtargeting techniques – in this case psychographics – in political advertisement poses a threat to democracy. Answering what this threat actually is, however, is difficult. This paper proposes that microtargeting is best understood as a threat to governmentality, rather than democracy or governance. This follows from an argument that microtargeting is in its simplest form efficient advertisement, and thus a part of the competitive advantage of private actors in a capitalist system; a competition that is constitutive of the very liberal democratic political arrangement that it supposedly poses a threat to. What is more, microtargeting as technique is also deployed by the state in security practices, and the data used by both government and corporations originate to a large extent from the same data brokers. Thus, referent object and threat conflate, making microtargeting as a security threat notoriously context bound. To deconstruct that very context is the aim of this paper. Here, understanding the logic of big data analytics compared to traditional statistics is key to understand how microtargeting is a threat to liberal governmentality. Furthermore, these epistemological changes lead to a transformation in the episteme threatening an analogue rationale of governmentality. This conceptualisation is applied to both the domestic and the international level of governmentality. Following this, the paper argues that ‘cyber’ should be understood as integrated into the so-called offline categories of society. Technology, with its epistemological consequences – the change of *rationale* of governing, should be analysed as constructed by, and transformative of, the very society whence it arises.

Acknowledgements.

My supervisors Kacper Szulecki and Øivind Bratberg deserve gratitude for their support and advice, for always replying to emails and guiding me through this project.

Additionally, I would like to thank everyone at NUPI's Centre for Cyber Security Studies for inputs and invigorating cyber lunches. An additional thanks goes to Erik Reichborn-Kjennerud for valuable feedback despite academic disagreements.

I would also like to mention Lise, Reidun, and Ida without whom the years at Blindern would have been a far less joyous voyage.

A thank you also goes to Marie and Hanne for proofreading. Øystein also deserves gratitude for his proofreading and comments, but most of all for surviving co-habitation in times of immense stress.

And of course, Ragnhild, as always.

Ellen Emilie Henriksen
Oslo, May 23rd, 2019.

Table of Contents.

Introduction.

Initially, this thesis had the ambition to find out where cyberspace is. It struck me as curious that this ever more dominating space; this cloud which surrounds our lives, was no-where to be located as if its power resided in its lack of materiality. Some of its power most definitely resides in its lack of materiality. Cyberspace is a "virtual reality inside the machine" according to Edwards (1996: 303). Cyberspace is more than that, cyberspace is a metaphor. And metaphors are more than poetic practices of describing one thing in terms of the other; they are practices of everyday language, as "the locus of metaphor is not in language at all, but in the way we conceptualize one mental domain in terms of another." (Lakoff 1993: 1) What is perhaps most interesting about cyberspace as a metaphor is the suffix 'space'. As if it were inconceivable to make sense of this new domain in our lives as anything but a physical space; as if cyberspace as a discursive construction depends on a narration of this 'thing' in fact being a tangible space. But cyberspace is no space, it is a virtual reality which resides not only inside the machine, but beyond hardware. The ambition of this thesis is no longer to locate cyberspace. The ambition of this thesis is rather to mobilise cyberspace as a metaphor in order to reveal something about how society is organised in an era which is increasingly narrated as a suffix to 'cyber'.

'Cyber' was first used as a prefix in the concept 'cybernetics', coined by the MIT-based mathematician Norbert Wiener in the aftermath of World War Two (Halpern 2014: 39). Cybernetics comes from the Greek verb kubernan, which means to steer, navigate, or control (Collins 2010). In its initial use, it was precisely the allusion to control which gave content to the sign 'cyber', where cybernetics described Wiener's "general theory of machines." (Branch forthcoming) 'Cyber' as meaning control and computation is also visible in popular culture, where the dystopian cyberman in the BBC television series Dr Who is human turned into machine through the removal of human emotions. Still, 'cyber' often bear connotations to something quite different from cybernetics. Cyber, which by and large has come to replace cyberspace, bear connotations to a distinct space liberated from earthly constraints. It bears connotations of technological progress and transnational connections. When this paper uses the sign 'cyber' it does so pointedly. I could have chosen a different metaphor. I could have chosen Knorr Cetina's (1999) 'epistemic cultures' or Katherine Hayles (2005) 'regime of computation' in order to capture the effect of information technologies on epistemology. I could have chosen to build on Edwards (1996) 'closed worlds', in order to capture the intertangled nature of materiality, discourse, and technology in the shaping of how we see the world. I could also have chosen to not use 'cyber' at all, but refer to the Internet, or communication technologies, as is the practice in for instance Chinese and Russian cybersecurity discourses (Branch forthcoming; Mueller 2017). I have chosen not to do so because it is an ambition of this thesis to explore what the metaphorical cyberspace beholds.

1.1) The research question

The Facebook-Cambridge Analytica scandal erupted as it was leaked that more than fifty million Facebook users' data had been scraped without their consent. This data had subsequently been used to train algorithms to nuance political advertisements, so-called microtargeting (Cadwalladr 2018a; 2018b). Individuals were segmented into a given composition of scores within the categories of neuroticism, extraversion, openness, agreeableness, and conscientiousness, a model known as the "Five Factor Model" (FFM) or the "Big Five personality traits" in psychiatry (Widiger 2015), to which ads would be nuanced accordingly (Brodwin 2018). Cambridge Analytica's involvement in both the Brexit campaign and in the U.S. 2016 primaries and presidential elections have raised concern about the use of big data analytics in democratic electoral campaigns (Lewis & Hilder 2018; Scott 2018). Microtargeting is "a type of personalised communication that involves collecting information about people, and using that information to show them targeted political advertisements." (Borgesius et al 2018: 82) Initially, microtargeting was done "using postal codes (…) and a geographical segmentation of the targeted audience was achieved." (Barbu 2014: 44) With the emergence of big data and cyber-technologies, however, microtargeting is better understood in its current form as the use of big data to perform "advanced psycho-geographic segmenting which is based on an algorithm determining a series of demographic and attitudinal traits to distinguish individuals for each targeted segment." (Ibid.: 45) It is the latter of these definitions, where big data is included, that is referred to when this paper analyses microtargeting.

The kind of microtargeting deployed by Cambridge Analytica was that of ‘psychographics’, where microtargeting is supplemented with core tenets from behavioural psychology. As such, prychographics is meant to capture the personality of the targeted audience to “resonate more effectively with those key audience groups.” (Halpern 2018) This thesis refers to microtargeting rather than psychographics when exploring the Facebook-Cambridge Analytica scandal, as psychographics is a form of microtargeting. I will refer to psychographics when that is relevant, as this is the term used by the actors involved in the scandal. However, the term microtargeting is meant to include psychographics as a technique.

The scandal came with a series of questions in dire need of answers. These questions were centred on topics such as online privacy, foreign interference in elections, as well as the new economy of big data arising from social media platforms. It is in the presence of these questions that this thesis is situated. Most prominently, the use of microtargeting techniques in political campaigns is viewed as a threat to democracy (Cadwalladr 2018a; 2018b; 2019; Hearn 2018; Heawood 2018; Halpern 2018; Koopman 2018; Rajan 2018; Tarran 2018) where microtargeting is considered a threat as nuanced political advertisements are divisive, and “can be used to manipulate and suppress human ideas” (Wilson 2017) which in turn distorts deliberative democratic conversations (Unver 2017). After the eruption of the scandal in March 2018, there were a series of hearings in the U.S. Senate on the topic of social media, big data, and elections. On September 5th, 2018, Facebook COO Sheryl Sandberg witnessed at the fourth of these hearings. Here, she was questioned by Senator Kamala Harris on the topic of divisive content on the social media platform:

> Harris: “Your company’s business model is, it’s obviously complex, but benefits from increased user engagement. And that results, of course, in increased revenue. So, simply put the more people that use your platform, the more they are exposed to third party ads, the more revenue you generate. Would you agree with that?”
>
> Sandberg: “Can you repeat? I just want to make sure I got that exactly right.”

> Harris: “So, the more user engagement, and the more then, that they are exposed to third party ads, the more that will increase your revenue.”
>
> Sandberg: “yes, yes, but only
>
> (…)
>
> Harris: “So a concern that many have is how you can reconcile an incentive to create and increase your user engagement when the content that generates a lot of engagement is often inflammatory and hateful. So, for example, Lisa-Marie Neudert, a researcher at Oxford Internet Institute she says, quote: ‘The content that is the most misleading or conspiratorial, that’s what’s generating the most discussion and the most engagement. And that’s what the algorithm is designed to respond to.’ (…)” (C-Span 2018d: 01:32:07)

This questioning captures a tension pertinent to the Facebook-Cambridge Analytica scandal. It is in Facebook’s interest that their site has divisive content, that is what generates user engagement. It is not necessarily in the state’s interest that the content is divisive as it polarises the populace which could undermine stability. But Facebook’s business model is so that this is how the company generates revenue. It is in the interest of the state that companies compete on an open and free market, where alternative strategies for generating value will invariably arise. It is easy to pinpoint where this contention is situated; but hard to eliminate the problem without undermining core values of the society one aims to protect. To limit the use of microtargeted ads or divisive communication is also to limit free competition under capitalism and freedom of speech. In chapter three of this thesis, I will argue that it is because of this tension that microtargeting can hardly be conceptualised as a threat to democracy. Opposing microtargeting to democracy would involve a distinction between microtargeted communication and other types of communication; a distinction that I will argue is arbitrary and flawed. Rather, I propose a conceptualisation of microtargeting as a threat to the Foucauldian concept governmentality, and in this case, liberal governmentality. Thus, my research question is as follows:

How is microtargeting a threat to liberal governmentality?

Microtargeting is also a security dispositif of government where the use of microtargeting techniques in security practices such as surveillance (see Ferguson 2017a; 2017b), makes it difficult to conceptualise microtargeting itself as a threat to either governmentality or democracy. The question 'how' in the research question is thus meant to capture the need for contextualising when answering how microtargeting poses a threat to liberal governmentality. As such, the 'how' is twofold: it begs the question on how and in what way microtargeting is constructed as a threat, a question which will be answered in chapter five, which is a discourse analysis of two of the hearings in the U.S. Senate following the scandal. 'How' also requires an answer to how come microtargeting beyond language uttered by senators may pose a threat to liberal governmentality. It is this question chapter six in this thesis will answer. Here, unpacking the underlying logic of microtargeting and opposing this to the rationale of liberal governmentality will unveil how the changed episteme of governmentality in the age of cyber, concomitant to big data and microtargeting, may threaten that very governmentality.

1.2) Key terms

As already mentioned, I propose a definition of microtargeting as a technique utilising big data. Big data is more than just a huge amount of data. Most commonly, big data is defined in terms of the 4Vs: volume, velocity, variety, and veracity (Parisi 2019). Kitchin (2015; 2017) proposes an expansion of this definition to also encompass how big data is

> *exhaustive* in scope, striving to capture entire populations or systems (…) Fine-grained in *resolution* and uniquely *indexical* in identification (…) *Relational* in nature, containing common fields that enable the conjoining of different data segs [and] *flexible,* holding the traits of *extensionality* (can add new fields easily) and *scaleability* (can expand in size rapidly). (2015: 471, emphasis in original)

Yeung (2016) refers to big data as both technology and a process, where the process of big data – big data analytics – allows for legibility of data sets too vast for human capacity to analyse. The key here is that big data is more than a lot of data. Big data allows for fast, dynamic collection of data, where the sample is meant to equal the universe; *n* is supposed to equal all. As dynamic, the data set develops together with the object. Rather than the data being collected based on an already formulated survey model, big data allows for the collection of data in real time. These properties will be expanded on in chapter two and six of this thesis, where a main conclusion is that the reproduction of the anomalous through the communication of divisive content in political and commercial microtargeted communication threatens the stability of governmentality.

Related to big data is the concept of computation. Computation is defined as “a calculation involving numbers or quantities.” (Collins 2010) Computational is defined as a “means using computers” (Ibid.) When this thesis refers to computation, or computational thinking, it is keeping both of these definitions in mind. However, computation is more than a technique of calculation; computation is the view that the world can in fact be quantified and calculated. In an age of cyber, this vision is exacerbated by the presence of computers and big data. Hayles refers to computation as a worldview connoting “far more than the digital computer, which is only one of many platforms on which computational operations can run.” (2005:17) Fundamental to computational thinking in cyber-age is therefore the idea that everything can be datafied (see Cukier & Mayer-Schoenberger 2013); big data can measure everything from personality to communication, behaviour or preferences. As such, computation lies close to the ambition of cybernetics, which

> suggests that steering or governing is one of the most interesting and significant processes in the world, and that a study of steering in self-steering machines, in biological organisms, in human minds, and in the societies will increase our understanding of problems in all these fields. (Deutsch 1966: 77-78)

1.3) Structure of the thesis

In order to answer the research question “how is microtargeting a threat to liberal governmentality?” this thesis will proceed as follows: chapter two will outline the background for the analysis, where the postpositivist nature of the analysis, the Facebook-

Cambridge Analytica scandal, and big data will be elaborated on. Chapter three will elaborate on the theoretical premises of the discussion, where the choice of governmentality as referent object will be justified. After having outlined the methodological fundament of the thesis in chapter four, chapter five is a discourse analysis of two of the hearings in the U.S. Senate following the scandal. Here, the purpose is to untangle the meaning attributed to the scandal in order to reveal the underlying narratives upholding the event. Chapter six will take the analysis to a level of abstraction, where I through an abductive analysis will demonstrate that the threat perceptions pertinent to the hearings are unable to capture the underlying logic of microtargeting in this specific context. Here, I argue that microtargeting in the context of the Facebook-Cambridge Analytica scandal threatens not only the rationale and technique of liberal governmentality, but also the very constitution of the liberal subject to be governed. Chapter six will conclude with an analysis of the relevance of my findings for the international level of Internet governance. Although this analysis will be incomplete due to lack of space, I will attempt to demonstrate that the internal conflict inherent in liberalism, reformulated and exacerbated in the age of cyber, is relevant also from the global perspective of how the Internet should be governed. In chapter seven I will offer some concluding remarks, summarise my findings, and suggest future research.

2) Background: Mobilising cyberspace.

> Cyberspace, a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts (…) a graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lives of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding …
>
> Gibson (1984:59)

The term cyberspace was introduced by William Gibson in 1982 and popularised in his 1984 novel *Neuromancer*. The current connotations to this space bear clear resemblance to the sphere of human consciousness as described by Gibson more than thirty years ago; as a seductively free and boundaryless space, market by abstraction and complexity, and which you can enter and leave at free will. This aspires to exceptionalism: to view everything 'cyber' as a unique and new world-building exercise, separated from the 'real' or offline categories of life. This thesis is an attempt to break down this exceptionalism. By doing so, it does not argue against the transformative effect that cyber-technologies have on society and politics. Rather, it considers this transformative power as integrated; produced and reproduced, in society, where cyber has fuzzy borders, indistinguishable from 'real' life: we are all cyborgs. Additionally, cyber should be situated within a wider narrative of computation, starting long before the emergence of cyberspace. As a 'consensual hallucination' narrated by Gibson in 1984, it was perhaps not unique in nothing but name. James Bridle tracks the idea of computational thinking – the idea that problems can be solved through mathematical analysis of data and technological innovations – back to Lewis Fry Richardson, a mathematician who during world war one attempted to calculate weather forecasts based on weather data subjected to mathematical equations. In doing so, he viewed history as a problem, that could be "transformed into a mathematical equation that, when solved, would produce the future." (2018: 20) Computational thinking is not only a breakdown of reality to data points and mathematics. It is also a breakdown of the temporal boundaries between past, present, and future. In the obsession with prediction inherent in computation, amplified by the availability of big data, lays also a transformation of our very cognition of the world, and thus formulations of rationality (Halpern 2014). The breakdown of the world into a binary language, subjectable to cybernetic manipulation entails a transformation of our cognition into *seeing* the world through a computational mind. Cyberspace, then, should not be viewed as a separate domain, distinct from 'real' life. Rather, this thesis proffers a view on cyber informed by Science and Technology Studies (STS) (see esp. McCarthy 2018a; 2018b; 2018c; Haraway 2016; Latour 2005; Law 2012) where technology is viewed in a reflexive relationship with the society within which it emerges. Microtargeting, as a process and technique is an example of this computational thinking. It is the reformulation of the human psyche, the human character, into data points; a transformation of the human into a mathematical equation that, when solved, can be used to manipulate behaviour, to produce the future. It is based on this that this thesis emphasises the need to analyse microtargeting – here in the shape of the Facebook-Cambridge Analytica scandal – not as an external event threatening an established referent object. Rather, microtargeting should be analysed as an integrated process in the very workings of the liberal state. This is crucial if we are to understand how microtargeting can arise as a threat to society as we know it. This is also crucial if we are to understand exactly what is threatened by microtargeting in society as we know it.

Cyberspace is no longer a space one can enter and leave at free will; it is a space transformative of space itself, increasingly omnipresent through the increase in computational thinking. To illustrate this argument, Bridle (2018) refers to 'code spaces', a concept that is similar to Kitchin and Dodge's (see esp. 2009; 2018) concept of coded spaces. These are spaces that only exist as the spaces we construct them to be as long as the network of computation is punctuated, that is stable and functioning. An airport ceases to be an airport if the computers break down: planes cannot take off, cannot land, tickets cannot be registered and approved, luggage and passengers cannot be checked in. The airport is not a result of the material constructions upholding it as an edifice. The airport is an airport because of technical communication devices enabling certain processes, that is: a network of cyber makes it so. This integration of technologies into the workings of everyday life is also visible at the level of Internet governance, where DeNardis identifies how Internet governance is not simply a question of managing Internet in a way to keep it operational and the “enactment of substantive policy around these technologies.” (2015: 5) The very design of these technologies construct governance itself; the very arrangement of the technical architecture of Internet is an arrangement of power (Ibid.: 8).

This thesis’ criticism of a tendency towards a cyber-exceptionalism pertinent to much cyber-related studies (e.g. Balzacq & Cavelty 2016; Goldsmith & Wu 2006; Reveron 2012; Lin 2012; 2016; Bucci 2012; Andres 2012) is informed by work within critical algorithm studies, especially the work of Katherine N. Hayles, Louise Amoore, and Volha Piotukh, in addition to STS. Hence, the integration of cyber-technologies in the ‘real’ world is acknowledged as a fundamental transformation of the totality of reality as we know it. By this is meant that the ‘cognitive assemblages’ – the expansion of “the traditional view of cognition as human thought to processes occurring at multiple levels and sites within biological life forms and technical systems” make a distinction between off-line and on-line categories of life arbitrary and flawed (Hayles 2016: 32). The basic idea of cognitive assemblages is that the distinction between human and machine does not apply to a study of technology, as technological changes are embedded in society and questions on what it means to be a human. Hayles therefore proposes to distinguish between cognition and non-cognition, where certain machines can be thought of as non-conscious cognitive thinkers (Parisi 2019). It is precisely due to the blurriness of cyber versus non-cyber both in terms of locating action and designating space, that the focus of this thesis is on governmentality, rather than say cyber-security. To posit governmentality as referent object is not to claim that governmental practices are distinct from the workings of cyberspace. As pointed out by critical scholars of cybersecurity (Collier 2018; Coles-Kemp et al 2018; McCarthy 2018) cybersecurity is increasingly embedded in security practices in general. Likewise, ‘normal’ state practices are increasingly embedded with cyber-technologies. This follows from Bridle’s conceptualisation of computation and ‘code spaces’ above: if ‘analogue’ practices such as travelling are dependent on digital cyber-practices in communication, the two become indistinguishable in any conceptualisation of a working airport. Likewise, the processes of governmentality are transformed by cyber: from applications for benefits to state surveillance, the practices of the state increasingly depend on information technologies and big data. This thesis acknowledges the transformative effect of cyber and the limitations of focussing on cyber as distinct from everything else, whatever the latter may consist of.

2.1) The postpositivist critique of individuation: computation, calculation, and cybernetics

> Calculating does not necessarily mean performing mathematical or even numerical operations (…) Calculation starts by establishing distinctions between things or states of the world, and by imagining and estimating courses of action associated with things or with those states as well as their consequences.”

Amoore & Piotukh (2016: 20)

Microtargeting is above else about calculation. Microtargeting is a continuation of the cybernetic ambition for control: of making the individual calculable through a dissemination of data collected from behaviour as if that data would unveil what the individual really is. As if countable data on an individual makes it susceptible to programming through calculated communication. It is not this calculation itself that makes microtargeting a threat to liberal governmentality. Rather, it is the specificities of the context of microtargeting, it is the imprinting of meaning to the practice of microtargeting in a specific setting that enables microtargeting to arise as a threat. The purpose of this thesis is to deconstruct that context in order to propose a useful reading of the Facebook-Cambridge Analytica scandal. And in doing so it is necessary to deconstruct microtargeting itself, to disclose its underlying logic of what can be referred to as computation, borrowing Bridle’s vocabulary.

An endeavour aimed at deconstructing computation will inevitably be a postpositivist one. Where positivist case studies are aimed at establishing causal relations, this thesis argues that the world is not best read as such. It argues that everything is connected to everything, and above all it argues that *things* and *actions* are only things and actions insofar as they are assigned meaning. Calculation, as noted by Amoore and Piotukh, is more than counting. Calculation and computation are closely related and above all they are about individuating *things.* As discursive constructions and social practices, computation and calculation are about making things separate and objectively observable from a Cartesian eye; able to generate cause and susceptible to effect in a neatly painted picture of A leading to a measurable consequence in B. Calculation is a promethean promise of objectivity. It holds that the individuation of phenomena makes *things* objectively observable and calculable through the method of mathematics. Calculation allows for *measurability* and direct comparison. As such, it is not only a promise arising from a cybernetic logic, it is also a liberal, and furthermore a neoliberal one. Foucault (1991) identifies this calculability in the development of the penal system in modernity, where the idea of 'punishment' as a theatre, as a ritual of redemption and sovereign strength, is replaced by a calculating logic weighing the diminishment of a crime in society against the expense of punishing the delinquent. Furthermore, calculability is imbedded in Foucault's elaboration on the idea of 'human capital', which involves the idea of 'interest' leaving the traditional realm of economics. Capital is not only a question of economics; capital is a measurement of the human. Economics emerges as the "science of human behaviour as a relationship between ends and scarce means which have mutually exclusive uses", involving an obliteration of the "relational mechanism between things or processes." Human behaviour ceases to be processes following certain logics, as they are reduced to 'activities' to be studied through an "analysis of the internal rationality, the strategic programming of individuals' activity." (2004: 222-223) Human activities are individuated, and best understood through analysing their embedded calculation. This lies close to the ambition of cybernetics: individuating and programming phenomena through obsessive control, subjecting the past to algorithmic calculation and thus mathematically formulate the future.

Furthermore, calculation and computation can be viewed in relation to critical theory's engagement with the project of Enlightenment. Stuart Elden (2013) tracks the modern notion of territory back to the invention of geometry as an epistemological technique, rather than a mental exercise of mathematics. He identifies this shift in cognition towards the calculability of space as a Cartesian shift consequential to the ideas of Enlightenment itself. This shift did not only change how we read maps, but also how state borders are drawn and how nations are understood. From the perspective of STS, this shift should also be understood through the development of modern cartography as a technique. The evolution of technology is not objective but is a product and a producer of the society whence it emerges, or in this case: maps make territory (see Branch 2011; 2016; 2017; Strandsbjerg 2012).

More famously, Adorno and Horkheimer (1997[1944])) track the idea of Enlightenment all the way back to Homer. Central to Enlightenment is the idea of the individual as guided by reason alone; the human realm is that of the mind and truth can be arrived at through the mental exercise of reason. This bear clear resemblances to Edward's (1996) analysis of cybernetic psychology, where especially the post-World War Two development of the field of cognitive psychology was centred on what Edwards refers to as a 'cybernetic discourse.' This discourse revolved, and to some extent still revolves, around the idea of the human mind as consisting of innate structures such as those providing us with the faculties of language and reason, rather than these faculties developing in conjuncture with socialisation. Edward's critical engagement with cybernetic discourse lays close to Adorno and Horkheimer (1997[1944]) and the Frankfurt School critique of the scientific ideals of Enlightenment that proffer the view that truth, and therefore knowledge of the world, is best arrived at through objective observation. Both critique the ideal of Enlightenment of the individual as autonomous and guided by reason, rather than say a holistic view of mankind driven by emotion. From the perspective of STS (see Cavelty 2018; McCarthy 2018a; 2018b; 2018c), the ideals of Enlightenment are also present amongst technological determinists, who view technology as an objective prolongation of human rationality that will develop in accordance with society's progression in linear fashion (see Manjikian 2018). Informed by the critical theory of the Frankfurt school and STS, this thesis argues that technology should be conceptualised in a reflexive relationship; constructing society as society constructs technology.

To meet this challenge from the theoretical point of view, Latour (2005) introduces Actor-Network Theory (ANT), a theory and method aimed at capturing the role of materiality in studying social phenomena. Latour argues that action is dislocated, and that human and non-human objects are ontologically symmetrical. This means that intent is irrelevant, as action can be generated by the conscious or the non-conscious alike. As such, Latour brings important insights to the study of science and society, as viewed from his prominence within STS. What is more, Latour does not give great importance to the size of the objects acting. Latour points out that the size of a giant is only relevant in their relation to the dwarf as long as the giant is awake. By this is meant that the mechanisms upholding asymmetrical social relations cannot be explained only in terms of the relative social strength among the entities. Rather, there must be something more durable than social ties upholding the asymmetry. It is here that the role of the material becomes relevant; as durable agents – or *actants* in ANT vocabulary – upholding relations. From the perspective of algorithmic studies, this is relevant in order to capture the power of 'little algorithms' in the government of things (see Amoore & Piotukh 2015). In order to understand technology and society; to capture their integrated nature as they reproduce and produce one another, the agency exerted by the non-human must be captured. This non-human is also increasingly autonomous; in terms of algorithms their formulation is not entirely predisposed by the coder. These developments driven by technological innovations and society with it, cannot be reduced to matters of technology alone; they are societal changes in that they are technological changes.

Halpern (2014) argues that these changes in technology also involve changes in cognition. These changes in cognition are not arbitrary, but mutually constitutive. Whether technology or cognition comes first, and whether that really matters, is not the focus of this thesis. However, the point that technology is not apolitical tools that inevitably develop as they do because that is how technological progress works, is crucial to this analysis. Furthermore, the idea that society itself, and most of all the idea of what the human being is, is not external to technology. Technology is formed by society and it forms us. Thus, technology shapes what it means to be human, how we experience being human. How we experience the nation is dependent on the technologies allowing for detailed cartography, how social media forms social relations have profound effect on how we experience and relate to one another (see Skeggs 2015; 2016). Embedded in these changes are not only technological tools, but also the economic and political ideologies shaping what kind of society is to be reproduced. In paraphrasing Haraway (2016) we are already technology; the cyborg is already here. In this way, this thesis is not only deconstructing computation, it is also deconstructing liberalism, and more specifically liberal governmentality. In the Facebook-Cambridge Analytica case, cybernetic ambition and liberalism converge in their intersubjective constitution.

This thesis is a theory-building case-study. As such it is to provide two main contributions to existing theories in the field. First, the ever-pressing need for sensitivity to context proffered by critical security studies is re-stated (see esp. Ciuta 2009; C.A.S.E. 2006). Secondly, I will demonstrate the usefulness of core tenets of post-structural discourse analysis for understanding the non-verbal construction of meaning by technology, echoing the emphasis on material discourse proffered by Iver B. Neumann (2002), Paul N. Edwards (1996) and Latour (2005). As such, this thesis argues fiercely against theoretical approaches to technology viewing technology as either deterministic or objective or both. Additionally, it emphasises the need for discourse analysis to pay closer attention to meaning formed outside verbal language in an age increasingly marked by autonomous technologies.

The purpose of this thesis is to study the Facebook-Cambridge Analytica scandal as a case by uncovering the underlying logics constituting the event and abstract these logics to the level of a theoretical framework in order to answer the research question "how is microtargeting a threat to liberal governmentality?" In doing so, I hope to fill the theoretical gap in how to understand online, targeted communication that do not fall under the category 'fake news'. Propaganda and disinformation have been topics studied in political science and security studies before (e.g. Benkler et al 2018; Hall 2017; Libicki 2007) The emergence of cyberspace, however, and with-it new forms of communication, present us with a qualitatively different landscape of manipulative communication. What is more, microtargeting as a technique, which is on a basic level nothing more than a clever segmenting of a population and identification of individuals based on certain criteria, is not an objective threat. By this is meant that microtargeting is also a useful tool within marketing as efficient advertisement. In surveillance practices it can be useful for identifying segments of a population or even individuals that potentially pose a threat (see Ferguson 2017a; 2017b) As such, it is hard to define exactly when and how microtargeting may pose a threat, as it evidently was in several electoral processes as shown through the Facebook-Cambridge Analytica scandal. I therefore hold that the most fruitful way to arrive at a conclusion on how microtargeting is a threat to what is through a context-sensitive analysis of the case at hand. I argue that established categories such as 'propaganda' and 'disinformation' fall far too short as they are too focussed on the message formulated in political communication, rather than the fundamental logic reading and creating the audience underlying microtargeting as a technique.

As a form of meaning-formation, I argue that the logic of computation, and in this case the concomitant logic of liberalism, is key to the construction of big data analytics in general, and microtargeting in particular. Despite positivism's promises of objectivity: of providing a neutral eye objectively *seeing* the world 'out there' generating absolute knowledge through the method of mathematics, computation and calculation are social constructs. They constitute a language susceptible to the same subjectivity as any linguistic endeavour. Calculation, or the idea that *things* can be calculated, is a discursive construction upheld through words and actions. As a social practice, calculation, or in the context of big data what Cukier and Mayer-Schoenberger (2013) has coined 'datafication'; *the making of things into something that can be calculated,* is "concrete, individual and context bound." But additionally, it is "institutionalised and socially anchored" and thus it tends "towards patterns of regularity." (Jorgensen & Phillips 2002: 18) The purpose of this thesis is therefore to deconstruct the narratives of what the Facebook-Cambridge Analytica scandal is about through a discourse analysis of how the event; how the practices constructing this event, are understood. This thesis argues that the interlocking vectors of computation and liberalism are key to this sense making.

The first task of this thesis is to identify the narratives upholding the case in question. To do so, post-structural discourse analysis is a natural starting point. Chapter five of this thesis will therefore be a discourse analysis of two Senate hearings on the topic, which will be conceptualised within the wider framework of the case. I have chosen audio-visual sources for the hearings in order to diminish the interpretational steps from spoken to written words. Transcription inevitably involves choices as to what to include and what to exclude. By approaching these hearings from videos, rather than transcripts, I hope to capture more of the context of these discourses. The time-references in this paper refer to the videos linked in the bibliography. The aim of this analysis is not simply to identify what is being said about the case, it is also to determine where the different narrators speak *from* when they speak of the event. The meanings attributed to the event are not only a matter of closed discourses narrating what actually happened. The significance of the event, and thus its consequences, are constantly being renegotiated. The relationship between data brokers and big data analytics is not an event of 'the past', it is a continuous mechanism; an inherent technique in the workings of society, the state, and the Internet in the age of cyber. Hence, the Facebook-Cambridge Analytica scandal is not only reformulating the referent object, it is also reformulated by the referent object in a reflexive relation of knowledge-production and assignment of meaning.

Rather than viewing the threat and the referent object as two distinct entities, I propose a conceptualisation of the relevant actors and relations of this analysis as an assemblage transformed by, and interlocked with, cyberspace. I identify the key actors in the case as the state, corporations, big data, algorithms, and the individual, where the relations between these actors are far from static. Big data, for instance, is both produced by individuals, and owned by (mostly) private corporations. Additionally, big data is nothing without algorithms, which in turn are nothing without big data. The relation between big data and algorithms can be one of machine learning or human extrapolation, and the ownership and formulation of algorithms is to a large extent a mysterious black box for users. The relationship between corporations and the liberal democratic state is one of mutual constitution: the state is legitimate as it protects private property, and the state is liberal as private corporations operate on a (more or less) free market. Individuals as an aggregate allocate sovereignty to the state through democratic processes but are at the same time subjects subjected to that sovereignty exerted as governmentality. Within this assemblage, microtargeting as a technique is on one hand nothing but the use of big data produced by individuals, employed through algorithms formulating a political or commercial message consumed by the individual. But on the other, it is a phenomenon inscribed with contradictory meanings in a discursive landscape that is far from closed. The confusion pertinent to this assemblage of relations and processes; this assemblage of contradictory *meanings* is not only present on a theoretical level. They are also very much present in the reception of the scandal. Where lawmakers see a difficulty in regulating activities such as data mining and microtargeting on which also governmental agencies depend, they also recognise the potential threat of big data and microtargeting towards the democratic processes on which they also depend. It is this confusion that makes this case difficult, and ever more interesting.

2.2) The Facebook-Cambridge Analytica Scandal

Untangling the Facebook-Cambridge Analytica scandal is a messy affair. On one hand, Cambridge Analytica was a company dealing with ‘strategic communication’, that is, using big data in order to tailor advertisement. As a practice, this lays in the borderlands between communication and manipulation, as one can arguably say much other advertisement do. On the other hand, there is the issue of the data scraped from Facebook users without their consent. Although worthy of critique, most data are collected without individuals’ consent (see U.S. FTC 2014). Furthermore, there is the issue of the money, and especially foreign money, which has been important in the American response to the scandal. Here, Russian interference through disinformation and fake news has been scrutinised beyond the Facebook-Cambridge Analytica scandal, most notably through the Mueller investigation (U.S. DoJ 2019) as well as in the US Senate hearings following the scandal (C-Span 2018a; 2018b;2018c; 2018d). All this is further complicated by aspects such as state security practices’ dependence on data provided by data brokers, as well as the role of free speech and privacy in political and commercial online advertisement. Additionally, there is Facebook’s monopolistic position within the social media market and its subsequent detrimental effects on innovation and real alternatives for users. These are all issues arising as civil society and politicians alike grapple to understand how the scandal should be *read* in a useful manner. The ambition of this thesis is to provide that useful reading. In doing so, I will start by untangling this messy picture, and in doing so, also answer why it matters how microtargeting is a threat to the liberal state; here understood through the lens of liberal governmentality.

In July 2018, following the Facebook-Cambridge Analytica scandal, the UK House of Commons Digital, Culture, Media and Sport Committee (DCMS) published an interim report on their investigation into disinformation and fake news. The investigation had started off in 2017 aimed at investigating fake news, but as its introduction notes: “[s]uch has been the impact of this agenda, the focus of our inquiry moved from understanding the phenomenon of ‘fake news’, distributed largely through social media, to issues concerning the very future of democracy.” (2018: 3) Furthermore, following the revelations emerging with the Facebook-Cambridge Analytica scandal, the report states that “[t]his kind of evidence led us to explore the use of data analytics and psychological profiling to target people on social media with political content, as its political impact has been profound, but largely unappreciated.” (Ibid.: 4)

It would be an understatement to claim that the Facebook-Cambridge Analytica had political consequences. Aleksandr Kogan, Alexander Nix, and Christopher Wylie – all involved in the affair – were called into hearings in the UK Parliament and the US Senate. Kogan and Wylie appeared at both, but Nix declined to show up in the US Senate due to his company’s insolvency proceedings – insolvency proceedings that were an expressed consequence of the scandal (Reuters 2018). Exploratory in their nature, these hearings were characterised by confusion as to what the scandal constituted – how and what exactly is a threat to exactly what? Most commonly, the affair was considered a threat to democracy, as noted in the DCMS interim report above. Likewise, the US Senate Select Committee on Intelligence (SSCI) report on the Russian Internet Research Agency (IRA), social media and political polarization identified the referent object as democracy itself (2018). The threat in the U.S. was largely conceived as being external to the U.S. electoral process, most notably pinned down as an issue of Russian interference. Where the UK reports above refer to the issue of data brokers in general and the subsequent power of these in the new economy of cyber, the American counterpart was less focussed on this aspect viewing the scandal in large part as a continuation of geopolitical rivalry. However, just as the media outrage following the scandal, the political reactions in the shape of reports and hearings, agreed on two crucial points. First, the threat illustrated by this scandal is viewed as a threat to democracy itself. Secondly, the scandal is only the tip of an iceberg of computational disinformation and manipulation. And we lack both the theoretical and the political tools to meet them both.

2.2.1) Big data

It is safe to say that there is nothing unique about the Facebook-Cambridge Analytica data scandal. As a data broker and analyst, the company is only one of many in the big business of big data. Data brokers are "companies that collect consumers' personal information and resell or share that information with others" (U.S. FTC 2014) In 2014, US Federal Commission published a report investigating the nine biggest data brokers on the market. They found, perhaps not surprisingly, that the business was virtually unregulated, and lacking in transparency, consequential to the practice of collecting consumer data without direct consumer interaction. The reason for this lack of transparency and regulation is not only a result of the mysterious workings of cyberspace itself, it is also a result of the unmet challenges of regulating a virtual space transgressing national borders and national jurisdictions (see Branch forthcoming; Mueller 2017). Despite the most obvious reaction to the scandal being the Mueller investigation on Russian interference, the use of data brokers is not limited to the purchase of big data by foreign countries wishing to interfere in national elections. The report by the U.S. Federal Trade Commission investigating the nine data brokers Acxiom, Corelogic, Datalogix, eBureau, ID Analytics, Intelius, PeekYou, Rapleafi, and Recorded Future shows that not only do six of these data brokers obtain some of their data from governmental sources, 'governmental entities' are also among their main clients, purchasing services such as 'Direct Marketing', 'Marketing Analytics', 'Identity Verification', 'Fraud Detection' and 'People Search' (U.S. FTC 2014). Cambridge Analytica, as a business within this landscape, is not a unique phenomenon, but an integrated actor within the larger economy of big data, governmental practices, and data brokers. What happens in cyber does not stay in cyber, rather, cyber-technologies, and big data collection and analysis, transform the workings of state security and practices. Additionally, big data, which is nothing without algorithms, which in turn are nothing without big data, is a black box for politicians and subjects alike. Therefore, in addition to the Facebook-Cambridge Analytica scandal not being unique, an important point is that the employment of psychographics by Cambridge Analytica, is not an incidence of exceptional manipulation, separate from the world working as "normal". The segmentation of people according to their beliefs and values, aimed at influencing certain behaviour is not limited to market advertising. It is also a technique of microtargeting and surveillance, where for instance the identification of potential criminals and the subsequent intervention by law enforcement is a stark image of the integration of big data analytics into the normal workings of the state (see Ferguson 2017a; 2017b).

In his research on police practices and surveillance in Chicago, Ferguson (2017a; 2017b) identifies not only the change in policing strategy in the use of big data: from a reactive or explanatory use of data to prediction, but also the secrecy of what the algorithms used in policing are. Like the findings by Brayne (2017) in her investigation of big data surveillance in Los Angeles, the problem of the lack of transparency and accountability is fundamental to a process marked by obscurity from the collection of data, to the purchase of data, and finally the implementation of data through algorithms. On this background, identifying what the threat of microtargeting is, is particularly strenuous. Microtargeting can hardly be conceptualised as a threat per se, rather it must be contextualised: who is doing what for what purpose, when and how is that threatening to what? This is the starting point of this thesis, where the research question "how is microtargeting a threat to liberal governmentality?" is a formulation aimed at allowing for this conceptualisation, placing liberal governmentality as a referent object. The choice of liberal governmentality is informed by the fact that microtargeting is embedded in liberal governmentality itself. Microtargeting is a *security dispositif* in the hands of the state; a tool in the governing of the individual. At the same time, the technique of microtargeting, exemplified by the Facebook-Cambridge Analytica scandal represents a threat to that governmentality. Thus, the context of microtargeting is what makes it a threat, rather than the technique objectively being so. The choice of liberal governmentality is not a normative one, claiming that the individual or exposed minority groups who are increasingly targeted by big data surveillance (e.g. Amoore 2006; Sparke 2006; Ferguson 2017a; 2017b), are not valid referent objects. Rather, it is an acknowledgement of the state being the main security practitioner, even when that practice is outsourced to private corporations. As pointed out by Leander (2005), among others, the privatisation of security does not necessarily imply competing security interests between state and corporation: the interests of the two align more often than not. The case of microtargeting is therefore interesting as the tension results not only from opposing interests, but also opposing interests depending on the same data brokers, using the same tools. An analysis aimed at unpacking the contextual aspects of meaning attributed to practices and logics underlying these mechanisms is therefore the best analytical starting point for arriving at a useful reading of the topic at hand.

The potential threat of microtargeting as perfected propaganda, if one were to hyperbolize, is not hard to grasp. If our online behaviour can be tracked and counted and thus facilitate an individualised representation of the web, subjecting us to manipulation, that is a dystopian future requiring counteraction. This image is of course exaggerated, which I will come back to. However, as a potential threat even its imperfect form would warrant countermeasures. It is also clear that as a manipulative force, microtargeting should be understood as something more than fake news. Where fake news, as pointed out in the DCMS report, as well as the SSCI report, refers to claims that can either be judged true of false, microtargeting pertains the promise of a certain truth to it. Microtargeted ads do not necessarily communicate straight out lies. Rather, they communicate nuanced messages that function to polarise.

Henry Farrell and Bruce Schneier argue that microtargeted communication is best understood as attacks on 'common knowledge' as they disrupt a shared agreement of what democracy is about. By this is meant that there are certain fundamental agreements in a democracy, as to how electoral processes should work, what the truth is, that "hold political systems such as democracies together" (2018: 2) There are other forms of knowledge in a democracy that are not shared among its citizens, such as what are the right priorities in its budget, how much state interference should there be in the economy, etcetera that there should be disagreement on as these disagreements are what makes a democracy a democracy. The problem of microtargeting, as well as fake news and other forms of disinformation, is that they attack the entire "information system" of society (Ibid.). Although useful as a starting point, as Farrell and Schneier acknowledge the integrated nature of offline and online information flows, this thesis argues that they miss a crucial point. Namely, the clear lines drawn up of what is contestable and what is incontestable knowledge fail to grasp how subtle nuances in messaging can easily fall in both categories. Furthermore, drawing these lines is itself a political practice; establishing what 'truths' form the fundament of a just political system is a fundamentally political exercise. Furthermore, the problem of microtargeting is that it is subtle. The problem of microtargeting is that as all manipulation it cannot easily be identified as such. As nuanced communication, this thesis argues that despite media outrage largely understanding the phenomenon as a threat to democracy, microtargeting is not best read as such. The polarising effect of nuanced communication cannot itself threaten democracy; questioning fundamental truths of how society should be organised cannot itself be considered a threat to democracy. However, it can be conceptualised as a threat to stability; as a threat to the very governmental reason of that stable democracy. It is here that governmentality arises as a suitable referent object for understanding the case.

3) Theory and core concepts: liberalism, democracy, and governmentality.

> Where there is power, where power is necessary, where one wishes to show effectively that this is where the power lies, there must be truth.
>
> Foucault (2012: 9)

> Myth turns into Enlightenment, and nature into mere objectivity. Men pay for the increase of their power with alienation from that over which they exercise their power. Enlightenment behaves toward things as a dictator toward men. He knows them insofar as he can manipulate them.
>
> Adorno & Horkheimer (1997[1944]: 9)

"How is microtargeting a threat to liberal governmentality?" is a question in requirement of conceptual clarification, as well as justification. Where microtargeting was defined in the introduction, 'liberal' and 'governmentality' are both concepts in need of a longer elaboration. The ambition of the word 'liberal' stretches beyond classical liberalism, and into what some may refer to as neoliberalism. The reason for the term 'liberalism' rather than 'neoliberalism' comes from an acknowledgment that the threat posed by microtargeting is not a threat posed specifically to neoliberalism. Rather, it is a threat posed on liberalism as it is formulated in its modern form, without the specific aspects of that ideology as grounded in neoliberalism being of exceptional importance. David Harvey defines neoliberalism as "a theory of political economic practices proposing that human wellbeing can best be advanced by the maximisation of entrepreneurial freedoms within an institutional framework characterized by private property rights, individual liberty, unencumbered markets, and free trade" (2007: 22) As an ideology it is apparent in the U.S. as well as in more 'social-democratic' political systems such as Sweden. It informs the outsourcing of welfare-services as well as the hegemonic discourse not only on how the economy is best organised, but also, how social phenomena is best understood; that is, read and measured. In Foucault's analysis of neoliberal governmentality, the expansion of the economic rationale into the non-economic realms of society is a key point (2004: 222) The choice of liberal rather than neoliberal governmentality is not a denial of these particularities pertinent to neoliberalism rather than liberalism. Rather, the choice of liberalism is an argument that the particularities of modern governmentality that makes it subjectable to the threat of microtargeting are not only a result of the rise of neoliberalism as an ideology and form of government. Rather, it is the result of a liberalism encompassing the particularities of neoliberalism. When this paper refers to ‘liberalism’ it is a concept meant to encapsulate the features of liberalism as well as neoliberalism. As such, it also escapes the conceptual discussion as to what to include in liberalism that is not included in neoliberalism, as well as the uneasy path towards delimiting what is neoliberal political ideology and what is an economic one, and what is liberal political ideology and what economic liberalism. This thesis holds that there is no significant distinction between political and economic ideology in the face of liberalism. Liberalism is, at least in part, defined by the government’s position vis a vis the economy: as the enabler of a particular capitalist economy. But what is more, liberalism is also tightly knit with the project of modernity, and in particular modernity’s claim to truth. It is here that Horkheimer and Adorno meet Foucault in the quotes at the beginning of this chapter: liberalism is not only an ideology presenting itself as such, but also a particular formulation of truth and a product of Enlightenment itself.

Foucault’s notion of power as knowledge (see also Foucault 1997); of definition of truth as a prerequisite of power, becomes apparent in the context of computation. It is here that the project of liberalism; of the antecedently individuated meets calculation as the episteme of the discursive formulation of reality. This thesis argues that it is at this fundamental assumption: that there is something individuated a priori, be that natural phenomena or the human, that these two ways of thinking meet. And it is from this starting point that they both adhere to a computational logic as a fruitful way of reading social phenomena. As such, the antecedently individuated work as a basic discourse shared by both computation and liberalism, from which different discourses are shaped by the practice of microtargeting. This final point will be elaborated on in chapter six of this thesis. Now, the basic concepts of liberalism and governmentality will be elaborated on, before providing a justification for why ‘liberal governmentality’ is chosen as referent object.

3.1) Liberalism and neoliberalism

> There is a limit to the legitimate interference of collective opinion with individual independence: and to find that limit, and maintain it against encroachment, is as indispensable to good condition of human affairs, as protection against political despotism.

Mill (2001[1859]: 9)

> The people is somewhat that is one, having one will, and to whom one action may be attributed; none of these can properly be said of a multitude. The People rules in all Governments, for even in Monarchies the People Commands; for the People wills by the will of one man; but the Multitude are Citizens, that is to say, Subjects. In a Democraty, and Aristocraty, the Citizens are the Multitude, but the Court is the People. And in a Monarchy, the Subjects are the Multitude, and (however it seeme a Paradox) the King is the People.

Hobbes (1998[1642]): Ch. XII, part VII)

Liberalism is often traced back to John Locke (1988[1689]) due to his formulation of property rights as a natural right. Just as Hobbes, Locke considered there to be inalienable rights in Man[1] that could not be infringed by the acts of the sovereign. Hobbes however, considered property rights to be a conventional right, whereas Locke famously expressed that property rights are an extension of Man's autonomy as property is the fruit of his labour. As such, property – just as the right over one's body – is a natural, inalienable right. As pointed out in the quote above by Mill, another early proponent of liberalism, liberalism is about the limits of the rights of the sovereign. The basic idea is that there is something fundamental in human beings that should be respected no matter what sovereign is put in place. That is, the sovereign is never completely sovereign, but limited by the fundamental rights of Man. What is curious in Mill's description of this limit

[1] The use of Man rather than human is here a direct reference to Locke's use of the term, and not an insinuation of the author's adherence to Locke's exclusion of women from a definition of human beings.

however, and which is why I have chosen to put it next to Hobbes elaboration of the people and the multitude, is that he writes about a sovereign which is not authoritarian, but democratically elected. For Mill, it was important to establish the limit of the sovereign precisely because democracy may give the majority tyrannical powers, powers that should be universally limited. Liberalism, therefore, is not only a limitation of sovereign powers, it is also an idea of the limitation of sovereign powers arising from a fear of what democracy may give us. As such, this fear, the fear of the 'multitude' as it were, bear clear resemblance to Hobbes writing two hundred years before Mill, of the fear of the many. That is, there is a fear of the collective underlying liberalism, where the positioning of the individual as the transcendental recipient of fundamental rights is the countermeasure to this potential threat.

With the idea of property rights as a fundamental right comes also the idea of the market as at least partially liberated from state interference. If property is an extension of Man's autonomy through labour, so must also other kinds of work be. Foucault writes on the two kinds of freedom formulated by liberalism: "one based on the rights of man, and the other starting from the independence of the governed" (2004: 42). The fundamental rights expressed by liberalism, therefore, are not only a limitation of the governor's power over the individual but is also a manifestation of the sovereign's responsibility to protect those rights for the individual. In its modern formulation, liberalism can be understood as comprised of a tripartite structure of political, social, and civil rights, where government is limited as it cannot infringe any of the three (Marshall 1950) The independence of the governed therefore includes the independence of the economy under liberalism. This independence of the economy from government has exacerbated under neoliberalism. As referred to by Foucualt, Hayek formulates certain laws for the economy under liberalism, or neoliberalism:

> if we want the Rule of Law to operate in the economic order, it must (…) have the possibility of formulating certain measures of a general kind, but these must remain completely formal and must never pursue a particular end. It is not for the state to say that the gap between earnings should be reduced. It is not for the state to say that it wants an increase in a certain type of consumption. (Ibid: 172)

The freedom from the governed has thus created an economic field that must also be liberated from the government. It is here that Foucault points to the two-faced nature of liberal governmentality: that its embedded logic of *not* governing implies an expansion of the logic of government despite its nominal decrease in governmental power.

Curiously, Bridle also refers to Hayek in terms of the expansion of the computational logic into our very cognition of what it means to be intelligent. Hayek, as an academic of psychology, proffered the view of a

> fundamental separation between the sensory world of the mind and the 'natural', external world. The former is unknowable, unique to each individual, and thus the task of science – and economics – is to construct a model of the world that ignores the foibles of individual people. (2018: 138)

Embedded in Hayek's conception of the human mind is an idea of the individual and the world as separate. The individual is antecedently individuated, the individual is not a social construct but an unknowable world to which societal organisation cannot accommodate individually. Hence, society must be constructed in an 'objective' sense, freed from individual particularities. From the perspective of computation, and more specifically the building of artificial intelligence, this entails a vision of connectivism, that is: "the belief that intelligence [is] an emergent property of the connections between neurons, and that by imitating the winding pathways of the brain, machines might be induced to think" (Ibid.) It is significant that liberalism and computational logic share fundamental beliefs of how reality is ordained. It is significant because that is yet another point where arriving at an objective definition of when and how microtargeting arises as a threat to liberal governmentality becomes even more impossible. The fundamental assumption of microtargeting is that there is something in human beings that is reducible to data points, or "connections between neurons" which lends itself to manipulation. That same presupposition also forms the basis for a formulation of a political system within which individuals are considered a priori individuated. The question then, of how microtargeting is a threat to liberal governmentality is therefore a question which should be answered beyond the technique of microtargeting itself. It must also answer the question on how the individual is read, and reciprocally constructed, in light of computational thinking through the technique of microtargeting.

3.2) Microtargeting and democracy

The positing of governmentality as a referent object deserves justification. Firstly, the choice of governmentality rather than democracy is based on the difficulty of formulating a definition of democracy allowing for microtargeting to pose a threat at all. Microtargeting is in this case, in its simplest form, a technique of advertisement. As such, it forms part of the competitive advantage of companies, fundamental to the workings of a (more or less) free market. Excluding microtargeting from a formulation of democracy would clearly appear as random. Additionally, it would counteract innovation in marketing techniques which microtargeting represents, undermining the whole idea of a democratic open market capitalism increasing efficiency and incentivising innovation. It would formulate a threat perception which would simultaneously counteract the very referent object one claims to protect. The referent object and the threat would conflate, where a conceptualisation of one towards the other would be circular and lead nowhere.

As a way out of this, one could formulate a definition of democracy within which the necessary economic power concomitant to the availability of big data and microtargeting for a political candidate would be viewed as a threat to democracy. However, especially in the U.S. context, this would oppose the provisions laid down in U.S. Federal election law ever since *Buckley v. Valeo* in 1976 (U.S. Supreme Court 1976), where limits to election campaign expenditure was ruled to be unconstitutional as it would limit freedom of speech. Opposing microtargeting to democracy would therefore require a conceptualisation of microtargeting as something different from just clever advertisement and thus an expression of free speech. However, psychographics and microtargeting can in their simplest sense be viewed as nothing but the incorporation of core tenets of behavioural psychology into the field of marketing, a technique that has been present long before big data business (Kahle & Chiagouris 1997). One would therefore be stuck with the same problem as before; one would have to formulate an idea of democracy as an institution and process within which microtargeting would not fit in.

One could, of course, argue that the employment of Facebook users' data without their consent is the threat to democracy inherent to the scandal. This would surely fit into a liberal narration of democracy, where privacy is a constitutive part of individualism. However, the fact that Cambridge Analytica was an intermediary corporation in the process of scraping data from Facebook, and the use of that data to train algorithms to formulate political adverts, diminishes Cambridge Analytica's role in this line of argument. Facebook has access to all this data anyway, and the expressed practice of Facebook of selling advertisements means that Facebook performs similar targeting techniques by itself, which are by no means illegal in terms of privacy rules: neither according to U.S. jurisdiction or to Facebook's own guidelines (C-Span 2018a, especially 00:51:06). This forms the fundament for the finance of Facebook as a social media platform, free due to the revenue generated by clever advertisement, a business model that is acclaimed for its representation of 'The American Dream' (Ibid., especially 00:08:56; C-Span 2018d, especially 00:33:05). By arguing that it is the accumulation of data through Internet use, and the subsequent lack of control individual users' have of that data after it has been produced, one undermines the whole logic of Internet in the era of liberalism, characterised by its "digital shadow of trading privacy for free private goods." (DeNardis 2015: 16)

Much of the response to the scandal has been caught in this circular trap, as exemplified by Heawood (2018). He attempts to formulate a threat representation within which the Facebook-Cambridge Analytica data scandal poses a threat to democracy as targeted adverts on social media conflates public and private speech. This conflation leads to a lack of critical thinking on behalf of the reader when encountered with what is public, but appear as private, communication on social media. The echo-chamber effect of this communication – where the subject to a large extent only encounters messages they agree with – leads to a lack of contestation of political ideas on "the marketplace of ideas" (Ibid.: 431). The problem with this argument, however, is that it presupposes that a conflation of public and private speech is itself a problem for democracy. One could argue that this distinction is not that clear in the first place: the use of personal allegories in political commentary, for instance, is not a new thing. The use of personal experiences – not necessarily shared in a public context – is a long tradition within feminism, where the slogan “the private is political” is key to understand second-wave feminism emerging in the late 1960s, to mention one example (Rogers & Kelly 2017). To draw a distinction between public and private speech is therefore a caricaturing of speech which does not necessarily make sense either without the context of social media. Building on this example, for Heawood’s argument to hold, one would also have to formulate an idea of democracy where this conflation would be a *bad* thing. On the one hand, this would involve a normative analysis of the case at hand, which is not the scope of this thesis. On the other, private communication has an important role in the deliberation, debating and sharing of ideas and experiences, especially in the history of virtually all forms of emancipatory politics. Where Heawood sees a blurry line between public and private speech, one could argue that this blurriness is irrelevant insofar as his conceptualisation of legitimate, or good, political speech lacks clarity and empirical fundament.

Secondly, he argues that the threat consists in the possibility of political actors to present one idea to one subject, and an incoherent message to another. This, apparently, leads to the inability of the electorate in the democratic process to hold politicians accountable to promises made. This latter point can easily be summed up as the claim that politicians lie. But there is nothing new about politicians lying. Furthermore, the premise that politicians cannot be held accountable for the paradoxical messages communicated with different segments of the electorate presupposes that individuals live solely on the Internet; that they in no way acquire news or political views from alternative sources, simply put that people do not talk to one another. Furthermore, if the problem was only the lack of transparency in political adverts, the solution could simply be to enforce advertisers to disclaim the different formulations of the message whenever they communicated one of the versions. This, however, has already been enforced by social media platforms such as Facebook, encouraged by the U.S. Honest Ads Act (Walker 2018; Singer 2018).

Heawood’s (2018) next point is that this conflation of public and private speech leads to the susceptibility of individuals to uncritically agree with messages they encounter, which in turn due to microtargeting will be messages they already are biased to agree with. Here as well, the argument only works insofar as the threat to democracy is understood as a threat to a certain variation of democracy we wish we had. Here, the argument follows along the same lines as Unver (2017), where not only microtargeting, but social media and Internet itself are seen as having detrimental effects on democracy. In his review of different narratives on how digital media threatens democracy, he identifies the tendency of polarisation in digital media, by which is meant that people with similar opinions form 'tribes' unwilling to communicate with 'tribes' of a different opinion. One can argue that this threatens a Habermasian deliberative democracy, a vision of democracy where the free exchange of opinions and views under freedom of speech, where all participants have the same capabilities for discourse and truth will emerge from consensus (Bohman & William 2017). That is, a good democracy is one where people are guided by reason and listen to others with different opinions, where everyone together has a healthy discussion aiding us to reach a common goal. This, however, is only one idea of what a 'good' democracy is. Mouffe (2005) criticises this vision of democracy for its inability to capture the opposing interests of the members of a democracy. A deliberative democracy allows no space for the antagonism inherent in politics, where we do not work towards a common goal. Rather, we have different interests, and different goals, and these differences must be expressed through political discussion, and compromised in the formulation of political solutions.

Additionally, the idea that rationality is the best guidance for democratic decision-making is a thoroughly normative one. One could also claim that emotional responses to political issues are just as legitimate as basis for decision-making as rationality. From this point of view, the tribal tendency of a cyberspace marked by "feedback loops of attention, attraction, and commodification" (Unver 2017: 132), where individuals more easily react based on emotion rather than so-called rationality, cannot itself be viewed as a threat to democracy. For microtargeting to be a threat to democracy, one would have to posit an ideal form of democracy which does not necessarily correlate with any of the versions of liberal representative democracies existing in the West. It would be an inherently normative exercise, where one would have to envision a democracy as it *should* be, and how it would be threatened by big data and microtargeting, which after all is a technique of advertisement which in the context of election campaigns can easily be viewed as an expression of the freedom of speech held so dearly by liberal democracies as they exist today.

3.3) Microtargeting and the individual

The choice of governmentality, rather than the individual, as referent object also deserves a justification. The use of Facebook users' data without their consent is a main concern in the hearings in the U.S. Senate on social media, democracy, and security following the scandal during 2018. Here, the right to privacy is an oft-mentioned theme. However, it is important to note that the vulnerability of individuals in the business of big data has mostly been viewed in the context of the possibility of this vulnerability being exploited by foreign adversaries, as exemplified in the opening speech of the Senate hearing on "Foreign Influence and Social Media" on September 5th 2018 (C-Span 2018d). By this is meant that the inherent vulnerability of individuals in the sharing of personal data, where the subsequent location and ownership of this data is unknown, leave them susceptible to foreign manipulation. This vulnerability is a consequence of the democratic process itself, that is, the fact that a 'free' and 'open' Internet is integrated into democratic elections is an element of the democratic process to be protected. The individualism and freedom constitutive of the representative democracy, is also the weakness of that very political system. The integration of online political behaviour with the offline action of voting therefore creates a new sphere of potential manipulation through misinformation, fake news, and microtargeted manipulation by foreign powers. The key here, is that this line of reasoning does not posit the individual as referent object. Rather, the vulnerability of the individual in this landscape is a threat because it may serve as a conduit for foreign intervention threatening democracy itself. Right to privacy, then, is not necessarily the referent object within this logic, rather, the aggregate of vulnerable individuals is considered a vulnerability of the U.S. as a democracy, framed within a geopolitical narrative within which Russia and Iran pose the main threat.

In addition to the possibility of manipulation of vulnerable individuals lays also a presupposition of what the individual is in liberal times. As will be identified in chapter five, before further discussed in chapter six, microtargeting threatens liberal subjectivity. Where the ideal of the individual is characterised by its autonomous decision-making, and fully-informed, microtargeting – or even algorithms and big data as a whole –

threatens this vision. However, this too does not necessarily put privacy as a basic right for the individual. Here as well, the individual vulnerability is first and foremost a question of protecting the individual as a way of protecting the societal order.

It should be mentioned that the U.S. Senate hearings following the Facebook-Cambridge Analytica scandal, which can be argued to reflect the general reaction by U.S. politicians after the scandal, are far from uniform in their threat perceptions. Notable exceptions are the identification of vulnerable minority groups and their algorithmic exclusion though automated advertisement tools, as well as the right to privacy itself being referent object to the aforementioned threat. However, the majority reaction, illustrated in its starkest form through the focus on Russian interference in the Mueller report on the investigation into Russian interference in the 2016 presidential election, places human security only secondary to wider geopolitical concerns. Although media coverage (e.g. Harzog & Richards 2018; Kosoff 2018) as well as subsequent lawsuits (e.g. Frenkel & Rosenberg 2018) have focussed on the right to privacy for the individual, most of the public political reaction has been centred on a logic placing democracy, and democratic processes in focus, leaving individual security secondary. Positing governmentality, rather than the individual as referent object therefore connects this analysis closer to the actual processes aimed at mediating the threat of microtargeting. Although positing the individual as referent object would be fruitful from a human security perspective, this thesis argues that the main effects of individuals' vulnerability is an effect only existing on the aggregate level. Clearly, the element of surveillance, especially in the interaction between state security officials and data brokers and analysts, is a threat to individuals' security as exemplified by Amoore's (2006) work on the biometric border, and the already mentioned big data policing, is important. However, from a political point of view, the fact that data brokers have more information on individuals than these individuals would like them to have, is not the security issue of main concern. However, the aggregate of this data harvesting, and the subsequent employment of this data for political manipulation, entails a theatre of power struggles between state and private corporate actors which is the focus on this thesis.

3.4) Governmentality and governance

Lastly, I will elaborate on the choice of governmentality, rather than governance, as the analytical tool for this analysis. As an analytical framework governmentality was introduced by Michel Foucualt in his *Security, Territory, Population* lectures (2007) and elaborated on through a series of lectures at Collège de France in the late seventies (see esp. 2001; 2004; 2012). The term lacks a comprehensive definition but can in its simplest formulation be understood as the 'conduct of conduct', that is an art of government meant to govern, or shape, the subjects in a certain manner (Foucault 2004). For Foucault, governmentality is not limited to the state. Government of children, of oneself, as well as subjects are all questions to be answered through governmentality: a concept that encapsulates both the technique and the rationale of government. It is central to this concept that it is the population that is the target of governmentality, be it the individual governing itself through Stoic ideals (Ibid.: 88) or be it the state implementing compulsory education for all its subjects. Therefore, in governmentality who governs is open for question, but the subject of governmentality will always be the population (Joseph 2009).

From a liberal perspective, governmentality as both technique at rationale of government is particularly useful. Whereas previous developments in governmentality witnessed an enlargement of the state: e.g. education, urban planning, health care, the police, neoliberal governmentality is marked by its apparent shrinkage of the state. Although developing the idea of governmentality at the end of the 1970s, Foucault identified this peculiar position of neo-liberalism, as "freedom through the encouragement of competition" (Joseph 2009: 414) By this is meant that the apparent shrinkage of state power or state involvement in subjects' life, is only a freedom from government to act according to the neo-liberal ideals of competition. In this sense, despite the decrease in government, governmentality remains ever so much powerful under neoliberalism. Empirically speaking, this claim gains support from research such as Curran and Hill's meta-study into the increase in perfectionism and its correlating increase in mental health disorders among millennials published in 2017. Curran and Hill identify how the competitive culture pertinent to neoliberalism leads not only to increased self-criticism among people born from 1989 and onwards. It also leads to increased expectations towards peers, and a devaluation of activities that are not deemed ‘productive’, i.e. as advancing a certain social mobilisation or a work-related career path. Neoliberalism, as ideology and rationale, is internalised in the subject; neoliberal governmentality is the governing beyond government. The allowance for open market competition is a tool of neoliberal governmentality, which entails a rationale within which the individual is responsible for their own success and happiness, and the competition between individuals to advance their respective goals is a healthy competition. Just as the competition between actors on the market is a healthy competition according to proponents of liberal market capitalism (Harvey 2005).

Governance, on the other hand is perhaps best understood as a “plurality of actors interacting in networks across the organizational and conceptual divides by means of which the modern state has conventionally and all too conveniently been understood: notably, the distinction between state and civil society, and the distinction between public and private sectors.” (Bevir 2011: 19). Thus, governance is about the decentralising of power, of transferring power away from the state and towards other actors. From the domestic perspective, the modern use of the term is usually traced back to Robert A. Dahl in his book *Who Governs? Democracy and Power in an American City* (1963) Here, governance as a theoretical tool was an attempt to answer the question on who governs in a democratic state, where there is nominal equality, but “knowledge, wealth, social position, access to officials, and other resources are unequally distributed” (Ibid.: 1) His main argument is that the liberal democracy is best described as a polyarchy, governed through democratic governance, where different groups with different interests compete to govern. As such, the power of government cannot be reduced to the government itself, rather it should be understood through several sectors of influence.

Although a main work on the theorisation of governance in the domestic context, the idea of global governance is a far more recent concept. Global, or international, governance is conventionally traced back to Rosenau and Czempiel’s *Governance without Government: Order and Change in World Politics* from 1992. Although it does not mention ‘global governance’, as it is conventionally used today, it is considered seminal as it distinguishes between government as institution and government as practice (Sending & Neumann 2006). In this distinction, governance has clear parallels to governmentality. Governance, however, upholds greater promises of governance beyond government, where the interaction of typically civil society, private companies and states is "coordinated through both formal and informal rules and guidelines in such a way that a common or public goal is advanced." (Ibid.: 653) A problem with governance, however, is that it implies a shift in power and authority from states to private actors. This shift does not necessarily capture the alignment of state and private interests in a political arena. Furthermore, it does not capture the fact that civil society, or private actors, may be allotted a place within a decision-making process on the states' mercy for the function of legitimising the said process. That is, the presence of non-state actors in a political process should not automatically be equated with a diminishing role of the state, and the transference of power from state to non-state actors (Joseph 2009; Mueller 2017; Carr 2015; 2016). Sending and Neumann (2006) argue that the shortcoming of governance in terms of analysing power relations within a political process lead to a focus on the institutions of decision making – that is, identifying the actors present, but not focussing on what they do (see also Jackson & Nexon 1999; Nexon & Neumann 2018). This posits governance in stark contrast to the initial promise of process before institutions as proffered by Dahl, and Rosenau and Czempiel. It is precisely because of this lack of power analysis that I have chosen to focus on governmentality rather than governance. Although this thesis mainly focusses on the domestic aspects of the case, this is due to lack of space rather than relevance. As I will argue in chapter six, the findings from this research should also inform work on cyber from the international level. Also, from this perspective, this thesis argues that governmentality is a better analytical lens than governance.

Here, it is relevant that Internet governance, as a field of study, is the most prominent of the theoretical, or ideological, approaches to global Internet politics. My focus on governmentality is thus also a criticism of multi-stakeholderism – the theory within Internet governance holding that Internet is best governed through the interaction of the stakeholders of government, private companies, and civil society. With exceptions such as Madeline Carr, Mark Raymon, Laura DeNardis and Milton Muller, multistakeholderism has proceeded virtually unchallenged within academia as well as public policy. One of the main problems of multi-stakeholderism, as identified by Carr (2015) is the limited role of civil society in the governance of Internet. The presence of civil society in a decision-making process serves virtually only a legitimising function. Furthermore, the role of international organisations, such as The Internet Corporation for Assigned Names and Numbers (ICANN) in the governing of Internet, are products of a Western, and most often American, history and vision of what the Internet is and should be. The problem, therefore, with governance as an analytical tool, is that it does not adequately capture the power structures discursively narrating the field of Internet politics, underlying national and international politics. Neither does it capture the underlying liberal rationale of proposing governance as the most suitable arrangement for governing politics.

3.4.1) Governmentality and the international

A problem, however, with applying the framework of governmentality to an analysis that seeks to be relevant to the international aspect of Internet governance, is that governmentality does not fit easily as a theory within International Relations (IR). One of the reasons for this is that whereas people are the object of governmentality domestically, the objects internationally are states. Mitchell Dean argues that an internationalisation of governmentality requires a conceptualisation of governmentality as operating "through both the existing arts of domestic government within nation-states and as an attempted extension and generalization of them across the planet. It thus seeks to move from a liberal art of government to a planetary *nomos* of world order." (quoted in Joseph 2010: 224) The problem, here, however, is that if the people are the subjects of governmentality, the rationale of a liberal governmentality would only apply as a *nomos* to the parts of the world enjoying a liberal order. Joseph (2010) resolves this problem by identifying international governmentality as only relevant for liberal countries. Although not being explicitly mentioned by Sending and Neumann (2006), their conceptualisation of the participation of civil society as both an object and subject of liberal governmentality presupposes that liberal governmentality is already a fact in the countries in question. This, of course, is factually dubious, as liberalism remains a Western phenomenon. In order to avoid this conceptual confusion, I propose a conceptualisation of international governmentality as an attempt to expand liberalism, at different degrees of success. The dominant position of Western liberalism within Internet governance, is thus an expression of an attempt to expand a certain idea of governmentality. And one can argue that the perspective of governmentality is even more relevant to the context of global Internet politics. Cyberspace, after all, is not nationalised, and the perspective of governmentality may be better suited to capture the element supra-national nature of Internet politics.

The success of the attempt to expand liberal governmentality is beyond the scope of this thesis, but to claim that liberalism is in a privileged position is far from controversial. Thus, the hegemonic order of international society, characterised by what Nexon and Neumann (2018) conceptualise as field-specific, borrowing Bourdieu's vocabulary, is better understood as an internationalisation of a specific form of governmentality, rather than governance. Governmentality, according to Foucault, should be understood along the axis of security-sovereignty-government, where the lack of governmentality can be replaced by either one of the three (Rose et al: 2006; Lemke 2002). Regarding Internet governance, governmentality is also a useful theoretical framework as the Western idea of governance and the liberal vision of Internet is prominent within Internet governance as an ideology. This is conceptualised by Carr (2015, see also Mueller 2017) as a Gramscian hegemony in Internet governance. Here, the dominant western idea of a 'free' and 'open' Internet – free from state interference, is dually captured in a distinct Western idea of what individualism, freedom, and openness entail. In that way, a liberal ideology of how individuals should be free within the domain of Internet, is an expansion of a liberal idea of government as Western jurisdiction of individual freedoms should also apply to the Internet.

4) Method and data: Language, practice, and discourse.

Discourse analysis is a subjective entrance point to reading the world in a useful manner. What is meant by this is that discourse analysis refutes the positivist claim of there being an objective way of gaining knowledge of social phenomena. As such, discourse analysis is always a subjective, interpretative endeavour aimed at revealing the construction of meaning through language, practice, and power. Discourse analysis is about the deconstruction and reordering of signs. Dunn and Neumann write that “all the factors that social science research examines – be they biological, psychological, institutional – are, first and foremost, discursive objects.” (2016: 43) This thesis goes beyond this claim to state that everything is not only first and foremost discursive objects, they are only discursive objects. This does not mean that there is no objective world outside of human perception, but it does mean that our only access to the world is through discourse; through signs. There is nothing outside meaning. This is a core distinction between critical discourse analysis (CDA) and post-structuralist discourse analysis. Where CDA, most famously formulated by Fairclough (see 1992; 2013) holds that there is a distinction between discourse and social practices, post-structuralist discourse analysis holds that this distinction does not exist. However, post-structuralist discourse analysis (henceforth only ‘discourse analysis’) still holds that “other social practices (such as media, schooling, and family) produce meaning only as a by-product, while language *primarily* intends to construct meaning” (Dunn & Neumann 2016: 43) I argue that this approach does imply that there is, in fact, an ontological distinction between social practices and discourse. This complicates how to posit for instance works of art, or routine actions such as introduction and a handshake – is art language and is there a distinction between giving a handshake and presenting one’s name, or is both a part of the same practice, and if so, is this a practice or language?

The problem of focussing explicitly on language in the study of discourse, at the same time as one holds that everything is discourse, has led to an ongoing debate within discourse analysis. Proponents of a linguistic turn argue that social phenomena are best understood through a focus on language, and the practice turn argues in favour of analysing practices as an entrance point for understanding social phenomena (Neumann 2002; Schatzki 2006). These two debates overlap on many of their assumptions despite their differences in focus. Hansen argues that “the strategy of discourse analysis [is] to ‘incorporate’ material and ideational factors rather than to privilege one over the other” (quoted in Dunn & Neumann 2016: 67). The significance assigned to materiality in Hansen’s discourse analysis does allow for a wider incorporation of practices’ significance within a discourse. However, from the perspective of STS, a problem with most language-focussed discourse analyses is also their inability to adherently capture how technology may autonomously produce meaning through machine learning and artificial intelligence (AI) Here, more practice-oriented approaches to post-structuralist methods, such as ANT (Latour 2005), offer important insight. As already mentioned, ANT claims that action is dislocated and can be generated through human and non-human actors alike (‘actants’ in ANT vocabulary). This implies two important things, namely that human and non- human actors are ontologically symmetrical, and it means that *intent* is irrelevant. It is these aspects that have contributed to ANT’s role within STS, as a premise of STS theorists is that technology is best understood in its reflexive relationship to society, meaning that technology should not be considered external to human activities, nor should it be considered objective (McCarthy 2018a).

ANT as a method does not make any prior assumption as to the network of actants and processes it is to investigate. Rather, it proposes an ethnographic approach to the research object liberated from prior categories. Subsequently, a problem with ANT is its concomitant one-dimensional approach to the world of meaning. As it is primarily focussed on local processes, aiming to investigate assemblages on a micro-level through ethnographic research, it lacks historicism in its approach to meaning-formation. Furthermore, it complicates any cross-case comparison. It is useful for taking ‘snapshots’ of social phenomena, for identifying which relations sustain the stability of a network. However, these ‘snapshots’ are less useful for understanding long-term power relations and hegemonies, upheld by discursive formations; closing concepts, stabilising language. Despite this, an important contribution by ANT is that it “takes materiality seriously” (Bueger & Stockgruegger 2018: 42) by dispersing the distinction between human and object, practice and discourse. Discourse analysis has a tendency to make a distinction between language and non-language through its expressed focus on language. ANT is not preoccupied with this distinction at all, and it is in relation to STS that this theoretical contribution is key. The focus on computation in this thesis requires an acknowledgement of the role of technology. Where discourse analysis would easily fail to recognise the production of meaning by technology, ANT offers a vocabulary for the incorporation of exactly that. To circumvent the problem of ahistoricism in ANT, Knorr Cetina (referred to in Bueger 2015, see also Knorr Cetina 2006) proposes a combination of ANT and practice tracing. Practice tracing is preoccupied with tracing practices and abstracting them to the theoretical level of mechanisms, where "practices describe ways of doing things that are known to practitioners", whereas mechanisms refer to the "theoretical abstractions that social scientists coin in order to classify practices, usually across cases." The purpose of mechanisms, therefore, "is not to match actual social instances, but to draw useful connections between them." (Pouliot 2015: 238) Like ANT, practice theory views causality as local and context-bound, with an emphasis on ethnographic research to identify this causality. However, where ANT does not aim to generalise causality across cases, as its main objective is on the micro-level of social assemblages, practice theory holds that "the social scientific gaze must always look beyond specific cases, towards cross-case generality" through the objectives of "induction, interpretation, and abstraction" (Ibid.: 240).

It is important to understand that 'causality' carries a different meaning in practice theory compared to the positivist understanding. Here, causality accommodates for the blurriness of temporal and spatial borders pertinent to the case at hand: causality simply means that all events relate to other events. Causality should be understood as local, and the generalisation of causality through theory should "capture the generative links between various social practices [as] practice theories are neither true nor false, but useful (or not) in making sense of messy arrays of practices." (Ibid.: 239) Furthermore, what renders a practice causal, "what makes it produce social effects, are the practical logics that are bound up in it and intersubjectively negotiated" (Ibid.) Following this, "the basic objective [of practice tracing] is to understand what the practice under study *counts as* in the situation at hand" (Ibid: 243) Thus, practices should be studied and reconstructed from within before abstracted to the higher level of mechanisms. Furthermore, central to practice theory is that the importance lays not in what actors say when they talk about practices, rather, the key is to understand where the actors speak *from* when they speak.

The emphasis on the tacit in practice theory, as “practical knowledge is generally unsaid” (Pouliot 2015: 246) fits neatly with the post-structuralist ambition to uncover the underlying logic of meaning-production within a wider definition of discourse. Whilst adhering to this principle, this thesis goes even further as its focus is not limited to the tacitly said; it also incorporates the explicitly silenced. This thesis shares the ambition of practice theories and discourse analysis in formulating a theory of the world that is ‘useful’; that makes sense, by uncovering the tacit logics formulating a messy array of phenomena. The purpose of a theory is not to offer a law-like account of how cause generates effect in the social world. The purpose of a theory is to offer a reading of the world that is useful. Where practice theory falls short, however, is in its reactionary role towards discourse analysis (Neumann 2002). Where discourse analysis fails to acknowledge the role of the non-verbal in meaning-formation, practice theory fails to focus on the verbally expressed discursive struggles to formulate the meaning of practices. Where one starts with practice, and the other starts with discourse, this thesis argues along the lines of ANT, echoing Hansen’s words, that the starting point of analysis need not be one or the other. This again echoes Neumann (2002) and his call for incorporating practices in discourse theory as a necessity for understanding social phenomena.

On the question of ontology, Judith Butler’s (1997) argument that speech is action is a useful premise and it is from that premise this thesis starts. There is no distinction between text and practice; rather they are both practices – or both discourses. This view is supplemented with the “overall idea of discourse theory (…) that social phenomena are never finished or total.” (Jorgensen & Phillips 2002: 24) Words and concepts; signs, acquire meaning in their relation to one another, as if language were a fishing net of relations between signs, where nodes are interlinked and ever-attempting to cement their relation to one another. But these relations, these nodes, are never totally fixed, and subsequently neither are their meanings. It is here the discursive struggle emerges, as “[w]e constantly strive to fix the meaning of signs by placing them in particular relations to other signs (…) we try to stretch out the fishing-net so that the meaning of each sign is locked into a specific relationship to the others.” The aim of discourse analysis, then, is “to map out the processes in which we struggle about the way in which the meaning of signs is to be fixed, and the processes by which some fixations of meaning become so conventionalised that we think of them as natural." (Ibid.: 25-26)

Chapter five of this thesis takes the discourses of the U.S. Senate hearings following the scandal as a starting point for understanding the Facebook- Cambridge Analytica scandal. This is not done to employ an analysis along the lines of critical discourse analysis, where the discourses are viewed as separate from the actions, practices, and mechanisms making up the case. In CDA, discourses are what enable social practices. From the perspective of post-structuralism incorporating the material components of discourse, however, approaching the discourse is a way of approaching the practices directly, as these practices are only practices insofar as they are inscribed with meaning. These meanings cannot be captured separate from the context whence they emerge. To understand this context, the ideal would be to employ ethnographic methods to the specific context of the Facebook-Cambridge Analytica case. As this is impossible, the second-best is to situate the case within the wider narration of computational logic. Thus, microtargeting, both as a technique as well as a part of the data collection practices of data brokers, reproduce a Cartesian understanding of the calculability of the individual. The logics of computation and liberalism underpin the conceptions of the data scraping and the microtargeted adverts, as well as the discourses on the ramifications of the scandal – questions on what Facebook is, what data brokers are, what data is, and how electoral campaigns should look like.

As already mentioned, there is nothing in microtargeting itself that makes it a threat. Rather, it becomes a threat within a specific context, within which it is prescribed a specific meaning through certain practices. However, the same practice, microtargeting, is also assigned with a meaning where it is not understood as a threat. It is the underlying rationale of these different narratives that is the focus of chapter five, rationales that will be contextualised within the rationale of liberal governmentality in chapter six. I propose that the best framework for capturing these meanings is through the perspective of computation as alluded to above. Rather than viewing the instances of data scraping, alleged foreign intervention in U.S. elections, and the use of microtargeting as separate phenomena, their very existence as discursive constructs mirror a wider adherence to a computational way of both prescribing the world with meaning, and subsequently reproduce that very world. It is from this perspective that the reception of the case, the practices making up the case, the discursive struggle in formulating what the Facebook-Cambridge Analytica scandal is, what Internet governance is, and the rationale of governmentality are interlinked and best studied. I argue that all these entities of meaning culminate in the case subject to this thesis. Rather than viewing verbal discourses and non-verbal processes as separate, they should be studied as interlinked practices producing and upholding meaning. By taking this as a starting point, the relevance of the logic of microtargeting, the epistemic presuppositions of microtargeting, as well as the rationale of liberal governmentality, should be studied as contextually interlinked; as practices with local causality, informing a theoretical abstraction.

Keeping this in mind, however, there are certain challenges to the method of this thesis. The first relates to the difficulty in approaching the topic through ethnography, which would have contributed to the findings in this thesis. Ethnography would allow for insight into the meaning of practices in their proper context, placing the researcher closer to the research object. However, in this case it would be impossible as it would require a travel back in time to observe or participate in the practices of Cambridge Analytica. Finding a contemporary case would be difficult as well, as the secrecy surrounding these operations are crucial to their functioning. One could also argue that it would have been beneficial to interview the key actors in the event. It would be difficult, given the temporal and financial limits of this thesis, to arrange for such interviews with high-ranking professionals, and doubtful that they would be willing to participate. However, Aleksandr Kogan, Chris Wylie, Alexander Nix, as well as Mark Zuckerberg have all been questioned in hearings before the UK Parliament and/or the U.S. Senate. These hearings provide useful insight into the meaning attributed to the practices in the case by the key actors on both sides of the questioning table. Using these hearings as analogous to in-depth interviews is therefore a fruitful approach for gaining insight into the practices forming the event; they give insight into where the actors speak *from* when they speak.

Another potential difficulty with the case, however, is gaining insight to the black box of psychographic algorithms. Where the general idea behind the psychographic algorithms deployed by Cambridge Analytica are known through both witness accounts as well as the corporation's own (biased) advertisement, the specificities of psychographics as a technique are difficult to gain knowledge of. But, as psychographics is a form of microtargeting, drawing on general knowledge of microtargeting is a second-best approach to the problem. One could argue that the meaning attributed to these techniques, rather than their 'objective' workings are the most important. However, when it comes to the production and assignment of meaning, ANT's emphasis on the ability of the non-human to act is highly relevant in relation to algorithms and machine learning. Algorithms do themselves generate meaning; they are data made legible. However, they perform a process of virtually no human intervention, except from the author of the source code. Through the process of machine learning, algorithms are characterised by their abstraction from human formulation. They generate meaning through their reformulation as they encounter huge amounts of data. In order to circumvent this, a reference to the implications of computational thinking in general – on our perception and cognition of the world – helps to abstract these hidden practices and identify their underlying logic.

Psychographics is a thoroughly computational way of understanding humans and human behaviour. In its promise of categorising values and beliefs lies a presupposition of what humans really are. In order to understand the Facebook-Cambridge Analytica scandal; the event 'itself', the focus should be on what key actors make of the case. The question should be what narratives are constructed by the actors involved to make sense of what happened. Actions, behaviour, and practices are all embedded with meaning; they are attributed meaning depending on context and actor. The next chapter is a discourse analysis of the event, where I will focus on two of the hearings in the U.S. Senate following the scandal including the main actors. I will argue that three ideas are central, each attempting to formulate a version of the Facebook-Cambridge Analytica scandal as 'new'. These three articulations are that of psychographics being qualitatively different from microtargeting, that the main threat represented by the case is that of the power of big data transforming capitalism, and that the individual in cyber-times is left vulnerable and susceptible to algorithmic manipulation. Chapter six an attempt to develop a theoretical framework of microtargeting as a threat through a discussion starting from the findings in chapter five. Here, the threat posed by microtargeting and big data to the function of the market is not the only issue to be discussed. The epistemological challenges posed to liberal subjectivity are also in focus. Therefore, the purpose of chapter six is to untangle both the threat posed by microtargeting to governmental techniques and rationale, as well as the threat posed to the liberal subject; to the subject of liberal governmentality.

5) Analysis: The meaning-formation of the Facebook-Cambridge Analytica data scandal.

> Blanket advertising, the idea that hundreds of millions of people will receive (…) the same advert, is dead. My children will certainly never understand this concept of mass communication. Today, communication is becoming ever increasingly targeted. It's being individualised for every single person in this room. You will not only see advertisements for products you care about, you will also see these advertisements nuanced in a way that reflects the way you see the world.

Nix (2016)

With the emergence of the utopian boundaryless space of cyber, characterised by endless information and possibilities, comes also the imaginary of a dystopian world characterised by surveillance and big data. What is curious is the concomitant nature of these depictions, as at its core, the Internet is nothing but information; the Internet *is* data. In a way, cyberspace is the literal presentation of the Foucauldian thesis of space as knowledge; it is literally constructed by a binary language transmitting information, knowledge, through electrons[2]. As such, big data is a necessary consequence of the Internet even existing. It is in this that the promise of the perfectly computational human being, receptible to the personalised, individualised presentation of the web, is contained. In many ways this vision is dystopian, but in other ways it is also exaggerated. In the end, human beings do not only live in a cyberspace distinguishing us from the physical presence of others. However, the increased computation of the world as we know it; the integration of the Internet, of data, into the functioning and perception of the world, entails challenges and possibilities. For Alexander Nix, the former CEO of Cambridge Analytica, it means complete individualisation. It means a complete calculability of human beings based on their cyber-behaviour. To a certain extent, this vision is flawed. As pointed out by Ansorge (2016), the collection of data and the surveillance of individuals provide the

[2] In the near future, this information may be transmitted through photons due to the emergence of Quantum Internet, see for instance Chen (2017)

observer only with a representation of the subject. This representation is only partial; it captures its identification, but not necessarily its identity.

Despite this, the invasion of privacy pertinent to the media outrage following the Facebook-Cambridge Analytica data scandal does illustrate the perception of something profound and personal as under attack due to big data business. There is something personal at stake when big data is proclaimed to be the new oil, as big data produced by individuals generates profit for corporations before it is reformulated and presented back to the individual who has gone from producer to consumer in the circular process of cyber (Adesina 2018). Our personal information leaves our control in its leap into the great void of electrons transmitting knowledge through algorithmic formulations feeding our representation of a cyberspace ever fixed in flux. The question of big data, however, is more than a matter of our personal life being subject to exploitation, it is also a question of our cognition of the world (Halpern 2018; Dieter & Gauthier 2019). Big data, and with it, big data analytics, carries with it a new epistemology: there is more to big data than the quantitative leap to ‘big’. Kitchin identifies these changes as consisting in its huge volume, its high velocity, its diversity in variety; it is exhaustive in scope, fine-grained in resolution, relational in nature, and flexible as it holds “the traits of extensionality.” (2014: 1) These points will be discussed in more detail in chapter six. However, the point that the emergence of big data is more than a quantitative transformation; it is a qualitative change in how we gain knowledge of the world, is an important point regarding microtargeting. There is more to psychographics than efficient advertisement and individualised communication. There are epistemological consequences in the way knowledge is produced, put in system, transferred, and made accessible. The Facebook-Cambridge Analytica scandal, despite the response to the event largely being framed as a problem of privacy and foreign interference in electoral processes, is more profound. What is more, psychographics as communication should be understood as a continuation of the ambition of early cybernetics, where the ‘cyber’ in cybernetics “already assumes a complex relationship to temporality and history – bridging the past with an obsessive interest in prediction, the future, and the virtual” (Halpern 2014: 41). Psychographics then, as an obsession, goes beyond prediction in its promise of the formulation of the future through the mechanism of manipulation, resulting from interpretation and control.

On March 17th, 2018, The Observer published an article describing how Cambridge Analytica, a data broker and analyst specialising in electoral campaigns, had scraped the data of more than fifty million Facebook users[3] (Cadwalladr & Graham-Ellison 2018). The data had been used to develop analytical tools deployed in the U.S. Presidential election 2016, as well as the UK Brexit campaigns among other electoral campaigns (Ibid.; Mayer 2018). The scandal that erupted lead to media outrage filled with questions as to what had happened, how data should be protected, as well as how electoral campaigns should be regulated in the era of big data.

The data had been scraped via a third-party app, called 'thisisyourdigitallife'. The app was designed by the Cambridge academic Alexandr Kogan, originally for a personality test categorising the subject along the five axes of openness to experience, conscientiousness, extroversion, agreeableness, and neuroticism: OCEAN for short (Hern 2018a). Kogan was affiliated with the Cambridge Psychometrics Centre, where he had developed the app, similar to the Cambridge researchers Michal Kosinsky and David Stillwell's app myPersonality quiz, in 2013. OCEAN is known as the 'Big five' or 'Five-factor' personality test. It is often referred to as a 'trait theory' in that "individuals can be characterized in terms of relatively enduring patterns of thoughts, feelings, and actions; that traits can be quantitatively assessed; that they show some degree of cross-situational consistency; and so on." (John et al 2008: 160) The basic idea of psychographics is that to categorise individuals according to these five personality traits would make it possible to nuance a communication in a way that would manipulate the subject's behaviour (Martinez 2018).

The myPersonality test, which was only available through Facebook, was launched as scientific research and the participants were paid for their answers. However, as the participants provided their responses, data on their online behaviour, as well as all their friends' data, was scraped via the app. Kogan was contacted by SCL Elections in 2014, a part of SCL Group and the mother company of Cambridge Analytica, and offered money

[3] The number was estimated to be about fifty million in the article referred to, but is now estimated to be the data of 87 million Facebook users (Lapowsky 2018)

in exchange for the data collected through the app. As the app was developed in 2013, it did not fall under the guidelines imposed by Facebook in 2014, which prohibit the scraping of data of consenting users' friends, making Kogan particularly valuable for SCL Elections (Wong et al 2018). SCL Group is a company operating through different daughter companies such as SCL Elections and SCL Defence, each specialising in their own field of 'strategic communication', that is the use of big data to microtarget communication to modify behaviour. SCL Elections claims to have been involved in "[m]ore than 100 election campaigns in over 30 countries spanning five continents." (Ghoshal 2018) SCL Group has also been involved in military and security operations in several countries, including NATO, the U.S., and U.K. SCL "carries a Secret Clearance as a 'List X' contractor for the British Ministry of Defence" and has "conducted surveys in Iran and Yemen for the Pentagon in the past." (Medium 2017) As mentioned in chapter two of this thesis, this is important as governmental entities are among the main customers of data brokers and analysts. Understanding the response to the Facebook-Cambridge Analytica scandal requires us to acknowledge the relations between SCL Group, a company which according to the whistleblower Christopher Wylie is synonymous with Cambridge Analytica (C-Span 2018b: 00:1:04) and the states put to resolve the issue.

Regarding tech in general, this dependence is not only in relation to data brokers, it is also applicable to the Silicon Valley companies. Here, Google's refusal to continue its cooperation with Pentagon on the Maven project, whose purpose was to develop AI for the military, is perhaps the most known example. (Wakabayashi & Shane 2018). In 2017 the project, also known as Algorithmic Warfare Cross-Function Team, was launched. It was to focus on "computer vision – an aspect of machine learning and deep learning – that autonomously extracts objects of interest from moving or still imagery." (U.S. DoD 2017) Google's involvement in the project led to protest amongst the company's employees and more than 3000 signed a petition against the company's involvement in the project (Frisk 2018). The protest against the weaponizing of AI lead to Google pulling out of the contract in June 2018 (and subsequently refusing to attend the hearing in the Senate on September 5th on the role tech companies and social media, see C-Span 2018d, esp. the opening speech) feeding a wider debate amongst Silicon Valley tech companies on the role of big data, AI, technology, and warfare (Fryer-Biggs 2018) Project Maven, AI and the military illustrate the complications in the relationship between data brokers, tech companies, and governments. These relationships are not only marked by the dependence on big data and technology by states. They are also symptomatic of the inability of governments to control tech companies and big data.

In 2014, Kogan set up the company Global Science Research (GSR) in order to sign a contract with SCL Group. The purpose of the data provided by Kogan was to develop analytical tools for training algorithms perfecting the targeting of political ads. The targeting technique used was that of psychographics: the categorising of individuals according to their demographic traits as well as their psychological characteristics. Psychographics refers to this technique of segmenting a population not only based on their demographic attributes, but also in terms of their values and beliefs. In marketing, some researchers even use the terms ‘psychographics’ and ‘lifestyles’ interchangeably to describe this analytical process of segmenting consumers (Kahle & Chiagouris 1997). The element of values and beliefs to this technique was marketed as key. Whereas ‘microtargeting’ is used interchangeably with psychographics in some of the literature, psychographics includes inputs from behavioural psychology, apparently making it more than ‘simple’ big data analytics. However, the fundamental logic of the technique is the same as for microtargeting: the individual can be understood on a profound level through an analysis of their online behaviour. The data can then be used to personalise communication, be it through the presentation of specific news articles on your Facebook feed, or be it the adverts for products presented on Instagram. The idea is that a binary language can make the individual calculable and susceptible to manipulation. The psychographic models used consist of algorithms, categorising people into specific segments according to their psycho-social traits. In order to develop these algorithms, however, one needs a sizable training set of data. That is, the algorithms themselves are not readily formulated by a data scientist, rather, they are developed through the process of machine learning: first the algorithm is coded to predict a certain outcome, before the data feeds back to the algorithm, modifying its ‘mistakes’, reproducing a better version of the original algorithm; perfecting computation.

In May 2018, Cambridge Analytica decided to close down and start insolvency proceedings following the media scandal (Solon & Laughand 2018). The problem, however, is that because of the loose structure of Cambridge Analytica and SCL, knowing exactly what was being closed down, and if Cambridge Analytica would simply re-emerge with the same people and the same data under a different name is unclear. SCL and Cambridge Analytica had, in May 2018, "at least 18 active companies, branches, and affiliates with similar names, based in the U.K. and the U.S." (Siegelman 2018) Especially the emergence of the firm Emerdata has raised concerns. The company was joined by Rebekah and Jennifer Mercer – the Mercer family was the main funder of Cambridge Analytica – in March 2018. Core players in Cambridge Analytica and SCL were transferred to Emerdata during the spring of 2018, including Alexander Nix, who became CEO of the new company (Ghosh 2018) What has happened to Emerdata is hard to know, but the obscurity of the issue illustrates how the intangibility of big data is not only in its collection and deployment. It also lays in the very corporate structure of the actors involved.

The purpose of this chapter is to unpack the black box of what happened in the Facebook-Cambridge Analytica data scandal. This is based on the premise that the practices causing the event to unfold are practices embedded with meaning. As such, the event itself is a discursive construction. By doing so, I will attempt to untangle the web of actors and their relations, in order to trace the logic and practices constituting the properties of a context within which microtargeting arises as a threat to liberal governmentality. Central is the question of what meanings are attributed to the practices in the event, and what are these meanings' underlying logic? And what is the context within which these practices occur? The empiricism of the chapter is that of secondary sources, due to the impossibility of investigating the scandal at a first-hand basis. The focus is on two of the hearings before the U.S. Senate following the scandal. The first is from May 16th, 2018, where Christopher Wylie testified at a Senate Judiciary Committee hearing, where he was joined by the director of telecommunications studies at the University of Florida, Mark A. Jamison, and Eitan Hersh, associate professor at Tufts University. The second hearing is from June 19th, 2018, where Aleksandr Kogan testified before the Commerce Subcommittee on Consumer Protection together with John Battelle, co-founder, editor in chief and CEO of NewCo and Ashkan Soltani, former chief technologist in the Federal Trade Commission. Both these hearings allow for insight to how the events are conceptualised by the legislature, the expert witnesses, as well as the people who were actually involved in the activities of Cambridge Analytica: Aleksandr Kogan and Christopher Wylie. Analysing these hearings provide insight into the central questions for understanding what logic underpins the meaning embedded in the processes of the event. How the actors in the event are understood and how they understand themselves; what electoral campaigns should look like, what social media is and how it should be understood - what cyberspace is and how it should be understood - are all questions pertinent to these hearings.

5.1) Noisy silence: the lacunae of the discourse.

> Let us beware of the dangerous old conceptual fable which posited a 'pure, will-less, painless, timeless knowing subject', let us beware of the tentacles of such contradictory concepts as 'pure reason', 'absolute spirituality', 'knowledge in itself'; - for these always ask us to imagine an eye which is impossible to imagine, an eye which supposedly looks out in no particular direction, an eye which supposedly either restrains or altogether lacks the active powers of interpretation which first make seeing into something

Nietzsche (2008[1887]: Essay III, part 2)

A discourse analysis is inevitably an exercise of subjective interpretation. Its aim is to uncover and deconstruct what appears incontestable; to unknit knots of signs intersubjectively constituting meaning. This exercise involves deconstructing a networked language which the researcher herself inevitably inhabits. It is an exercise aimed at deconstructing the 'seeing' of others through the 'seeing' of the interpreter; a project that is nonetheless illuminating despite its subjectivity. Transparency in the steps taken in this subjective trek towards a fruitful reading of discourse is invaluable; and it is a principle this analysis adheres to. The question asked here is: how is the Facebook-Cambridge Analytica scandal *seen* by the actors involved? How is the event interpreted, what discursive constructions uphold the practices making the event constitute something 'out of the normal', something special subject to 'extreme' measures such as media outrage and a series of hearings and legislative propositions? Answering this requires a deconstruction of the logics underpinning the narratives of the event. However, these narratives do not only rest on the words uttered in dialogue at Senate hearings. These logics also rest on the tacit, and furthermore they rest on the silent. As a discourse analysis, this exploration acknowledges the importance of meaning carried by what is *not* being said; as an exercise it criticises the myth of inertia attributed to silence.

To understand practices, Pouliot emphasises the hidden nature of the production of meaning attributed to practices. Practitioners are seldomly aware of their own practices, and least of all what these practices mean. Practices are fundamental know-hows of behaviour. Thus, gaining knowledge of subjects' ideas of their practices' meaning is like "asking fish, if they could speak, to describe the water in which they swim. The solution is to focus less on what interviewees talk *about* than what they talk *from*." (2015: 246, emphasis in original) This does not imply an adherence to a latent structure behind language along structuralist theories of discourse analysis, as if there were a constant non-discursive structure on which all discourses supervene. (Dunn & Neumann 2016: 24; Phillips & Jorgensen 2002: 22) But, it does mean that what is not said in a discourse says as much about a discourse as what is being uttered. I have identified four crucial elements in the Facebook- Cambridge Analytica scandal that are silenced in these hearings, as well as the other hearings on social media and data privacy in the US Senate. The first is the contract between SCL Group and the U.S. State Department (as well as the British Ministry of Defence, see Medium 2017). The second is the continuing investment in psychographics by Alexandr Kogan, despite his argument on its inefficiency, in his company Philometrics (Robertson & Baker 2018). Additionally, whilst Hersh argues strongly against the efficiency of psychographics in *persuasion*, that is, the ability of targeted ads to make an individual change partisanship, a natural counterargument would be that in a country with a turnout of 58 percent in the 2016 election, *motivation* may be an adequate function of targeted advertisements to have a substantial effect on an electoral result. This point, however, is virtually left unsaid. Finally, the involvement of Cambridge Analytica in Ted Cruz's campaign in the U.S. Primaries in 2016 is left unmentioned, despite Cruz himself being present at the May hearing, where he criticises the Obama campaign's use of big data analytics in 2012 (C-Span 2018b: 01:36:40). As these four points are publicly available knowledge, it would be absurd if none of the Senators or witnesses present had any knowledge of them. A central question is therefore why they are left unsaid, and what role they play as a fundament for what is actually being said: how their latent presence forms meaning.

‘Microtargeting is not a new thing’, is the main message from the May and June hearings in the U.S. Senate on social media and data privacy. This statement, however, begs a ‘but’ and a subsequent formulation of a ‘newness’. As such, ‘new’ works as the overarching theme of the discourses on the Facebook-Cambridge Analytica scandal. As an overarching theme, it is best understood as a representation, that is an invention “based on language” which does not consist of “neutral or innocuous signifiers” but is inherently subjective and political (Dunn & Neumann 2016: 60). The representation; the *identity* articulated for the Facebook-Cambridge Analytica scandal is therefore that of being *new*, and as an identity it includes an articulation of “the reasons why policies should be enacted” and the subsequent (re)production of that identity “through these very policy discourses” (Ibid.). The Facebook-Cambridge Analytica scandal is represented as constituting something new, and it is this new which requires action to be taken against it. Despite the signifier ‘new’ being filled with different content by different actors, the alternative narrative - namely that there is nothing exceptional or new in the case – gains no preponderance. Thus, the temporary cementing of the identity of ‘new’ is “simultaneously [a] (discursive) foundation and product.” (Ibid.) The new in ‘microtargeting is not a new thing, but’ is a discursive construction of there in fact being something ‘new’ that is different from the ‘normal’ or ‘old’ practices of microtargeting, deserving of the scandal’s subsequent media outrage and in need of exceptional policies. This ‘newness’ both produces the context of the hearings – without the scandal representing something ‘new’, there would be no reason to hold the hearings – at the same time as this ‘newness’ is being reproduced by the hearings themselves.

I have identified three main articulations of the ‘new’; of the problem to be met, by the senators. Here, *articulation* should be understood in discourse theory’s sense of the word. Articulation refers to “any practice establishing a relation among elements such that their identity is modified as a result of the articulatory practice. The structured totality resulting from the articulatory practice [is what we] call discourse" (Jorgensen & Phillips 2002: 26) Alternatively, as formulated by Weldes, articulation refers to the "construction of discursive objects and relationships out of a particular society's 'cultural raw materials' and 'linguistic resources.'" (in Dunn & Neumann 2016: 50) The different articulations of what is 'new' are therefore attempts at differentiating between 'new' and 'old' using the 'cultural raw materials' of the context; of separating microtargeting from psychographics; separating current privacy issues from old privacy issues; and separating the economic power of big data from economic power in general. These articulations do not occur in a vacuum, they are not mere productions of differentiations present in these hearings. As articulations utilising the 'cultural raw materials' and discursive resources, they are also reproductions of representations already existing in society.

The three main articulations constituting the discourse in these hearings revolve around the technique of psychographics, the economic power of big data, and finally the vulnerability of the individual in the age of cyber. As such, 'new' is posited as a nodal point in the discourses produced and reproduced in these hearings. As a nodal point, it is a "privileged sign around which the other signs are ordered" as all three articulations acquire meaning from their relationship to the concept of 'new' (Phillips & Jorgensen 2002: 26). Mouffe and Laclau (Ibid.) refer to 'nodal points' as temporarily fixed moments in a discourse. I propose a modification of this conceptualisation. These hearings are characterised by a struggle to fill the signifier 'new' with meaning, rather than 'new' operating as a closed concept to which other conceptualisations must relate. The different narratives all aim to answer the question 'what is new?' There is no general agreement as to what the answer to this question is, but there is an agreement that this is the right question to ask. In that way, the 'new' in these hearings is tacit and uncontested, and it is to this measure all narratives must compare.

These articulations are supported by 'basic discourses', "that construct different others with different degrees of radical difference; articulate radically diverging forms of spatial, temporal and ethical identity; and construct competing links between identity and policy." (Dunn & Neumann 2016: 105) The three basic discourses informing the discourse are that of democracy, that of the liberal market, and that of a liberal, autonomous individual. These basic discourses inform different outcomes. ‘Democracy’ as a morally good value both informs the idea of the necessity of a transparent, open, and free Internet as a platform of democratic exchange of meanings and beliefs, as well as the idea of Facebook as an Internet behemoth threatening democratic processes through its cynical economic growth through its willingness to aid foreign intervention in elections by selling data. In addition, the idea of democracy as the morally good standard threatened by the Facebook-Cambridge Analytica scandal also produces the representation of microtargeting as an undemocratic technique. ‘Liberal market’ informs propositions of economic regulation by the state to combat monopolist tendencies in the market and encourage innovation, as well as the idea of data being a new currency; transforming the very logic of the liberal market. Finally, the notion of the liberal individual, autonomous and guided by reason, underlies both the idea of democracy and the market, where microtargeting threatens the idea of the fully informed individual arriving at autonomous decisions “through a process of rational self-deliberation, so that the individual’s chosen outcome can be justified and explained by reference to reasons which the agent has identified and endorsed” (Yeung 2017: 124) Here, it is noteworthy that as the liberal subjectivity is threatened, so is also the object of liberal governmentality. As threatened, the liberal individual is most explicitly present in the articulation of the vulnerability of the individual, but also it underlays the articulations of the liberal economic system and democracy. As basic discourses these are tacit. They posit a certain variety of democracy, economy, and subjectivity normatively and indisputably. As such, they are always in the background of the discourse’s main articulations.

The narratives articulating psychographics as a new thing build on the supposition of there being a qualitative difference between microtargeting and psychographics. Within this narrative, the manipulative nature of psychographics is conceptualised as not only different, but also morally ‘bad’, compared to microtargeting. Where microtargeting allows for the tailoring of the representation of the Internet for each individual user, psychographics aims to exploit the vulnerabilities of individuals. It is noteworthy that within this narrative, the counterargument to the efficiency of psychographics in some sense adheres to this same idea of ‘newness’. Although arguing on opposite sides as to the effect of psychographics, both the argument (psychographics is new, and it is bad) and the counterargument (pscychographics is new but it doesn't work) agree on the content of the concept 'new'.

The articulation of the economic power of big data as the new emphasise the new status of big data 'as a currency' or as 'the new oil'. In addition to the threat to governmental monopoly of currency, social media companies are viewed as threatening to the order of market capitalism. Especially Facebook's role as a monopolist within the market of social media is conceptualised as a threat to innovation in the market. In the April and September hearings in the Senate on the topic, Facebook (as well as Twitter) was largely envisioned as a democratic force, spreading liberal values to the world (C-2018a: opening speech, and 2:46:07; 2018d: 33:05; 02:44:00). Within the economic power narrative in the May and June hearings, however, Facebook is reduced from a social media platform to that of a tech company operating under the same rationale as any other big business. Additionally, what is new with the role of big data is not only the economic power in the product. On one hand, data produced cannot be called back (C-Span 2018c: 01.24:00) – there is a profound lack of physical control of 'a new currency' virtually fixed in flux. On the other, there is the distortion of the role of the individual as both consumer and producer of big data and microtargeting (ibid.: 00:36:00; C-Span 2018b: 00:33.00; 00:35:00). Combined, the whole rationale of the 'old' market is threatened by this confusing assemblage of 'new' relations of production and a 'new' nature of commodities.

The narrative articulating the vulnerability of the individual in the age of cyber as the new thing emphasises the role of consent in the collection of data. Here, the individual is framed as referent object threatened by social media and tech companies. What is new, and what makes the individual vulnerable, is the illegibility of tech companies' privacy policies, and the practice of using social media users' data for purposes the users are unknowing of. In order to mediate this threat, Congress should act to control the collection and use of big data. This conceptualisation also ties into a geopolitical narrative where the sum of individuals' vulnerability makes the state susceptible to foreign intervention in elections. Individuals as an aggregate become potential objects of foreign manipulation, and thus 'privacy risk' is a question of state security.

What is central to especially the first two conceptualisations, is the reification of the power of calculation and computation. Psychographics is a threat because its promise of manipulation; of formulating the future based on data points on individuals' psycho-social characteristics, is held to be true. As such, microtargeting threatens the very fundament of the democratic system consisting of autonomous, fully informed individuals making independent decisions. This relates to the articulation of the vulnerability of the individual as the referent object. The vulnerability of the individual, however, is not only an issue by itself. Privacy breaches are viewed as leaving the state with a huge number of individuals open to manipulation, both through psychographics and microtargeting. Additionally, the individual is viewed as *passive.* What is more, the individual is viewed as nothing but a constituent. Calculation and manipulation are things that happen *to* the individual, completely out of the constituent's control. The *active* role of individuals in the creation of cyber is absent from the discourse. The active role of individuals communicating across borders and across political opinions both online and offline is replaced by a narrative of social media as a platform inducing individuals with echo-chambers.

The narrative centred on the economic power of the economy is more explicitly related to the liberal idea of a functioning market. If liberal economy is understood along the same lines as initially proposed by Hayek (Schmidtz 2017); as the absence of government interference in the economy, the very idea of that economy is fundamentally changed if a 'new currency' is introduced. Additionally, if one adheres to Foucault's analysis of neoliberalism and the idea of every individual as *homo oeconimicus*; individual enterprises calculating the output and input of their own labour (see Foucault 2004), big data business distorts this whole process as well. The value is created by individuals producing data in an activity that cannot be conceptualised as mere work, in the market sense of the word, where this 'new oil' – data – is produced with virtually no marginal costs. In producing this value, the individual is also the consumer of social media, through which action the individual themselves is the product to be sold to external advertisers. The individual goes from producer of goods (the data) to product to be sold (data for targeted ads) to consumer (of the targeted ads) in a circle which distorts the whole rationale of liberal capitalism. Thus, in this ‘new’ economy, the whole idea of the individual as an enterprise is distorted as individuals ‘produce’ through something that is not really ‘work’ generating revenue not for the individual, but for someone else.

Additionally, all three narratives *speak from* certain implicit ideas of what the electoral process should look like; how cyber in relation to the electoral process should be; how cyber should look like for the individual; and what the economy should be like. These conceptualisations of how the world should appear are all framed as ‘old’ threatened by the ‘new’ aspect of microtargeting and big data. It is also significant that the dominating discourses, with Christopher Wylie as a noteworthy exception in the May hearing, view ‘cyber’ as something external and ‘new’ happening to the establishment on one hand or reduces ‘cyber’ by analogising tech companies and big data to companies in general on the other. From the perspective of STS, the latter point is important as the acknowledgement of cyber technologies as a political product of the very system produced and reproduced by the senators themselves is generally omitted. The senators are eager to formulate a version of microtargeting as a threat where they themselves are not included. They articulate a digital ‘new’ where the senators as distinctly analogue are unequivocally excluded.

In addition to these three narratives on the ‘new’, the “coordinated network” (C-Span 2018b: 01:05:00) of the scandal is also outlined in detail, intersecting with the aforementioned articulations of the event. Additionally, the different articulations of what constitutes the ‘new’ in the scandal are far from separate and the links between them will be explored below. As a theoretical framework, I understand these three articulations as *stories* as conceptualised by De Certeau. “[S]tories ‘go in a procession’ ahead of social practices in order to open a field for them” (in Dunn & Neumann 2016: 64) This is significant because the idea of ‘stories’ as articulated by De Certeau captures the field of possibilities arising from dominating articulations. That is, once an articulation becomes a representation; once it is incontestable and taken for granted, it enables certain discursive social practices and exclude the possibility of alternatives. Discursive power is not limited to verbal prowess. Just as discourses expand beyond words, discursive powers expand beyond text. In this regard the function of ‘new’ as nodal point in these discourses should also be understood as *interpellation*. Interpellation refers to "the processes through which these discourses create subject positions for individuals to identify with and to 'speak from'. One is interpellated or called into subject position: a subject position is specified and the subject fulfils it." (Ibid.: 50) As acts of *interpellation* the subject positions created should not only be understood in terms of positioning Facebook, Cambridge Analytica, or Alexander Nix, for that matter. As exercises of interpellation, the Senate is also called into subject position. By identifying psychographics as the 'new', the 'old' practices of microtargeting – the practices common amongst the senators themselves – are constructed as 'normal' and 'acceptable'. The 'new' in these discourses is always something 'different', and 'different' in this context has a distinct taste of 'morally bad'. When the senators identify tech companies and data brokers as threats to the market, they are at the same time articulating an 'old', or 'normal' market as functioning. From the perspective of the senators, the 'new' in these hearings is always external, rather than an inherent flaw in the system within which the Senate also partake. The 'new' in these hearings is subsequently the 'Other', and through identifying the Other the actors within these discourses are engaged in an interpellation through which themselves are identified as Self.

5.2) Microtargeting is not a new thing, but psychographics is.

Two hours into the hearing on May 16th, senator Cory Booker says

> I have a lot of concerns on how these platforms can be used to pit people against each other. One of the greatest values of America is this idea that indivisibility, that we have these lines that tie us together that are stronger than the lines that divide us as a country (…) I was just so deeply disappointed and angered when Nigel Oaks, who's the founder of the SCL Group (…) would say things in a recorded conversation where he's ehm.. it's things like this that resonates sometimes to attack the other group and know that you're going to lose them is going to reinforce and resonate with your group. Which is why Hitler attacked the Jews. Because he didn't have a problem with the Jews, at all, but people didn't like the Jews, so he just leveraged an artificial enemy. Well, that's exactly what Trump did.

> He leveraged a Muslim. Trump had the balls, and I mean really the balls, to say what people wanted to hear. This is, to me [Booker], a very frightening reality, a threat to the very idea of a nation that wasn't founded because we all pray alike, because we all looked alike, but we had a set of common aspirations and democratic principles that united this country. Our founders talked about pledging to each other, not religious alliances, not racial alliances, but our sacred honour. (C-Span 2018b: 02:04:34)

For Booker, the threat of psychographics is a threat to American values. As he is formulating a vision of this threat, he is simultaneously (re)producing the very idea of American values he considers as threatened. He mobilises an idea of American history as a history of unity despite differences; and it is this unity which forms the fundament of the American democracy. Thus, the use of psychographics, represented by Cambridge Analytica, is not only a threat to democracy, but a threat to a specific American formulation of democracy. As a discursive strategy, it is particularly efficient in that it conceptualises the threat as external, as something 'out there' and not American, threatening the 'good' and 'normal' functioning of an American democracy. This threat coming from 'out there' is not only formulated as un-American. It is also characterised by a specific tint of cynicism. Where American values are characterised by a 'sacred honour', the new format of electoral campaigns in the age of cyber are cynical and cold. It is the cynicism of calculation – be it through the cynical calculation of electoral advisors pitting groups against one another or be it algorithms performing segmenting operations – threatens the sacred honour of American society. By its very nature, microtargeting as a new form of electoral campaigns divides the country; feeds off differences and opposes different groups against one another.

This, of course, is not the only narrative that could be told about American democratic history. One could claim along the lines of Hersh, the expert witness in the May hearing, that "campaigns do things that are not nice all the time" (C-Span 2018b: 02:00:05) For Hersh, there is nothing sacred in how electoral campaigns are carried out. Political opponents will always use any tool available to win an election. Thus, for Hersh, microtargeting is just a new addition to the technological repertoire of political campaigners. It is simply a step forward of technological developments whose effect should not be exaggerated. In his opening statement, he argues:

> Every election brings exaggerated claims about the effects of the latest technologies. After an election there is always a demand for finding out why the winning campaign won, and the latest technology used by the winning campaign is often a good story line even if it's false. Campaign consultants also have a business interest in appearing to offer special skills and products, so they often embellish their role to the media. (C-Span 2018b: 00:21:49)

He is not only disputing the whole idea of microtargeting as exceptional and external, he is also disputing the effect of the technique. Later, he is asked by Senator Lee:

> The use of social media to microtarget is a fairly new practice, but it is my understanding that microtargeting itself is not. Sadly, the use of provocative information to either divide the electorate or mobilise a portion of the electorate has a long history in our country's political campaigns. Is the use of microtargeting different from how it's been done in the past?

To this, Hersh replies:

> So, there is a lot we don't know, there is a lot we don't know about its effectiveness, but it often looks the same. And in response to Senator Kennedy, just because campaigns spend a lot of money on a particular advertisement, doesn't mean that it works (Ibid.: 1:02:38)

What is noteworthy in this exchange is that Hersh does not answer the question. He is not disputing that there is something 'new' in psychographics. He just questions the efficiency of psychographics, and thus whether this 'newness' is even worth talking about. This strategy is replicated by Kogan in the June hearing (C-Span 2018c: 00:27:00), who also points out that if the availability of immense amounts of data is the threat, then Facebook is put in a much more worrisome situation than Cambridge Analytica (Ibid.: 29:00; 35:00). When it comes to Kogan, however, it is important to remember that he himself was a key actor in the Facebook-Cambridge Analytica scandal, so diminishing the significance of the incidence is also a strategy for diminishing his own possible wrongdoing.

So, neither Hersh nor Kogan dispute that psychographics is ‘new’, but they dispute the efficiency of the technique. Additionally, Hersh views electoral campaigns, and thus also the process of democracy, as notoriously cynical – quite the opposite of Booker. For Hersh, psychographics is just the continuation of the development of political advertisements, whose effect should be dedramatized. Along the same lines, but in a less optimistic fashion, Soltani argues in the June hearing that “all of this has happened before, and it will happen again” (C-Span 2018c: 00:22:25). Soltani argues that the use of misappropriated data in order to manipulate voters is an old problem but increasing. This problem is a consequence of the three elements of the role of tech-companies in the market: the logic of “growth at any cost”, that the “consumer protection framework is broken”, and that there is a “monolithic market with no real choice [for consumers]” (Ibid.: 21:05) Here, it is not the cynicism of the algorithms that is the main problem, rather, the cynicism of an unregulated market allowing for the use of microtargeting in political campaigns is the problem. Booker, Hersh, and Soltani all agree on the newness of microtargeting being that of psychographics. But whereas Booker and Soltani agree on the efficiency of psychographics to divide the electorate, Hersh disputes this. Where Booker views psychographic political adverts as distinctly ‘new’, threatening the old order of political campaigns, Soltani views psychographics as the newest development of a long emerging problem. Hersh, on the other hand, views psychographics as ‘new’, but only in terms of being the latest tool in the hands of political campaigns. In a certain sense, Hersh – as the only one in these hearings – is in some way disputing whether there even is a problem to be discussed at all. Central to these claims are also how they differ in what they consider as cynical. For Booker, it is psychographics itself that is cynicism; the power of the algorithm induces the political process with cynicism. For Soltani, the market is cynical, and for Hersh, political campaigns are, and have always been cynical. All these three narratives, however, view psychographics as something external, something occurring *to* processes already existing. Technology is apolitical rather than a creation of the society whence it emerges. What is more, technology threatens this ‘old’; society as it is and should be. Here, Christopher Wylie offers an alternative articulation:

> Cambridge Analytica is the canary in the coal mine. We must address the digital echo chambers that are being exploited to algorithmically segregate American society. Online communities should unite us, and not divide us. Data is the new electricity of our digital economy, and just like electricity, we cannot escape data. (C-Span 2018b.: 00:26:14)

Data is omnipresent, and the challenges arising from this wave of the omnipresent will engulf society unless we take steps. Furthermore, he says:

> All revolutions draw up new power structures. The American revolution required the Constitution to ensure that citizens of the young republic were protected from the excesses of arbitrary government. The industrial revolution required protections for the workers against hazardous conditions in the work place, and in the environment. So too, with the digital revolution must we realise that there is a new game being played. (Ibid.: 26:48)

Psychographics is new as the last in a series of technological revolutions. As new, these massive technological changes are dangerous and a threat to society as we know it. The solution, however, is not to go back to the 'old', but to reformulate society in order to meet the challenges of the 'new'. In that sense, his view is radically different from the interpellation performed by the senators within this discourse. The senators, as well as Hersh and Soltani, articulate psychographics as something external, and thus different from the system in which they are participants. They are interpellated into a subject position distinct from this 'new' arising. Wylie, on the other hand, views psychographics, and the Facebook-Cambridge Analytica case, as an event emerging within a society which should change with it; technology is not the Other, it is a part of the society whence Wylie speaks from. As such, the 'threat' of psychographics cannot be met by retracting to the 'old'. It must be met by a society acknowledging the integration of technology into the 'normal'; reformulating itself as it meets technological changes. The Facebook-Cambridge Analytica scandal is thus the beginning of a new form of societal organisation, which will "algorithmically segregate American society" unless something is done.

From this point of view, what is interesting in Wylie's statement is not only how revolutionising the practices of Cambridge Analytica are deemed to be. It is also noteworthy that technology is first and foremost a subjective phenomenon. Technology is inherently political and closely knit to the political progress of society; it is all-encompassing, cannot be escaped, and should not go unregulated. Furthermore, this complete integration of technology, in this case specifically big data and big data analytics, has led to a transformation tantamount to a revolution. This revolution is inevitable, and it can only be met by a society ready to meet the challenges it poses. Here, it is also noteworthy that big data is not the main problem, rather it is the function of psychographics to make big data legible in a specific, manipulative manner which is the threat, which echoes Amoore & Piotukh's work on algorithmic governance (2015). Big data is like electricity; asking whether it is 'good' or 'bad' makes no sense, as it is merely something, we all depend on. Furthermore, the Facebook-Cambridge Analytica scandal is not only important in its own role. It is a canary in the coal mine – it is a symptom and a warning of something bigger inevitably changing society as we know it. For Wylie, this can be countered by another vision of technology. As fundamentally political – "online communities should unite us, and not divide us" – technology is not bad, or cynical, per se, but unless society transforms technology and itself with it, the cynicism of algorithms will prevail. This cynicism, represented in its starkest form by Cambridge Analytica, is a new kind of cynicism distinct from the workings of other technologies of advertisements:

> Cambridge Analytica sought to identify mental vulnerabilities in voters and worked to exploit them by targeting information targeted to activate the worst characteristics in people, such as neuroticism, paranoia, and racial biases. To be clear, the work of Cambridge Analytica is not equivalent to traditional marketing. Cambridge Analytica specialised in disinformation, spreading rumours, kompromat, and propaganda. For those who claim that profiling does not work, this contradicts copious amounts of peer-reviewed literature in top scientific journals. Even Facebook applied for a patent on, quote 'determining user personality characteristics from social-networking systems.' (C-Span 2018b: 00:29:10)

Where microtargeting is a question of targeting adverts towards the individual, psychographics holds the promise of manipulation. Where microtargeting gives the user what the user wants in the form of targeted ads or newspaper articles, psychographics aims to manipulate as it seeks “to identify mental vulnerabilities in voters [in order] to exploit them.” Furthermore, along the lines of Booker:

> The United States went through a civil rights movement a couple of decades ago in order to de-segregate society. And one of the things we’re seeing now is a re-segregation of society that is catalysed by algorithms. So, some people call that ‘echo chambers.’ (C-Span 2018b: 02:06:41)

Algorithmic cynicism is even more clearly expressed in references to the actual practices of Cambridge Analytica. Quoting from Wylie’s testimony, paragraph 13, senator Lee comments on the description of the Russian project and its “particular focus on the dark triad traits of narcissism, Machiavellianism, and psychopathy.” (C-Span 2018b: 01:04:40) In relation to Project Ripon, Cambridge Analytica’s campaign platform developed by AggregateIQ (Cameron 2018), Senator Feinstein says:

> Cambridge Analytica obtained detailed personal information on approximately 87 million people from Facebook without their knowledge. The massive data set, which reportedly included approximately 4000 data points on each individual was used by Cambridge Analytica and SCL Canada to develop a comprehensive voter targeting and online behavioural influence tool called Project Ripon. Reportedly, Project Ripon was a software program that used sophisticated algorithms to allow campaigns to segment voters into groups based on psychological characteristics, such as neurotic or introverted. Once individuals were identified and grouped, the platform then provided preselected and group tested images and keywords, that were most likely to alter the behaviour of those individuals. Examples of the messages developed and used by Cambridge Analytica include keywords such as ‘drain the swamp’ and ‘deep state’, as well as images of border walls. In an undercover

> video, Cambridge Analytica managing director Mark Turnball explain that Cambridge Analytica also created the brand 'defeat crooked Hilary' (C-Span 2018b: 00:10:58)

The framing of psychographics as 'new' and 'cynical' is closely related to the general strategy prevalent among all the participants in the hearings except Kogan and Hersh, of identifying the 'new' as morally 'bad'. This arises partly from the difficulty of characterising the activities as illegal, due to the 'common' or 'old' nature of microtargeting as a technique of political advertisement. However, it is necessary for the Senators to identify themselves away from the activities of Cambridge Analytica. If not, they would themselves be subject to the same scrutiny as Cambridge Analytica has suffered after the scandal erupted in May 2018. This issue is exacerbated by the dependence on data brokers and analysts for the state's own security practices. The main strategy to avoid their own implication in the scandal is through not mentioning it. This silencing does not only relate to the use of big data in surveillance, but also regards the expressed potential efficiency in microtargeting in motivating or demotivating electoral behaviour. Here, the key problem is that if psychographics is *not* a new thing, that is, if psychographics is, despite its promises of manipulation, not more effective than microtargeting in general, then the Senators are all guilty in utilising the technique subject to the hearings. This silencing is perhaps at its loudest when the infamous use of Cambridge Analytica's services by Ted Cruz in the U.S. primaries are not mentioned, not even as he himself, present at the May hearing, comments on Obama's use of microtargeting techniques. Except from Obama, it is noteworthy that when U.S. political figures' use of psychographic techniques are mentioned, it is only in relation to political figures who are already in a bad light, morally speaking. Here, Bannon is an obvious example, and his activities in relation to the Trump campaign are identified as undertaken to "circumvent U.S. election law." (C-Span 2018b: 01.06:00, see also 00:09:45; 00:52:50). Additionally, these activities, together with those of the Mercer family are framed as "propaganda" and part of the

> Breitbart doctrine, which posits that politics is downstream from culture, so that if you want to have any lasting or enduring changes in politics you have to focus on the culture. And, when Steve Bannon uses the word 'culture war', he uses that term pointedly and they were

> seeking out companies that could build an arsenal of information weapons that could fight that war, which is why they went to a British military contractor [SCL] who specialised in information operations (C-Span 2018b: 00:56:51)

Here, the moral judgement is complimented with references to ‘weapons’, ‘war’ and ‘arsenal’, enforcing the exceptionalism of the topic at hand through analogies to conventional security threats.

The strategy for circumventing the issue of state security’s reliance on data brokers is also silence. The contractual relationship between SCL and U.S. security services is unmentioned, despite the “coordinated network” of Cambridge Analytica not only being mentioned, but also expanded on (C-Span 2018b: From 01:06:00). From SCL’s relationship to the software developer AggregateIQ (C-Span 2018b: 01:05:00), to the development of Application Programming Interfaces (API) privileging access to private data channels for providers (C-Span 2018c: 00:02:00; 00:45:00) to the alleged relationship between Cambridge Analytica and Julian Assange (C-Span 2018b: 00:15:00; 00:29:00), and subsequently Russia through relationships with Lukoil (Ibid.: 00:15:00; 00:30:00) and FSB (Ibid.: 00:46:00) and the production of “fake news” (Ibid.: 00:41:00), the relationship between SCL and Pentagon is left unmentioned. This happens despite the fact that Wylie, in the quote above (correctly) refers to SCL as a ‘military contractor’. What this entails, is left uncommented. The problem, of course, is how to frame the data collection practices of data brokers as bad, when it is the same data brokers that create the fundament for algorithms used by Western powers in their security practices. There is no easy answer to this, which perhaps is why the question is not asked.

As a discursive strategy, the lacunas of this discourse are important. Through not mentioning the role of Cambridge Analytica in the senators’ campaigns, and not mentioning the direct links between SCL and Pentagon, the senators are able to construct a representation of the Facebook-Cambridge Analytica scandal as something happening out of their control. Something they should perhaps have regulated, but still an external event characterised by cynicism threatening the democratic processes they depend on. As a strategy, this is efficient. However, there is one significant rupture to this discourse. Two hours into the May hearing, senator Hirono breaks the silence as she says to Hersh*:*

> let’s assume that we can come up with some way to define what demobilises, because that is a serious matter to your concern, you said it’s easier to affect. So that may be an area for us to pursue in terms of any kind of regulation (C-Span 2018b: 2:00:28)

Furthermore, she asks:

> Mister Wylie you obviously have an awareness of the use and misuse of massive amounts of data, so I wanna ask you this: the US Immigration and Custom Enforcement [ICE] has proposed a new extreme vetting initiative or life-cycle vetting… They’re planning to hire contractors to exploit publicly available information such as media blogs, public hearings, conferences, academic web sites, social media web sites, such as Twitter, Facebook, LinkedIn, to extract pertinent information regarding targets to determine who will be a productive member of society and who will commit crimes and terrorist acts. We’re talking about people who are applying for visas to come to our country (…) ICE’s plan would automatically fad people for deportation or visa denial based on the exact criteria for the original Muslim ban (…) Do you think that kind of prediction of human behaviour, as to whether somebody is gonna become an outstanding contributing member or whether that person is likely to become a terrorist or become a criminal, is even possible? (Ibid.: 2:01:24)

There is no follow-up from Hirono’s statement, which is followed by senator Booker’s statement quoted at the beginning of this section. However, Hirono does illustrate the uneasy ground on which the different conceptualisations of ‘microtargeting is not a new thing, but psychographics is’ rest on.

5.3) ‘It’s the age of access, rather than the age of transfer’: power and access, big data and the economy

> As a publisher myself, I became increasingly concerned that Facebook’s appropriation of public discourse would imperil the viability of independent publishers and cause the kinds of externalities with which we now struggle. Facebook employed two main strategies to grow its services in its early days. The first is the news feed which mixed personal news from friends with public stories from independent publishers. The second strategy was the Facebook platform which encouraged developers to create products and services inside Facebook’s walled garden. The potent mix of news feed, platform, and a subset of bad actors leveraging both combined delivered us the Cambridge Analytica scandal. But it is important to remember that Cambridge Analytica was a predictable outgrowth of the governance decisions taken, or not, by all parties, including government. Facebook’s business model is driven by its role as the largest data broker in the history of technology. To understand Facebook, we must understand the business model of online advertising (C-Span 2018c: 00:11:42)

This quote is from John Batelle’s opening statement at the June hearing. Here, the core of the problem is Facebook’s monolithic position within the market of publishers. Cambridge Analytica is but a product of a business model and a market with inherent flaws. The problem, therefore, is not Cambridge Analytica *per se*, as was the case in the articulation focussing on psychographics as the ‘new’ thing. The problem is social media, more specifically the data generated through social media use. The focus of the second articulation on what is ‘new’ in the Facebook-Cambridge Analytica scandal is thus centred on the economy. Within this narrative of the scandal, Facebook, and not Cambridge Analytica, is the focus. Facebook’s monopolistic position within the market is not only a problem in terms of freedom of speech, or diversity of publications. It is also a problem for the functioning of the market. Independent publishers are implicitly constructed as morally ‘better’ than the domination of the market by one company. Battelle is here constructing himself as morally superior to Facebook. The lack of governance of this market by the government has led to Cambridge Analytica. The scandal is thus inevitable given the governance structures at place, or not, for regulating Facebook. Ten minutes later, Ashkan Soltani says: "I cannot stress enough, Cambridge Analytica's access to and sale of personal information from Facebook is not new. It's a foreseeable result of a business model that essentially pays developers with access to consumer information." (Ibid.: 22:28) Further, he states: "growth at any cost is the new unsafe at any speed" (Ibid.: 26:17)

The business model of data brokers, social media, and big data has introduced the market to the new oil, or a new currency. Facebook trades with data; the emergence of Cambridge Analytica is a foreseeable consequence of the business model of online advertising. The focus here is not on microtargeting as a technique – what is new is not psychographics – what is new is big data. And this lack of government interference in the market allows actors such as Facebook to cynically grow at the cost of a functioning market and privacy of consumers. However, it is not only the position of Facebook as an "Internet behemoth" (Ibid.: 6:51) that is the problem. In addition, the role of data as a currency is qualitatively different from traditional trading. Rather than selling data, online advertising is about giving access to data; it is about trading legibility rather than data points.

One and a half hour into the June hearing, senator Tillis remarks that

> All of us in these committees have already used data from aggregators. We take the voter data, we know what voting propensities are, it's downloaded from the boards of election. You use that as a basis for targeting voters. Then there was the next wave, data aggregators so that you can overlay people's affiliations with association, the magazine prescriptions. That has all really become passé, in terms of data matching it has been happening for probably ten or twenty years in our campaigns. Now, that is where they buy data and aggregate it and then they build their proprietary platforms around it. Now, with the advent of social media, we have entities who have come into play that really don't want to sell their data, they want

> to sell the analytic result of that data so that they can target people on certain social media platforms.

To this, Wylie responds: “It’s the age of access, rather than the age of transfer (…) Data is the new oil” (C-Span 2018b: 01:24:07).

This does not only mean that the role of data brokers is not translatable to the role of banks in the sense that they trade currency. It also means that data brokers have the role of gatekeepers of information. It is this new power of big data business which is the ‘new’ in ‘microtargeting is not a new thing.’ This problem is not an external problem threatening a functioning market, rather it is an inherent element of the business model of online advertising. This is not primarily viewed as a problem for social media users’ privacy. It is primarily a problem for the functioning of the liberal market; it leads to Facebook obtaining a monopolist position within the market of social media. In this view, Facebook is reduced to the role of a business, rather than a social media platform or publisher driven by other motives than that of economic growth. This contrasts the view on Facebook pertinent to the April and September hearings on social media and privacy. In the Senate hearing on September 5th, Facebook COO Cheryl Sandberg says:

> Social media enables people to celebrate their birthdays (…) And small businesses [to] grow. All around the country I meet with small businesses from a woman making dresses in her living room and selling them on Instagram, to a local plumber who are able to find their customers on Facebook and able to grow and hire people and live their American dream. (C-Span 2018d: 00:33:05)

Additionally, throughout the September hearing, Twitter is referred to as a “digital town square” (e.g. C-Span 2018d: 00:27:20; 00:34:25; 01:14:45; 01:52:55) insinuating that social media is more than a platform; it is a democratic force spreading liberal values. From this point of view, Facebook (and Twitter) cannot be reduced to mere businesses. The nature of social media is viewed as inherently democratic, as a force bringing people together. This view is virtually absent from both the May and the June hearing on the topic. In June, Senator Blumenthal refers to the “two Facebooks”, where one is

> the ideological technology company, driven by altruistic purpose to connect people with people they love, voices that need to be heard,

> communities that can be built. The other Facebook is an Internet behemoth that is one of the most powerful social and political tools in history building pervasive data collections. (C-Span 2018c: 00:06:51)

It is the second of these "two Facebooks" which is the dominant representation of the firm in this discourse. This articulation therefore has two sides. On one there is the 'new' role of big data within the market. On the other is the role of Facebook as a monopolistic company. The first relates to the 'new' of big data; the second recognises an 'old' problem.

Facebook as a monopoly is viewed as a threat to innovation, above else. This is the least prevalent formulation of the 'new' in the case in terms of the economy. Here, the role of government is to regulate the market so that innovation can be fostered. In the opening speech of the Hearing on May 16th, Senator Grassley identifies one of the main purposes for the hearing to be "what role Congress should play in promoting transparency for consumers regarding data collection and use while ensuring a well-functioning market place for our data dependent technologies to drive further innovation" (C-Span 2018b: 00:02:38) The subject of innovation is also tied to the question of data protection regulation, where references to Europe's General Data Protection Regulation (GDPR) is brought up several times. As Senator Blumenthal argues in favour of a "privacy bill of rights." (C-Span 2018c: 00:10:17) This is criticised by Battelle:

> I am actually a fan of the intent of GDPR, I am not a fan of what happened after it was implemented which is that all the large firms which had the lawyers, the staff, the resources and the ability to bring compliance between you and the next picture of a baby, hey by the way do you agree to this? And you hit OK to get rid of it so, you know, you can see the neighbour's baby photos. Whereas very small companies do not have the ability to do that kind of compliance. (C-Span 2018c: 01:09:19)

Here, Battelle does not speak from a different logic than Blumenthal does; they both agree on the necessity of data protection, as well as the detrimental effects of a monopolist market structure. They both agree on what the market *should* look like, and how this vision is threatened by the existence of oligarchs like Facebook. This is not a point of contention within the hearings. What is given more attention in terms of the threat of Facebook and social media, however, is the role of data as a new currency.

If data is the new currency, it is in Facebook's interest that its users spend as much time on the platform as possible in order to generate this currency. This is formulated as the inherent logic – or in this case the inherent flaw – in Facebook as a business model. In the June hearing, Kogan says:

> I think it's pretty clear is in a business of trying to keep you on Facebook as long as possible, because then they can serve you more ads. This is interesting in terms of the contrast to Google, where they want you off as quickly as possible. That's their success rate, because you've found the information you want. (C-Span 2018c: 00:49:55)

In terms of the role of hate speech, or controversial posts on Facebook, Kogan's statement is followed up with observations made by senator Harris in the hearing on September 5th on the same topic:

> So, a concern that many have is how you can reconcile an incentive to create and increase your user engagement when the content that generates a lot of engagement is often inflammatory and hateful. So, for example, Lisa-Marie Neudent, a researcher at Oxford Internet Institute she says, quote: 'The content that is the most misleading or conspiratorial, that's what's generating the most discussion and the most engagement. And that's what the algorithm is designed to respond to. (C-Span 2018d: 01:33:30)

In these narratives, there is something fishy about the business model of social media. There are some fundamental problems with the way data is the new currency. It is a new currency produced by individuals who believe they are the customers of social media services, but in fact are the products to be sold on the online market of advertisement. As exclaimed by Blumenthal: "We are the currency" (C-Span 2018c: 00:37:15) The problem, therefore, is not simply one of regulation, it is a problem necessitating a complete transformation of how the market of social media is to be. It requires a rethinking, a revisualisation, of how the Internet should be structured as its flaws are not external events threatening a stable and functioning world wide web. The flaws are inherent in how data is made; how money is made, online.

5.4) The problem of consent, and the vulnerability of the individual

The third narrative defining what is 'new' in the Facebook-Cambridge Analytica scandal is centred on the vulnerability of the individual in the age of cyber. Central to this narrative is the liberal ideal of the autonomous individual, that is "mentally competent, fully informed [whose decisions are] arrived at through a process of rational self-deliberation, so that the individual's chosen outcome can be justified and explained by reference to reasons which the agent has identified and endorsed." (Yeung 2017: 124) This ideal is also intertwined and fundamental to the narratives elaborated on above but is most clearly present in the narrative centred on the vulnerability of the individual, threatened by microtargeting. Microtargeting has the potential of manipulation, distorting the liberal subjectivity. In these discourses, this narrative builds on a diversity of discursive logics. One logic focuses on the importance of liberal freedoms. Here, privacy itself is viewed as a liberal freedom to be protected. Another logic is centred on geopolitics. Here, the vulnerability of individuals makes them susceptible to geopolitical meddling. This logic incorporates the links between Kogan and Russia through his teaching position at St Petersburg University (C-Span 2018b: 00:16:00; 00:44:00), Cambridge Analytica's contact with Lukoil and FSB (Ibid.: 00:45:00; 00:15:00; 00:30:00; 00:25:00; 00:41:00), how certain data collected by Cambridge Analytica ended up in Russia (Ibid.: 00:44:00) as well as the impact of Cambridge Analytica in a global context. The third logic is centred on consent. This is interlinked with both the geopolitical and the liberal values rationales. However, it is interesting in its own right as it posits consent as a central right for individuals. Still, it is also a concept centred in a struggle to define what consent really is. Blumenthal proffers an American version of GDPR as the solution (C-Span 2018c: 00:10:17), whereas Wylie argues that there is no real consent in the context of social media as there is no real alternative. Within this complex landscape of trying to fit analogue values into the digital domain, the actors in these hearings seem to struggle to envision what consent even means in the context of cyber.

When the vulnerability of the individual is conceptualised in relation to the idea of liberal freedoms, this vulnerability is itself the referent object. Here, consent is closely related to ideas of democracy and privacy rights. The Facebook-Cambridge Analytica scandal is thus seen as primarily a problem for the individuals whose data had been scraped without their knowledge or consent. This ties into the discussion on a privacy bill of rights and GDPR as discussed under the section on the economy above. Here, the main purpose of the government is to protect the individual from actors trying to exploit their data. Additionally, this resonates with Kogan's testimony in which he argues that he had misunderstood how individuals would react to the appropriation of personal data, and that this had led him to believe that GSR and Cambridge Analytica's data collection had been fine. Sixteen minutes into the June hearing, Kogan says

> As I've watched what has unfolded, I have naturally taken a hard look in the mirror on my own role in the controversy. What is clear to me now is that I made a mistake in not appreciating how people would feel about us using their data, and for that, I'm deeply sorry. (C-Span 2018c: 00:16:41)

When the vulnerability of the individual in the scandal, in terms of liberal freedoms, is mobilised the language used is highly emotional. It resonates with feelings of surveillance and discomfort in the light of large companies using individuals' data without their knowledge. There is an underlying idea of data on online behaviour being personal and thus analogous to personal data in offline, or 'real', life. This view is perhaps strongest expressed by senator Harris in the May hearing*:*

> (…) there are broader issues, of privacy, that are highlighted by this incidence, and I think it's worth to step back and pull all this in context for the American public. To put it plainly, most Americans have entered into a bargain with Facebook and other web service providers in which users unknowingly give these companies huge amounts of personal data in exchange for the free service of social networking (…) Let me put this in perspective. In the real world, this would be like someone following you every single day as you walked down the

> street watching what you do, where you go, for how long and with whom you're with. For most people, it would feel like an invasion of privacy. (C-Span 2018b: 01:47:33)

For Harris, the invasion of privacy is the referent object, and it is threatened not by the specific workings of the Facebook-Cambridge Analytica scandal. Rather, they are consequential to the business model of social media and big data. This echoes DeNardis, referred to in chapter 2.2, of the basic logic of the liberal Internet being characterised by the "digital shadow of trading privacy for free private goods." (2015: 16)

The vulnerability of the individual is also very much present within the geopolitical narrative on the scandal. Here, it is noteworthy that the individual itself is not the referent object. That is, the individual should not be protected primarily because of privacy being a basic right. Rather, the lack of protection of individuals' privacy leaves the state susceptible to foreign intervention. The freedom inherent in the workings of a liberal system, where companies such as Facebook establish their own business model based on selling data in exchange for providing a free service for its users becomes a problem. This problem is complicated, as it is the very liberal democratic system that is threatened because of the weaknesses within that system. That system produced Facebook, which inevitably led to the Facebook-Cambridge Analytica scandal, which led to foreign countries, mostly Russia, being able to misuse that data to attack the liberal democracy itself through intervening in the election. Within this narrative, the "coordinated network" (C-Span 2018b: 01:06:00) of Cambridge Analytica is often referred to. From this perspective, the "privacy risk" inherent in the scandal (C-Span 2018c: 00:10:01) is viewed in relation to the importance of "alerting the American public to (…) those threats and challenges to their privacy, as well as the potential threats to our national security from Russian interference in our elections" (C-Span 2018c.: 00:10:28) Compared to the narrative positing the vulnerable individual itself as referent object because of infringements of liberal freedoms, this narrative is characterised by a less emotional reasoning. It is most of all present in the May hearing, in dialogues characterised by senators trying to untangle the network of actors involved in the scandal. Wylie is asked by Senator Whitehouse: "You've said that Cambridge Analytica and the SCL Group are effectively the same thing and that Cambridge Analytica was the front-facing company for SCL's American operations. Is that correct?" Wylie affirms. Whitehouse continues: "What is SCL Elections?" Wylie:

> So, there is a group company in the UK, or was, called SCL Group which had several different divisions. The largest division, when I first joined was Defence, so SCL Defence. SCL Elections was one of the other divisions, SCL Commercial et cetera. They all handled different markets for the company. So SCL Elections handled political...

Whitehouse: "What are SCL Canada and AggregateIQ?" Wylie: "Those were subcontractors that were set up during the time that I was there to build out a software infrastructure, they played a very significant role in building the actual infrastructure of Ripon" (C-Span 2018b: 01:04:28) Further, Wylie is asked: "What is Global Science Research?" Wylie responds: "Global Science Research was the company that was set up by doctor Kogan" Whitehouse: "And you've said it became a company simply to serve Cambridge Analytica, is that correct?" Wylie: "It became a company so that it could sign a contract with Cambridge Analytica, or rather, technically SCL" Whitehouse: "Is it fair of me to describe all the entities I have now described as a coordinated network?" Wylie: "Yes" Whitehouse: "And, what was the role of Robert Mercer in funding that coordinated network?" Wylie: "he was the primary funder who put in tens of millions of U.S. dollars into Cambridge Analytica which then distributed that money to that network." Whitehouse: "Did that Cambridge Analytica Network, including SCL, have a recurring contacting relationship with Black Cube?" Wylie: "ehm, when I was there, we did not have a contract with Black Cube" Whitehouse: "Have you since become aware of connections between SCL Group and Black Cube, have they been working together on projects?" Wylie: "I've become aware of relationships that the company had with former members of Israeli security services." (C-Span 2018b: 01:05:55) When it comes to a potential Russian involvement, Senator Feinstein asks about the harvested data on Americans ending up in Russia. To this, Wylie responds

> What I can say is that the lead researcher, doctor Kogan, who was managing the Facebook harvesting project for Cambridge Analytica was at the time working on projects that related to psychological

> profiling in Russia with a Russian team as that was going on. I also know that he was traveling to Russia. I also know based on conversations I was having with him at the time that he was making it known to colleagues of his about the project. So I can’t say definitively if these data sets did end up in Russia, but what I can say is that it would have been very easy to facilitate that. (C-Span 2018b: 00:44:12)

What permeates this narrative is the fear of where the data has ended up, and to what use. Here, it is noteworthy that compared to the April and the September hearings on the topic (e.g. C-Span 2018a: 02:54:49), Facebook is not primarily viewed as an American company characterised by its American values. Rather, the narrative of what Facebook *is,* is largely framed on the role of data brokers mobilised by the discourse centred on the economy. Facebook is a company which will grow at any cost, even when that potentially means trading data with foreign adversaries that can use that data to threaten American democratic processes. Thus, consent and subsequently privacy should be regulated not only to ensure competition on the market, but to protect the U.S. from geopolitical rivalries.

The logic of consent in formulating the vulnerability of the individual as the referent object is interesting as the articulation of what consent even means is unclear. On one hand, a ‘privacy bill of rights’ modelled after GDPR (C-Span 2018c: 00:10:22) is viewed as able to ensure that users can consent to their data being collected. On the other, however, consent is viewed as a measure difficult to live up to because of the all-encompassing nature of the Internet. Wylie points out that

> social media is not really a choice for most people. The Internet is not really a choice for most people. It is very difficult to be a functioning member of the work force or society and refuse to use the Internet. I don’t really know any job that would let you go in and not use Google, for instance (C-Span 2018b: 01:13:27)

In June, Soltani points out that the idea of consent should be modelled after the premise that “consumers must have the possibility to enact meaningful choice” (C-Span

2018c: 00:54:00) Like Wylie, he emphasises that if there is no alternative to the way social media works, consent is by definition absent. There is no consent if there is no real alternative but to accept the data practices of social media companies. Wylie states that "Online platforms' terms and conditions present users with a false choice, because using the internet is no longer a choice. Americans cannot opt out of the twenty-first century." (C-Span 2018b: 00:26:36) The absence of any real consent on the Internet is viewed as an inherent feature of how the Internet functions within the problematic structure of the market outlined above. Here again, the threat is not external. The threat is internal to the system and a symptom of an unregulated market. In June Soltani touches this problem as he says

> I think focussing too much on notice and just giving consumers choice, it's kind of like food safety, right, so we can give people choices, but food can't contain arsenic, right (…) we can give people choices but there needs to be some baseline protections (C-Span 2018c: 00:52:21)

What is noteworthy here is that the problem is not Cambridge Analytica, it is data brokers and analysts in general. Within this line of reasoning, Facebook is an oft-mentioned theme as well. Regarding the practice of Facebook to divide its users into specific cohorts used for the targeting of advertisement, consent is coupled with the lack of transparency in data collection practices, as well as the absence of the possibility of enacting meaningful choice by users. Fischer asks*:*

> Can a Facebook user right now view how they're targeted with the ad targeting, with the predictive analysis, can they see that, can I see how viewed, what cohort I'm put in can I change that? Can I determine what cohort I wanna be in?

To which Battelle replies: "Not exactly, no." (C-Span 2018c: 00:39:13)

To sum up, there are three main articulations of the Facebook-Cambridge Analytica scandal. One is centred on psychographics, holding that psychographics is a new technique, characterised by its cynicism. Here, Cambridge Analytica is the focus, rather than data brokers and social media in general. Although Hersh and Kogan dispute the efficiency of psychographics as a technique of manipulation, this rupture to the narrative on the detrimental effects of psychographics as a marketing tool gains little preponderance. Secondly, there is the articulation of the economic power of big data as a new thing. Here, Cambridge Analytica is not the main focus. Rather, Facebook, as well as data brokers and analysts in general, are viewed as a problem. Here, the position of Facebook as a monopolist is one side of the problem, whilst the power of big data as a new currency is the other. Finally, the vulnerability of the individual is a third articulation. The focus of the next chapter is that of governmentality. Here, not only the technique and governmentality will be the focus. What is crucial is also to understand the object of governmentality. Therefore, the threat to liberal subjectivity in the age of algorithms and big data is a central argument, and it is the intertangled uneasiness of the object and the technique of governmentality that will be deconstructed in chapter six, before leading the discussion on to the international level of analysis.

6) Discussion: The threat to governmentality in cyber-age.

> "Before anybody can be disciplined and punished they need to identified and sorted"
>
> Ansorge (2016: 1)

One cannot understand governmentality without understanding the subject. As Ansorge points out:

> In a rich intellectual history, the sovereign's information needs produced copious instrumental models and techniques to better understand and act on the social and political order. While the functional categories, systems, processes, organising principles, and regulative ideals of these identifying and sorting practices changed historically, their underlying animating inquiry always remained the same: Who the hell are all these people? (Ibid.: 2-3)

To answer the question what governmentality is in the age of cyber, one must also understand what the subject – all these people – are in the age of cyber. More specifically, one must understand how the sovereign sees the people, how the populace is identified, categorised, and taxonomized. Governmentality is the conduct of conduct, it thus presupposes that one knows what conduct to be conducted; before anybody can be disciplined and punished, they need to read. Foucault points out that statistics originally meant "science of the state" and is a technique developed in search of an art of government in "efforts to rationalize the exercise of power, precisely in terms of the knowledge acquired through statistics." (1991: 101) Statistics then, as an "apparatus of knowledge" (Ibid.: 275), is a form of reading. What is more, it is also a form of "making up people"; of creating the very subjects to be governed (Hacking 1986). It is the collection of data on the populace making it subjectable to strategies of government, allowing the creation of an ensemble of humans over which biopower – the government of man as species – can be exerted. What then, are we to make of big data as the new statistics? This thesis does not argue that big data has, or necessarily will, replace statistics. It does, however, hold that big data is an additional tool analogous to statistics in the hands of the state. The question, therefore, is what does governmentality look like in the age of big data and computation: what happens to governmentality in cyberspace? This thesis argues that calculation is key in answering this. The quote by Amoore & Piotukh at the beginning of chapter 2.1 in this thesis states that "[c]alculation starts by establishing distinctions between things or states of the world, and by imagining and estimating courses of action associated with things or with those states as well as their consequences." (2016: 20) Calculation then, is about legibility. From a Cartesian perspective it can be viewed as part of what Edmund Husserl referred to as a movement directed towards "a systematic universe of 'logical laws,' the theoretical totality of the truths destined to function as norms for all judgments which shall be capable of being objectively true" to which "also arithmetic, all of pure analytic mathematics" belong. (Husserl 1970[1936]: 13) Thus, calculation forms part of the "arithmetisation of reality." (Ansorge 2016: 93) Calculation, then, as described by Amoore and Piotukh as being more than just counting, is also an attempt to arrive at the objective and *a priori;* universal and transcendental. In cyber-world, this calculation is supplemented with vast amounts of big data in an age of computation where the mathematical exercises are performed by algorithms, constantly evolving through the process of machine learning. What is more, these mathematical operations go beyond mathematics through the acknowledgment of the limitations of "formal languages, such as mathematics and explicit equations, [as they] do not deal well with complexity." (Hayles 2014: 200) Calculation then, especially in the age of cyber, goes beyond counting.

The previous chapter demonstrated how the Facebook-Cambridge Analytica scandal is primarily understood as constituting something 'new' in the way electoral campaigns and advertisement work. This 'newness' is viewed both in terms of the specific technique of microtargeting, as well as the economic power of big data in reshaping the economy and subsequently how a liberal society works. These ideas of the 'newness' of the Facebook-Cambridge Analytica scandal build on certain assumption as to what the economy should look like, what electoral processes should look like, and what the subject in a liberal state should be. Although these three basic discourses are intertwined, the starting point and focus of this chapter is on the latter. Here, microtargeting and the Facebook-Cambridge Analytica case will be conceptualised within the rationale and technique of government.

In order to deconstruct this web of epistemological changes produced and reproduced in the context of microtargeting, this chapter starts out with an analysis of statistics in the age of big data. Following this, the subject of governmentality will be conceptualised, where the intertangled nature of online and offline categories of life; of human and machine will be viewed in terms of Katherine Hayles work on cognitive assemblages. Cognitive assemblages are useful as theoretical framework due to their focus on cognition, rather than conscious and non-conscious thinking. Thus, the autonomous character of automated thought is allotted a place within the conceptualisation of thinking. Here, the blurriness of the line between human and machine will be analysed as a threat to the autonomous liberal subject. Questions to be answered are what to make of algorithms as non-conscious cognition in general, and in microtargeting in particular; how do we best understand the challenges to liberal subjectivity posed by the algorithmic 'nudge' pertinent to microtargeting techniques? Thus, this analysis will encompass the microlevel of the algorithm, and how the algorithm relates to the human and its environment. After having deconstructed the intertangled nature of human and algorithm, the analysis will return to the macrolevel of governmentality; discussing what to make of liberal subjectivity in the age of cyber, and what to make of governmentality in relation to that.

6.1) Statistics (and data) as security dispositif

> [T]he generalization of the economic form of the market beyond monetary exchanges functions in American neo-liberalism as a principle of intelligibility and a principle of decipherment of social relationships and individual behaviour (…) thanks to this analytical schema or grid of intelligibility, it will be possible to reveal in non-economic processes, relations, and behaviour a number of intelligible relations which otherwise would not have appeared as such – a sort of economic analysis of the non-economic.
>
> Foucault (2004: 243)

Ansorge (2016) states that the sovereign hungers for data. The sovereign needs information, and this data needs to be legible in order to produce knowledge. As pointed out by Ian Hacking: “Counting is hungry for categories” (1986: 280) The technique of legibility is not static but evolves and changes over time. Statistics is a form of legibility. In the quote above, Foucault conceptualises the logic of *counting* phenomena as part of the expansion of the economic logic into non-economic realms of society; as an expansion of a liberal economic logic. The economic logic then, is a form of data collection and legibility of non-economic realms of society. Thus, if we are to follow Harvey’s (2005; 2007) line of thought, this “economic analysis of the non-economic” is a form of expansion of a governmentality centred on a capitalist logic despite the same ideology’s shrinkage of the state: we are only free insofar as we can choose between certain options liberalism presents us with, in a context characterised “by efforts to foster unconstrained competition between self-interested individuals” (Curran & Hill 2017: 412) Economic rationality is closely related to mathematics; it defines rationality in terms of an arithmetic calculation between scarce means, costs and benefits. For Foucault, this rationality of government, the emergence of *raison d’État* can be traced back to the seventeenth century’s mercantilism, “understood not as a theory or representation of the State, but as art of government, as rationality elaborating the very practice of government” (2012: 12) This rationality is inextricably linked to the project of Enlightenment, and in its adherence to principles of rationality lies also an implicit compliance to the idea of calculation. The idea of calculation is perhaps even more present in Foucault’s elaboration on liberalism following the claim that

> there cannot be any government without those who govern indexing their actions, choices, and decisions to a whole set of bodies of knowledge, of rationally founded principles, or exact knowledge, which do not arise simply from the prince’s wisdom in general or from reason tout court, but from a rational structure specific to a domain of possible objects, which is that of the State (Ibid.: 13)

This idea of calculation lays not only in what the liberal government actually does, it lays also in what the government do not do, what it stays out from, namely the economy.

For Foucault, the expansion of the economic logic is not frictionless. Liberalism invented civil society as we know it, but civil society is characterised by the internal conflict between "interests" and "disinterested interests". That is, by the conflict between economic interests and "disinterested interests which [are] much wider than egoism itself" (Foucault 2004: 301) Despite this, "civil society is not a primary and immediate reality; it is something which forms part of modern governmental technology (…) a technology of government whose objective is its own self-limitation insofar as it is pegged to the specificity of economic processes" (Ibid.: 297) As such, civil society in liberalism is at once a production of liberalism itself, functioning as a technology of government; expanding the economic rationale. At the same time, civil society is characterised by an internal opposition between economic interests (egoistic) and disinterested interests (wider than egoism itself). But, disinterested interests,

> the collective good must not be an objective. It must not be an objective because it cannot be calculated, at least, not within an economic strategy. Here we are at the heart of a principle of invisibility. In other words, what is usually stressed in Smith's famous theory of the invisible hand is, if you like, the "hand", that is to say, the existence of something like providence which would tie together all the dispersed threads. But I think the other element, invisibility, is at least as important (Foucault 2004: 279)

What cannot be calculated, governmentality will always attempt to render invisible. Within this, lays not only the objective of governmentality as the calculability of society, but also the acknowledgement that calculation is never complete. However, the vision of the perfectly calculable individual, prevails. Foucault identifies the liberal conceptualisation of the subject as "the worker himself appears as a sort of enterprise for himself" (2004: 225) This conceptualisation is not only relevant in that it eradicates any non-quantifiable element of the human subject, it is also relevant as subsequently,

> the basic element to be deciphered by economic analysis is not so much the individual, or processes and mechanisms, but enterprises. An economy made up of enterprise-units, a society made up of enterprise-units, is at once the principle of decipherment linked to

> liberalism and its programming for the rationalization of a society and an economy (Ibid.)

It is clear, that for Foucault, liberalism reeks of individualism and calculation. Faced with a society consisting of individual enterprises, a liberal “analysis must try to bring to light the calculation” inherent in the individual’s choice – “the internal rationality, the strategic programming of individuals’ activity.” (Ibid.: 223) This entails the obliteration of any analysis of society and history where mechanisms and processes are the focus. Action is reduced to ‘programming’; programming that is equal to the economic rationale, reducible to the calculation of market value. As such, it bears clear resemblance to ‘code fetishization’ as described by Matzner (2019), where the cybernetic logic invites us to view the source code as the epitome of programmed intellect. As if processes and algorithmic performativity could be reduced to the initial formulation of the programmer.

In liberalism, it is the rationality of the individual, autonomous from historical processes or overarching structures which is the focus of analysis. As such, one can argue that the individual is granted an excess of agency; an excess of free will guided by rationality. This is the liberal subject. This rationality is a fundamentally economic one, where reason operates as it measures costs and benefits. Raising a child, for instance, should be understood from the perspective of calculation, as an “investment in human capital” (Ibid.: 230) A parent invests in a child, giving care and a safe upbringing to their children so that the child may grow to become a fruitful member of society. Everything is quantifiable: care, love, safety, are all investments into this curious measure of human capital. So, for Foucault, liberalism, and specifically neo-liberalism, is about making ‘all these people’ – both their actions and their identity, in fact their actions can be reduced to their identity - legible, and the language used to provide that legibility is that of the economy. For Foucault, this means the invention of *homo oeconomicus*, an invention which, just as the perfectly computational individual, is imperfect and unfulfilled despite its resilience. This is relevant for liberal governmentality, because “*homo oeconomicus* is eminently governable.” (Ibid.: 270)

The idea of calculation, which is perhaps what James Bridle would refer to as computational thinking, expanded into the non-economic realms of society, is exacerbated by big data. To illustrate this, it is useful to start out with the role of statistics; the science of the state. In his *Security, Territory, Population* lectures, Foucault says:

> [T]he sovereign's necessary knowledge (savoir) will be a knowledge (connaissance) of things rather than knowledge of the law, and this knowledge of the things that comprise the very reality of the state is precisely what at the time was called 'statistics.' Etymologically, statistics is knowledge of the state, of the forces and resources that characterize a state at a given moment. For example: knowledge of the population, the measure of its quantity, mortality, natality; reckoning of the different categories of individuals in a state and of their wealth; assessment of the potential wealth available to the state, mines and forests, etcetera; assessment of the wealth in circulation, of the balance of trade, and measure of the effects of taxes and duties, all this data, and more besides, now constitute the essential content of the sovereign's knowledge. So, it is no longer the corpus of laws or skill in applying them when necessary, but a set of technical knowledges that describes the reality of the state itself. (1991: 274)

Statistics is about producing the truth of the state itself, of a *raison d'État,* as the production of truth inherent to any art of government seizes to be centred on the law but is moved towards the population, governing it as man-as-species.

Big data is not a mere amplification of the legibility provided by statistics. There are fundamental differences between big data and statistical data, which have implications for big data and big data analytics' role in governmental practices. Sinan Aral states that

> Big Data reframes key questions about the constitution of knowledge, the processes of research, how we should engage with information, and the nature and the categorization of reality (…) Big Data stakes out new terrains of objects, methods of knowing, and definitions of social life. (in Kitchin 2014: 1)

These epistemological changes are present not only in statistics, but also in the quantitative sciences that rely heavily on statistical conventions. The ideal process of producing scientific knowledge, through an experimental, controlled environment from which data is collected before subjected to certain statistical criteria (see Hellevik 2011) is threatened by the emergence of big data. In addition to its volume, big data is high in velocity, meaning that its collection happens close to real time. Where surveys, for instance, gather data over years, or even longer, big data is available from the second you 'like' something on Facebook. Related to its velocity, big data is also diverse in variety, as it is "structured, semi-structured and unstructured in nature." Furthermore, big data is exhaustive in scope as it strives for the sample to equal the population, and "fine-grained in *resolution* and uniquely *indexical* in identification." Finally, it is relational in nature "containing common fields that enable the conjoining of different data sets" as well as "[f]*lexible*, holding the traits of *extensionality* (can add new fields easily) and *scaleability* (can expand in size rapidly)" (Kitchin 2015: 471, emphasis in original) Thus, Kitchin expands on the '4Vs' of 'big data' commonly used to identify the phenomenon: increased volume, variety, velocity, and veracity of data elements. (Amoore & Piotukh 2016: 17)

Where established statistics conform to a series of conventions, as well as limitations, big data offers a new entrance point to understanding the social (as well as the natural-scientific). Where statistics is limited by everything from survey-fatigue in populations to financial limitations, big data is data produced without the "sample" even knowing they participate. Their behaviour is tracked in real time, analysed not according to pre-established categories but through algorithmic searches for patterns pertaining the promise of perfect objectivity. Where a survey studying lifestyles in a sample over years is stuck with the same questions every time the entities comprising the sample are questioned, big data is fine-grained data that is produced dynamically as the research objects evolve. Perhaps not coincidentally, Kitchin acknowledges that big data is not entirely new to the age of cyber. He traces big data as a phenomenon back to weather forecasts parallel to Bridle's genealogical account of computation starting from Lewis Fry Richardson's meteorological ambitions in the early 1900s. Somehow, big data can be traced back to the development of what Bridle refers to as computational thought. Computation and big data are entangled concepts; it is through big data the subject can be objectively read, predicted, and manipulated.

Big data does not only pertain the promise of providing data on ‘everything’, it also offers the analytical tools to make that data legible without any prior categories or preconditions. What is more, a “key contribution of Big Data is the ability to find useful correlations within data sets *not capable of analysis by ordinary human assessment”* (Yeung 2016: 119, emphasis in original) To illustrate this, Kitchin refers to the data mining and visualisation software Ayasdi, which proclaims to “automatically discover insights – regardless of complexity – without asking questions. Ayasdi’s customers can finally learn the answers to questions that they didn’t know to ask in the first place.” (2014: 4) Of course, there is nothing unique about Ayasdi. Along similar lines, the data mining company KNIME claims to be “designed for discovering the potential hidden in data, mining for fresh insights, or predicting new futures” (KNIME 2019) and Salesforce Analytics Cloud promotes its ability to help you “discover the story your data has to tell” (Salesforce 2019) The key being that it is the data that speaks, rather than previously formulated hypotheses. This is symptomatic of data-driven sciences which “hold the tenets of the scientific method but is more open to using a hybrid combination of abductive, inductive and deductive approaches to advance the understanding of a phenomenon” (Kitchin 2014: 5). Some have claimed that big data is the ‘death of theory’ (see Kitchin 2014; 2015; 2017) – data speaks for itself, there is no need for a readily formulated theory on how things are related to other things – the correlation is formulated by algorithms finding patterns in massive amounts of data.

This, however, rests on an idea of the data being complete, and the algorithms being objective and thus able to uncover an absolute truth hidden in all these data points. That is not necessarily the case. Just as all data sets are subjected to errors both in terms of reliability and internal validity, big data can never flawlessly capture the reality it aims to describe. There are systematic measurement errors in data collected through social media, for instance: what is shared on social media, who has access to social media, and how do people present themselves on social media compared to offline life? Psychographics, as promised by Cambridge Analytica aims to capture psychological traits in individuals despite these measurement errors; the attempt is to capture something hidden in the individual, which may even be hidden for the individual itself. Although illuminous, Kitchin (2014; 2015) does not adherently capture this element in big data. Big data analytics do not necessarily only aim to capture the links between data points, as if each data point was an individual existing in a vacuum. In some ways, big data also attempts to disclose hidden patterns in behaviour, disclose underlying structures. Big data does not only go from the inductive to the deductive, but also to the abductive. Somehow, big data goes beyond the liberal analysis of society in that it aims to capture underlying structures, processes, or mechanisms, rather than to simply depict a world inhabited by individual enterprises. In that way, the Facebook-Cambridge Analytica case attempts to say something about the subject that the subject itself does not know; "pray on vulnerabilities" as Wylie put it, that the individual does not necessarily know it has.

Another important point in Kitchin's (2014; 2015; 2017) analysis, which distinguishes big data from statistics, is the focus on outliers in the statistical model. Where 'conventional statistics', in lack of a better term, hold that outliers in a statistical model may be caused by variables the model has not necessarily taken account of, or from measurement errors in the collection of data, big data analytics view the outlier as constituting an anomaly in the data set. To put this in perspective: if one aims to study the effect of the level of education on life expectancy, some data points – some individuals, will not be predicted well by the statistical model describing this correlation. This can of course be the result of some individuals acting out of the normal, but it can just as well be the result of the collection of data being inadequate, or that certain control-variables that should be included in the model are not included. Nonetheless, the focus of the statistical analysis is not necessarily on these outliers, the focus will be on the general trend (Aradau & Blanke 2017). Despite these outliers, therefore, the model will be considered 'true' in the scientific sense – namely that its probability of being true extends what is usually put to 95% probability (Christophersen 2018). The statistical model never expects to get everything right. In big data analytics however, which is perhaps most clearly illustrated in state surveillance (see Ferguson 2017a), the statistical model, the regression line, is calculated by algorithms attempting to find a pattern within the data set. This process happens through machine learning: first a coder formulates an algorithm, before the algorithm attempts to predict an outcome based on a training set, tests the algorithm on the sample, modifies its mistakes, before perfecting its ability to predict the data. The result is thus the perfected algorithm, generated automatically with minimal human bias. The resulting data points that the model cannot predict are thus anomalies; the fault lies within the data, not the model. In state surveillance and security practices, the outlier represents the risk and should therefore be subjected to extraordinary measures. The underlying assumption here, is that all these data points have a certain identity that is measurable and possible to capture by big data. The assumption is that there is something magical in the absolute truth that can be performed by autonomous algorithms. Aradau and Blanke (2017) refer to the "performative effect of algorithmic rationalities" as a reformulation of the other as an anomaly. The line is no longer drawn between friend and enemy, or normal and abnormal, in algorithmic security identification. Rather, the algorithmic security risk is drawn as an anomaly, as an outlier in the statistical model as described by Kitchin (2017). In algorithmic security, the outlier is a "subject of security proactively produced", taxonomized in categories of "'undesirables' and risky selves to be monitored, corrected, or excluded based on the anticipation of future behaviour" (Aradau & Blanke 2017: 6) It is as if the individual which escapes governmentality, the potential criminal, abnormal, or revolutionary is captured by big data so that extraordinary governmental techniques can be applied; disciplining and governing the anomaly.

The promises made by big data are perhaps most clearly illustrated in algorithmic security practices, where "the computing literature has departed from statistical considerations by developing an analytical interest in detecting anomalies or outliers not as a measure of error, but as the very object of analysis." (Ibid.: 8) One problem here, however, is that the object of big data surveillance is never the subject itself, despite big data's promise of complete datafication; it is a "data double or (…) digital twin." (Ibid.: 6) It is as Ansorge points out: an identification but not an identity. The 'data double', a term usually attributed to Haggerty and Ericson (2000), is produced as the subject of security is not only a faulty representation of the analogue subject, it is the active production of the computational, calculable subject over which governmental techniques are exerted through taxonomizing and categorising. The extent and the depth of this legibility bear consequences for the quality of the governmental intervention made possible, however: "[l]egibility is a condition of manipulation. Any substantial state intervention in society (…) requires the invention of units that are visible" (Ansorge 2016: 37) However, despite the reflexive relationship between phenomenon and category, "there is always a remainder, a liminal character that does not belong to any devised category. This character is queer, obscure or appears anomalous but, it must be emphasised, only appears so because the sovereign's schema or taxonomy has no place for it." (Ansorge 2016.: 6) It is the queer character that big data security must correct.

So, big data is more than a simple qualitative leap from data to big data, but also a profound transformation of epistemology and cognition as

> processes of machine learning algorithms identifying clusters from data, generating attributes, and finding those very attributes in the patterns of other people are also shaping the relations to the world, from Cambridge Analytica's clustering of the attributes of voters to SKYNET's attributes of terrorist threat. (Amoore 2019: 4)

This alone, however, does not answer the question "how is microtargeting a threat to liberal governmentality?" One answer to this question lies in the different logics underpinning Cambridge Analytica's microtargeting and state practices of segmenting populations into subjects of security using big data. State security practices are about controlling and modifying the anomaly; the outlier. Microtargeting, however, in the context of Cambridge Analytica, is about reproducing that very anomaly; it is about reproducing each individual's digital echo-chamber. Microtargeting of the state – which is largely based on the same logic as microtargeting for the advertisement firm – is about governing anomalies, proactively producing the subject of security. Microtargeting in marketing, however, is about proactively reproducing the anomaly, outside of security. The epistemological consequences inherent in big data inform practices ascribed different meanings, different logics, by different actors. As such, the calculable individual, ready for computation, work as a basic discourse informing different outcomes in different articulations of what it means to render an individual legible in the age of cyber. Where liberal governmentality is the expansion of the logic of the market into all aspects of society, that very logic has also produced microtargeted ads. Cyber-capitalism made Cambridge Analytica. In the context of microtargeting however, the different outcomes produced by these algorithmic practices are paradoxical, always competing, as if they were two opposing rationales of governmentality, each attempting to govern the algorithmic subject – render the individual legible for manipulation – in separate ways. It is here that microtargeting arises as a threat to liberal governmentality; it is here that the rationale of the market – the rationale of liberal governmentality – folds in on itself, threatening itself in a circular manner, reproducing its own threat. Microtargeting is a paradox threatening liberal governmentality.

This is not the only context within which microtargeting is a threat to governmentality. As already argued, algorithms are a way of making data, of making the Internet, legible. In that way, algorithms are a form of 'ordering method' resulting from the "publics as always in need of orientation in uncertain situations." (Birkbak & Carlsen 2016: 39) Uncertainties are unknowns, and "[t]aming unknowns has been a key to critical discussions of security, risk, and uncertainty in security studies." (Aradau 2017: 329) Aradau identifies this uncertainty at the heart of algorithmic security practices as 'enacting non-knowledge' where especially the conflict between security and law is a key tension as "future-oriented security practices insert radical uncertainty at the heart of legal reasoning" (Ibid.) This conflict is exacerbated by digital technologies, and more specifically big data. There is more knowledge, and subsequently more uncertainty and more non-knowledge, as "transactional data turns knowledge about past behaviour into a 'form of actionable intelligence', which enables 'the *pre-emption* of what could be terrorist schemes or attacks." It is here that the way "security practices do not just tame but also enact unknowns" becomes visible. (Ibid.) O'Grady (2016) describe how legislations such as the *Civil Contingencies Act* "brought about major renegotiations in the operation, rationale and organisational shape of emergency response in twenty-first century Britain." An increasing number of security services are "charged with preparing and intervening in the present to secure emergencies in the future" (2016: 104) The present is increasingly formulated by uncertain futures. The sovereign wants data, but the more data one has, the more possible outcomes can be predicted, and the more unknowns can be acted on. This does not only entail an increased securitisation, or riskification (see Aradau & Lobo-Guerrero 2008; Corry 2012), but also an unbalance at the heart of sovereign computation. Ansorge points out how "[t]he sovereign hungers for data, but what it really needs is stability" and that "these contending drives produce legitimacy crises and 'constitutional moments' during which fundamental questions of social order become unsettled, and the relationship of central authority and knowledge to individual subjects can be renegotiated" (2016: 7) This echoes Aradau's point above, namely that the tension arising from this non-knowledge increases the tension between security and law. Where more data means more knowledge, it simultaneously leads to more non-knowledge; as the sovereign wants data, stability is undermined. As already pointed out, big data is nothing without algorithms; and algorithms are nothing without data. In order to understand the inherent instability in the sovereign's wants for data, one must also consider how the inscription of meaning to algorithms creates instability itself. Matzner writes that "as soon as predictive algorithms are applied and their results are acted upon they change the world that prediction inhabits. Thus, using the algorithm produces effects that counter the precondition of algorithmic design – the stability of the world." (2019: 126) The sovereign wants data for security practices; for surveillance and legibility of the people. But as this data is made legible by algorithms promising prediction, those very predictions, *those uncertainties*, prescribe action. But as soon as those actions are acted upon, the data on which these predictions are made is changed, rendering these predictions invalid. The temporal boundaries between past (informing the present), present (prescribing the future) and future (formulated in the present) collapse into a state of instability. The stability on which the state depends is threatened by the very algorithmic rationale of security practices. Microtargeting, as a process and tool of big data security practices, thus arises as a threat to liberal governmentality even without the presence of companies such as Cambridge Analytica. As such, just as liberal governmentality folds in on itself in microtargeting; producing its own threat, the algorithmic logic underpinning big data security folds in on itself as its enactment of non-knowledge reproduces uncertainties and instability.

6.2) The subject of governmentality

Among other things, big data means a lot of data. This does not only mean an amplification of data available for analysis; its volume means that new forms of deduction (and induction) must be applied to even render that data legible. Stanislaw Lem, referred to by Hayles, describes these huge amounts of data as "society facing what he called an "information barrier", a deluge of information that would overwhelm scientific and technological enterprises unless a way was found to automate cognition" (2014: 200) Microtargeting is a form of automated cognition (Wilson 2017). By this is meant that microtargeting, whose underlying logic is also present in recommendation algorithms applied by companies such as Netflix, are not mere "mechanical reproduction[s] of instructions" (Parisi 2019: 90) formulated by a programmer. Traditionally, automation has been exactly that – it has been the process of making industrial machines, for example, programmed to carry out a specific job previously carried out by a factory worker. Similarly, ticket machines are reproductions of work that was previously carried out by a ticket operator. Automated cognition on the other hand, or automated thinking, is different. Through the process of machine learning, the machine itself engenders automation. Automated thinking, as it were, is "the automation of automation" (Ibid.) This process lends itself to challenges as to what theoretical framework one should apply to analyse these cognitive processes, as they are in no way limited to the human. Here, Katherine Hayles (see 2005; 2012; 2014; 2016; 2017) has been a pioneer in the field, notable among other things for her concept of 'cognitive assemblages'. She defines cognition, and subsequently cognitive assemblages

> as a process of interpreting information in contexts that connect it with meaning. This view foregrounds interpretation, choice, and decision and highlights the special properties that cognition bestows, expanding the traditional view of cognition as human thought to processes occurring at multiple levels and sites within biological life forms and technical systems. *Cognitive assemblage* emphasizes cognition as the common element among parts and as the functionality by which parts connect. (2016: 32)

In the context of microtargeting, this means that the process of microtargeting should not be viewed as a mere expression of the programmer; as if the source code was the transcendental image of intellect. Microtargeting is not simply automated and effective advertisement. Microtargeting is a form of automated thinking. Before elaborating on this point, however, I would like to return to the most basic idea of the liberal subject as a subject of liberal governmentality, and how this very notion is threatened by microtargeting.

As described above by Foucault, the liberal subject is one governed by the logic of the market. The individual is understood – and should understand themselves – as an enterprise, as “an entrepreneur of himself” (Foucault 2004: 226) Under liberalism, the human is a consumer as well as a producer, as he produces his own satisfaction through consumption. Liberalism, therefore, came with “the essential epistemological transformation [in its] claim to change what constituted in fact the object, or domain of objects, the general field of references of economic analysis” (Ibid.: 222) Liberalism came with a transformation of what constituted the subject of governmentality. The individual should be understood as an enterprise that has scarce means, “and we do not have a single end or cumulative ends for which it is possible to use these means, but ends between which we must choose.” (Ibid.) The liberal subject, therefore, is a being with scarce means who make choices based on how they are to rationally deploy those scarce means in order to produce satisfaction for themselves. This ties into the emergence of “two absolutely heterogenous conceptions of freedom [inherent to liberalism], one based on the rights of man, and the other starting from the independence of the governed.” (Ibid.: 42) Foucault emphasises that heterogeneity does not automatically refer to exclusivity and paradox. Rather, these two conceptions of freedom coexist in the context of liberalism. The liberal subject, then, is the human as enterprise granted certain fundamental rights by the sovereign, free to engage in an economic order that is liberated from state interference. This individual is meant to reach “autonomous decisions [as a] mentally competent, fully informed individual, arrived at through a process of rational self-deliberation, so that the individual’s chosen outcome can be justified and explained by reference to reasons which the agent has identified and endorsed” (Yeung 2016: 124) The liberal subject, therefore, is not only free from the state and free because of their protected fundamental rights. The liberal subject is also one guided by rationality, and in order to be so, the individual must reach their decisions autonomously and fully informed. This is an image of a subjectivity that is threatened by microtargeting.

Microtargeting can be understood as regulatory governance by design. Microtargeting is a sort of automated behavioural marketing, that as a tool can “be used to manipulate and suppress human ideas” (Wilson 2017: 56) As a tool it is perhaps most visible through the actions of companies such as Netflix, or other streaming services, where the service suggests films and TV shows based on what you have watched before, that is, your previous behaviour. The technique of microtargeting used by Cambridge

Analytica was a form of ‘collaborative filtering algorithms’, meaning that they are “based on large amounts of digital data on users’ behaviour, activities or preferences and leads to predictions of what users will like based on their similarity to others” (Lury & Day 2019: 22) Another type of recommendation algorithms is that of ‘content sharing algorithms’, where recommendation is based on the characteristics of what you have already liked, and the algorithm attempts to find something similar to recommend (Ibid.). Cambridge Analytica’s clustering method was based on an idea that subjects in a specific segment of the population would respond likewise to a specific message. Data was collected so that every individual could be segmented into a specific type, categorised along the psychometric measurement known as the ‘Big Five’ (Heery & Noon 2017), the five axes of openness to experience, conscientiousness, extroversion, agreeableness, and neuroticism. What the individual liked would therefore say something on what the individual is like. Algorithmic tools were then deployed to formulate a specific form of communication, to guide the individual towards making a specific choice. Microtargeting can therefore be understood as a form of ‘nudge’, that is, as “any aspect of choice architecture that alters people’s behaviour in a predictable way without forbidding any options or significantly changing their economic incentives” (Yeung 2016: 120) When Netflix recommends a certain film to watch, this is precisely that – a recommendation. There are no external changes in economic incentives for the customer to choose to watch something different. When a microtargeted political advert encourages a constituent to vote (or not) for a candidate, this is only a ‘suggestion’ – not a coercion or an economic incentive. The recommendation is simply there to ‘guide’ the individual towards making a specific choice. Similarly, the existence of speed bumps is an example of ‘nudging’ – the speed dump does not force the driver to slow down, rather, the speed bump makes it more comfortable to drive slowly, incentivising the driver to do exactly that. All these three examples are what Karen Yeung describes as modes of ‘regulation by design’. By regulation by design, or regulatory governance, she refers to “a form of systematic control intentionally aimed at addressing a collective problem.” (2016.: 120). Regulation can be understood as “cybernetic processes, involving three core components that form the basis of any control system”. These are: “ways of gathering information (…), ways of setting standards, goals or targets (…) and ways of changing behaviour to meet the standards or targets” (Ibid.: 120). Both the speed bump, and microtargeting, are examples of regulatory governance by design: the ‘nudging’ towards the ‘right’ behaviour is built into the very architecture.

If one considers the Facebook-Cambridge Analytica case as a form of cybernetic process, regulation by design, one can see that the data gathering through the app ‘thisisyourdigital life’ paves the ground for the standard-setting – making the individual vote or not vote in a certain manner, and the algorithmic formulation presenting a political advert as the way “of changing behaviour to meet the standards or targets.” (Ibid.) This is an example of a ‘digital decision-guidance process’, which in contrast to ‘automated decision-making processes’ are “designed so that it is not the machine, but the targeted individual, who makes the relevant decision” (Ibid.: 121) In the context of big data, these digital decision-making processes through regulatory governance have certain characteristics distinguishing them from regulation by designs such as speed bumps. Where speed bumps are the same for everyone and are constantly there no matter if anyone is driving, big data has, as already mentioned, a certain dynamic nature. Big data regulatory governance can change and develop in real time; it develops through the recursive loops of data feeding into the algorithm; perfecting the *personalisation* of design. As already mentioned, microtargeting is a form of automated cognition: as regulatory design the very architecture learns from its environment. Yeung therefore refers to big data regulation as ‘hypernudge’, as

> [n]etworked, Big Data-driven digital-guidance technologies [that] operate as self-contained cybernetic systems, with the entire tripartite regulatory cycle continuously implemented via a recursive feedback loop which allows dynamic adjustment of both the standard-setting and behaviour modification phases of the regulatory cycle, enabling an individual’s choice architecture to be continuously reconfigured in real time. (2016.: 122)

The epistemological changes enacted by big data described in the previous section are therefore translated onto how behaviour is regulated, and how information is communicated, in cyberspace. This bears clear resemblance to the vision verbalised by Alexander Nix at the beginning of chapter five, where communication is individualised, and mass communication is dead. For Yeung (2016) this is where the liberal critique of microtargeting is situated: the individualisation of communication entails manipulation as it distorts the ideal of the individual as fully-informed making rational decisions. As a product of the liberal democratic order, "how then should the legitimacy of hypernudge be assessed, if legitimacy is understood primarily in terms of conformity with liberal democratic principles and values rooted in respect for individual autonomy?" (Yeung 2019: 123) The hypernudge challenges the very ideas from the society whence it arises, it questions the autonomy of individual decision making. As such, it goes further than the discourse centred on the privacy rights described in the previous chapter. Hypernudge – enabled by big data – is more than a question on infringement of privacy as a fundamental right. The hypernudge questions the mere ability to reach an autonomous decision; questioning the whole legitimacy of the liberal democratic process. From a constructivist or post-structuralist point of view, one could of course claim that the idea of the autonomous individual always was flawed (e.g. Luhman1986; Schneewind 1986; Meyer 1986). However, as a legitimising force, the discursive construction of the liberal subject informs not only the project of liberal governmentality, but the very concepts of sovereignty and legitimacy under liberalism. Individualised communication can never be complete information, and the subtle effects of online 'hypernudging' pave the basis of manipulation, distorting liberal subjectivity. As such, microtargeting arises not only as a threat to liberal governmentality through its employment within a market logic; it also distorts, from below as it were, the whole idea of what subject is to be governed by that very governmentality.

Tobias Matzner (2019) argues that automated cognition does not necessarily threaten liberal subjectivity and may even strengthen it. He analyses surveillance and architecture in order to illustrate how automated cognition can be viewed as complementing the rational aspect of liberal subjectivity. Like Hayles (see 2005; 2012; 2014; 2016; 2017), he argues that the ensemble of humans, machines, big data, and algorithms are best understood through the lens of 'cognitive assemblages.' This entails that the distinction between entities is not a priori, but "the very activity produces the entities in their specific form in the first place" (Matzner 2019: 127) The boundary between human and algorithm, then, is "enacted in a combination of continuity and difference" (Ibid.: 137) The algorithm should therefore not be posited as opposite to the human a priori. In the context of smart

CCTV – where algorithms detect anomalies in surveillance data – this means that the algorithm ‘fills a gap’ in the capacity of the human. The smart CCTV analyse massive amounts of data in order to track potential criminal activity by detecting anomalies. The final decision establishing whether or not there is something anomalous in the video, however, rests with the human operators. The final decision constructing the object of security is thus a human decision. In this context – as in all contexts with big data – the algorithm performs analysis on data sets that are simply too large for human cognition to process. In the context of smart CCTV, the function of the algorithm is not simply to analyse massive amounts of data; it also works to counteract the bias underlying human evaluation of the data. In this way, Matzner argues, the algorithm functions to reconfirm liberal subjectivity. Where liberal subjectivity is understood as the idea of the autonomous individual, rationally, thus unbiased, acting under free will, the inability of the human to perform this task in the context of surveillance is in fact performed by the algorithm instead. The activity of the human and the algorithm should here be understood along a continuum, where the continuum combined performs a task conforming to the ideas of liberal subjectivity: the algorithm aids the human in reaching autonomous, unbiased, and rational decisions.

Though somehow convincing regarding smart CCTV, this analysis is not so easily translatable to the Facebook-Cambridge Analytica case. The idea behind psychographics is not to reach autonomous, rational decisions. Rather, the idea is to reinforce and play on emotional responses and prejudices inhabiting the subject. As such, the very idea of the objective algorithm is not applicable to the case at hand. Additionally, it is harder to argue that the work of psychographics is to more efficiently perform activities that would otherwise be performed by human beings. The idea behind psychographics is that through analysing massive amounts of data one can uncover a certain rationale to behaviour specific to certain segments of a population – a rationale that is not even known to the subjects themselves. Psychographics is modelled after the construction of the liberal subject being flawed. And as such, it is necessarily threatening that very subjectivity through its discursive formulation of its counterpart. In Matzner’s analysis of liberal subjectivity in the context of smart CCTV, the underlying assumption is that the difference between data and big data is ‘big’. As analysed in the previous section, this does not encapsulate the epistemological changes pertinent to this movement towards 'big'. The idea behind smart CCTV is that more data may tell us more about what less data would tell us less about. The contribution of algorithms in this regard is to increase efficiency (and diminish bias). In psychographics, however, the idea is that big data may tell us qualitatively different things about subjects than less data could – that there are underlying patterns on the non-conscious level of human behaviour that can be uncovered using psychographic techniques. Additionally, these behaviours can be dynamically encountered with microtargeted communication; simultaneously evolving as behaviour changes. The difference is – psychographics is aimed at manipulation, whereas anomaly detection is simply that: detection. Yeung's (2016) analysis of the threat to liberal subjectivity posed by microtargeting is thus convincing even taking Matzner's (2019) analysis into account.

This is not the only way liberal subjectivity is threatened by microtargeting. The epistemological challenges at the heart of big data go deeper than that of the liberal ideal of the autonomous individual. Microtargeting challenges more than liberal subjectivity; it challenges the very idea of what it means to be a human. Matzner (2019) acknowledges the transformation of computational intelligence pertinent to big data as he argues that this challenge to what it means to be a human being does not necessarily threaten liberal subjectivity per se. However, I argue that anthropocentrism lays at the heart of liberalism. The very project of Enlightenment is centred on an idea of the individual guided by reason leading society towards progress. In this regard, technology is viewed as tools in the hands of human beings, in a similar manner as algorithms are often understood through references to their source code "ignoring that source code too, is just a part of the complicated interplay of many factors." (Matzner 2019: 125) This in turn leads to the conception of the program being the expression of the programmer, ignoring the dynamic interplay between algorithms, data, and environment (Parisi 2019). The obliteration of the idea of agency as centred in the human – even if this idea was always flawed – is itself a threat to the project of Enlightenment (see Adorno & Horkheimer 1997[1949]) When cognition – and agency – is automated; when a dating app algorithmically nudges you towards choosing your spouse (when an algorithm partly chooses your spouse); when autocorrect corrects your spelling or makes you question your own writing skills; and when automated cars analyse the traffic for you – what happens to human subjectivity? How are we to understand what it means to be human as opposed to machines (is there any human opposed to the machine?) when our very cognition is outsources to artificial cognition? In 1985, Donna Haraway published *The Cyborg Manifesto.* On the distinction between human and machine, she writes:

> Pre-cybernetic machines could be haunted; there was always the spectre of the ghost in the machine. This dualism structured the dialogue between materialism and idealism that was settled by a dialectical progeny, called spirit or history, according to taste. But basically machines were not self-moving, self-designing, autonomous. They could not achieve man's dream, only mock it. They were not man, an author to himself, but only a caricature of that masculinist reproductive dream. To think they were otherwise was paranoid. Now we are not so sure. Late twentieth-century machines have made thoroughly ambiguous the difference between natural and artificial, mind and body, self-developing and externally designed, and many other distinctions that used to apply to organisms and machines. Our machines are disturbingly lively, and we ourselves frighteningly inert. (2016: 11)

Ansorge writes that there is a tacit agreement in these digital times, that "the sovereign may look at and collect as much information as it can find, as long as it only uses the information to protect and prosecute – not persecute – and as long as it does so competently." (2016: 4) Informed by Haraway, I propose to extend that agreement to the machine. There is a tacit agreement that the machine – the algorithm – may collect as much information as it can find as long as it uses that information for our own benefit; as long as it is used to provide us with a representation of the world we would like to see. There is a tacit agreement that it is okay for the recommendation algorithm to suggest what we would like – to think instead of us – as long as it does so well. From a normative perspective, there may be much to say on this, but the aim of this thesis is not to arrive at normative conclusions. Rather, this tacit agreement warrants new conceptual frameworks for understanding where this automation of thinking leads us, because the simple distinction between human and machine; between human thinking and artificial thinking, is clearly flawed. It should be noted, however, that this conflation of boundaries is not a dystopian depiction of the world we behold. As exclaimed by Haraway it is also an "argument for *pleasure* in the confusion of boundaries and for *responsibility* in their construction" (2016: 7)

Algorithms are always present nudging us towards making certain decisions: what podcast to listen to next, who appears on Tinder or suggested friends on Facebook, what autocorrect wants you to write, or what Instagram wants you to buy. Parisi (2019) argues that this newly formed space for decision making in cyber-times as human and machine thinking become entangled is situated in the space between critical reasoning, logical inference, and sheer calculation. This space is not inhabited by a pure definition of the human. Rather, this space is inhabited by an assemblage of cognitions. In order to read this landscape, therefore, it is useful to take a step back and acknowledge not only the integrated nature of the algorithm into society, but into us as human beings. This is particularly important considering automated thinking. It is in response to these challenges that Katherine Hayles introduces the concept of 'cognitive assemblages.' Cognitive assemblages focus on the ability for cognition, rather than consciousness, as the common characteristic assembling certain entities and processes. As such, both human and (some) machines can be included in an analysis on how cognition operates. Thinking is something that involves awareness, whereas cognition "does not require consciousness, but can perform complex modelling and informational tasks" (Parisi 2019: 91) From an historical perspective, this move from non-cognition to cognition in machines is significant. Machine learning involves a "shift in computational models of logical reasoning: namely, from deductive truths applied to small data to the inductive retrieval and recombination of infinite data volumes." (Ibid.: 92) Machine learning involves a "change in [the] relationship between data and algorithms" as they are constantly responding to each other (Ibid.)

Lury and Day (2019) argue that the apparent individualisation of microtargeted communication – which function according to a similar logic as recommendation algorithms – is better understood as a form of personalisation, rather than individualisation. By this is meant that once recommendation algorithms formulate a certain presentation of the Internet to the individual, that presentation is not created based on the individual itself, but through references to what similar individuals, what that type of individuals, would like. In a curious manner, what you 'like' becomes what you 'are like'. Despite its appearance as individualisation, recommendation algorithms formulate what can be referred to as personalisation; they are not about the individual as distinct, they are about an abstracted persona composed of specific 'likes', applicable to a segment of individuals. Lury and Day refer to this as a-typical individuation, as a "mode of recursive inclusion, in which both the individual and the type are repeatedly specified anew" (Ibid.: 25) Here, the autonomous liberal individual is not only challenged through as it is subjected to manipulation by what appears on the Internet. The autonomous liberal individual is also threatened as the distinction between offline-and online categories of life are blurred. It is not only the type that is adjusted to the individual, the individual is formulated by the type and reformulates the type in a constant recursive loop. Lury and Day describe personalisation as "a *pathway* of a-typical individuation" (Ibid.: 27) The individual, and the type are inextricably linked: they are constantly reformulated through the pathway referred to as a-typical individuation. You become what you like.

Algorithms can be analysed as autonomous objects nudging the human towards a certain behaviour: in an extreme sense microtargeting is algorithms performing the thinking for the human behaviour. From this perspective, Parisi (2019) argues that algorithms, or automated thought, have not only taken over certain aspects of thinking, they have also profoundly changed the scientific image of what computational logic even is. This shift should be understood as a shift in the scientific image of intelligence mediated by the manifest image of intelligence. The manifest image of intelligence refers to the "socio-cultural self-awareness of a form of artificial thinking that admits the capacity of machines to think conceptually and act rationally", whereas the scientific image refers to "the material physical, biological computational description of intelligence" (Ibid.) From the scientific image of intelligence being centred on the Turing description, where the machine is a result of the source code of the programmer, the machine is now a deductive, inductive and abductive analyser of its environment, in a reflexive relationship with the context it inhabits. From the scientific image being centred on the programmer as the epitome of computational intelligence and cybernetics, as "the code is seen as the expression of the will of the programmer, and all other elements are reduced to determinist execution" (Matzner 2019: 125), "machine learning is the inverse of programming." (Parisi 2019.: 92)

Hence, the source code – the programme – is not the algorithm expressing the behaviour of the machine. Rather, the adaptive quality of machine learning – of the context – is what formulates the algorithmic function. This "non-logical thinking of automated systems overlaps with the efficacy of cybernetic calculus whereby control and prediction rely on inductive learning." (Ibid.: 91) Where the cybernetic ambition referred to in chapter two of this thesis, related to the idea of programming the world in a perfectly calculable fashion, machine learning adds to this power through its inductive and abductive ability. Here "cybernetic control becomes infused with the non-conscious algorithms of cognitive capital" (Ibid.). From this perspective, Parisi (esp. 2019), and with her Hayles and other scholars of STS, question the assumed objectivity of artificial thinking. Artificial thinking, which is increasingly based on the scientific image of machine learning, is inherently context bound as it responds to its environment (Lury & Day 2019; Parisi 2019; Hayles 2016). By referring back to Matzner (2019), this is another point where the analysis of algorithms in the context of smart CCTV as a reconfiguration of liberal subjectivity falls short. Smart CCTV is about identifying anomalies, and the algorithms employed have an adaptive quality – they perform machine learning. However, as is pointed out by Matzner, the identification of anomalies may be flawed. For instance, a disabled person may move in an anomalous manner without that being the anomaly – the potentially criminal behaviour – the surveillance is trying to identify. For Matzner, this is where the role of humans as the ultimate decision makers in defining what constitutes an anomaly is central. Here, it is human cognition that is able to identify that although a certain movement is anomalous, that is not the anomaly the CCTV is looking for. For Matzner, this functions as a sort of 'safety' and is an example of where the human and the machine complement each other by performing the task they respectively perform the best. However, if we return to the space of decision making outlined by Parisi, as situated between critical reasoning, logical inference, and sheer calculation, it becomes clear that the assemblage of cognition operating within anomaly detection should not merely be understood as a partial outsourcing, or automation of human surveillance. Rather, as has already been mentioned, machine learning entails the emergence of a new meta-level of thinking, one that Parisi (2019) refers to as ‘automation of automation’. By this is meant that the adaptive quality of the algorithms implies that their performativity is more than a mere ‘tool’, they are performing a new space of meta-cognition. The potential bias of the algorithm will thus be twofold. On one hand, the source code of smart CCTV algorithms will be subjected to biases through its identification of anomalies. This source code will be developed based on a training set within which a certain formulation of anomaly will be present. Here, the risk is that the algorithm will automate the same biases as a human being may have. Additionally, the algorithm will go beyond a mere automation of human surveillance. The algorithm will evolve autonomously, thus dislocate human agency, through a process of deduction-induction-abduction. As such, a new space of thinking evolves, within which the algorithm will be subjected to the same epistemological challenges as discussed previously in this paper. Automation of automation involves a shift in cognitive capital from human to machine, and it is here that “cybernetic control becomes infused with the non-conscious algorithms of cognitive capital” (Parisi 2019: 91) This thesis argues that it is this algorithmic autonomy pertinent in the shift in cognitive capital which challenges the ideology of liberal subjectivity at the most profound level.

6.3) Governmentality in the age of cyber

> Government governs not through wisdom in general, but through the truth, that is to say (…) that reality that constitutes population, the production of wealth, work, commerce – if it governs through the truth then it will have to govern even less (…) if men were to govern according to the rules of evidence, it would be things themselves, rather than men, that govern.

Foucault (2012:13-14)

For Foucault, power is inextricably linked to truth. The formulation of truth is an act of power, and enactment of power is enactment of truth (Ibid.) Big data, as was also discussed in the first section of this chapter, is a new form of truth-production. Yeung defines big data as a technology and a process. As technology it refers to the "configuration of information-processing hardware capable of sifting, sorting and interrogating vast quantities of data very quickly" and as process it "involves mining data for patterns, distilling the patterns into predictive analytics and applying the analytics to new data." (2016: 119) Big data then, brings with it, epistemological consequences reformulating truth. Historically, the emergence of statistical models such as the Bell-curve have been the formulation of the average man. As such, the average man has served as a truth around which governmentality has been structured (Amoore 2016, see also Hacking 1986). With the emergence of big data statistics, I have argued that the focus is not so much on the second and third quartile of the normal distribution. Rather, the focus has increasingly been on the tails of the curve; about normalising the abnormal, detecting the outlier, governing the anomaly. As such, the normal has been defined, inscribed with truth, around which governmental technics have been formulated to discipline deviance.

In the previous two sections I analysed how mictotargeting arises as a threat to governmentality through the different meaning assigned to anomalies in state security practices on one hand, and marketing strategies on the other. Additionally, big data as a phenomenon poses challenges to the stability of the state through its overload of information. I have also demonstrated how microtargeting threatens the very subject of governmentality, both through its distortion of an ideal form of rationality, as well as through its relocation of cognitive capital. Kitchin refers to these assemblages of non-conscious cognisors as 'algorithmic machines', and points out how these algorithmic machines' dominance have "led a number of commentators to argue that we are now entering an era of widespread algorithmic governance, wherein algorithms will play an ever-increasing role in the exercise of power, a means through which to automate the disciplining and controlling of societies and to increase the efficiency of capital accumulation" (2017: 15) From a Foucauldian perspective, this shift in power towards algorithms should not only be viewed in terms of technics of governments. It also entails a transformation of the rationale of government. If the 'automation of automation' entails a shift in cognitive capital, then that automated rationale will also have an impact on the rationale of that very governance. Algorithmic governance is more than governance through different means, it is a transformation of liberal governmentality.

6.3.1) The digital mode of power

Foucault’s disciplinary society was one characterised by enclosures. It was about disciplining in school, in prison, in the factory or in the family. These different enclosures came with their own norms and regulative practices, which one would leave when entering another. The society of enclosures has undergone a crisis since World War II, argues Gilles Deleuze, as “these institutions are finished” and are replaced by society of control. The enclosures of disciplinary society are “*molds,* distinct castings, but controls are *modulations,* like a self-deforming cast that will continuously change from one moment to the other, or like a sieve whose mesh will transmute from point to point” (1990: 4) In society of control education does not end in school, rather we are expected to constantly evolve and learn. Competition does not end once you have secured a job, rather it continues at work where you are constantly pitted against your colleagues in competition for higher positions. “The disciplinary societies have two poles: the signature that designates the *individual,* and the number or administrative numeration that indicates his or her position within a *mass*” (Ibid.: 5) In society of control we no longer find ourselves dealing with this pair of categories, rather “[i]ndividuals have become *‘dividuals,’* and masses, samples, data, markets, or *‘banks’*” (Ibid.) Governmentality then, in society of control should be understood as the government of samples or data, constituted by dividuals; of data-doubles. Deleuze (Ibid.) argues that the new technic of power in society of control is the computer.

Ansorge refers to three different modules of power in the hands of the governor. These are the ritual mode, the archival mode, and the digital mode. In his quest to answer the question on how people are identified and sorted, he invites the reader to “[c]onsider the ritual. Hierarchic and classificatory distinctions do the heavy lifting of identifying and sorting processes. They can be grounded in a ritual order, just as much as they can be anchored in bureaucracy or a bill of rights”, the ritual mode is “prescribed formal behaviour for occasions not given over to technological routine” (2016: 55) The archival mode, however, is different from the ritual mode in that it is centred on the written. The written word, and with it, literacy, opens up “novel avenues for the centralised control and homogenisation of human actions” as it provides whole new modes of legibility.” (Ibid.: 69) Last of these three modes, which evolve in procession without excluding the former, is the digital mode. With the digital mode of power comes also the database, which Ansorge conceptualises as a new tool of governance. Databases are hierarchic, rhizomatic, or anarchical organisations of datapoints that logically relate to one another. The information produced by databases are "inherently instrumental (…) both external things and the behaviour of people – can be ruled by calculation" (Ibid.: 94) As a new tool of governance it is situated "somewhere between ideal and material, theory and practice, structure and agency." (Ibid.) Ansorge argues that the method of organising and categorising this data on people and behaviour creates so-called 'limit-shapes' – "a new technology of segmentation that would be applied to many different aspects of domestic and world politics." (Ibid.: 95) One of these limit-shapes is present in Cambridge Analytica's application of microtargeting, or psychographics. The division of a population into the a given composition of scores within the categories of openness to experience, conscientiousness, extroversion, agreeableness, and neuroticism is a way of making people legible, and thus produce information. These categories are, of course, artificial in the sense that they are socially constructed by data produced under certain conditions – they are limited in their ability to reflect the world as it is, excluding certain attributes, while including others.

Similar to Ansorge's concept of the digital mode of power is Buyng-Chul Han's (2017) concept of 'psychopolitics'. Psychopolitics represent a move away from Foucault's biopower, as it is the mind rather than the body that is governed. There are two main problems with Han's psychopolitics. One relates to the clear distinction between the mental world of the citizen contrasted with their physical presence as a body. This separation bear resemblance to Hayek's connectivism discussed above where the external world is equal to all and the intellect is the makeup of a network of neurological patterns that can be disseminated and replicated. This leads to the second problem with psychopolitics. Han does not capture what Ansorge so brilliantly does: namely that the database's representation of the citizen is a data-double; an identification of the individual which will never be complete. Additionally, Ansorge points out that although the digital mode of power is fairly new and increasingly dominant, it has not come to completely replace the archival and ritual mode. Where psychopolitics are to replace biopolitics, Ansorge does not presume that the database is to replace the material aspects of governance in a digital age. To claim that what happens in cyber does not stay in cyber implies a translation of the digital to the analogue. That implies that the analogue still exists.

Another point to make is than the digital cannot be reduced to the virtual; there are material aspects to cyberspace. Where servers are located, for instance, has come to be a question of geopolitical power (see Bridle 2018; DeNardis 2014; Halpern 2014) Likewise, our access to cyberspace is mediated by tangible machines, be that computers or phones. The recent discussions on Huawei's bid for expanding the 5G network capacity is a clear example of this. Here, the debate is twofold. On one hand there is the question of the power underlying ownership and control of the 5G Internet by a company with alleged ties to the Chinese government (Neate 2019). Here, the focus is on the virtual, on the flow of information. This is intertwined with discussions on the monopolist position of developers of a new generation of the Internet. On the other hand, one can also find arguments claiming that Huawei's development of the 5G network would not be a bigger concern than the role of Chinese industry in manufacturing digital devices (Bui & Wee 2018). Here, one acknowledges the materiality embedded in technology. Information and control of the Internet cannot be separated from the devices that enable information flows. One can argue in a similar manner, that the human body as a site of biopower cannot be separated from the mental exercises – the psyche in psychopolitics. Matzner (2019) makes the point that the use of apps that monitor bodily functions, such as sleep or eating, represent a break with the ideas of Enlightenment, and to some extent with liberalism. Liberalism views human beings as governed by reason and thus less bodily. The outsourcing of the reading of bodily signals to technical devices is also an acknowledgement of the bodily aspect of existence. As such, one must ask what biopolitical powers are embedded in this kind of monitoring. And what is more, if this monitoring is the outsourcing of cognition in order to govern the body, it becomes difficult to claim that the distinction between the digital mode of power and biopower can be reduced to bodily versus mental focus, as Han implicitly claims. Just as Huawei's ambition to build the 5G net cannot be reduced to the digital flows of information, the technics of governmentality embedded in the digital cannot be reduced to the virtual.

However, the digital mode of power brings with it new technics of governmentality. The database allows for the government of the unknown. This is not entirely new to the Internet as risk has been a topic of study in security studies since the end of the Cold War. Most famously, Ulrich Beck defines risk as “a systematic way of dealing with hazards and insecurities induced and introduced by modernization itself.” (Elbe 2005: 181; Rasmussen 2001: 290). As such, risk, according to Beck, exists in a reflexive relationship with society in modernity, as it is modernity itself that produces its own dangers. This will lead to a conflation of the referent object and the threat. Stefan Elbe (2005: 178) argues that this is corroborated by the conflation of ‘risk’ and ‘security’ in notions such as ‘risk security’. Beck’s notion of risk has however been criticised for its shortcomings. Along the lines of Francois Ewald’s conceptualisation of risk as a neologism of insurance (see Elbe 2005; Ericson & Doyle 2004), Leander (2005) and Krahmann (2011) identify how risk is omnipresent and a product of the privatization of security. An important distinction between risk and security is that security deals with a known threat. As such, one can enact security practices in order to mediate the threat. From the perspective of security studies, this is where exceptional measures are put in place. Risk, on the other hand, deals with the unknown. Risk is, by definition, something with low probability of happening compared to a security threat. As such, risk constitutes something unknown. It is unknown if it would happen, and oftentimes, it is also unknown exactly what would happen (Leander 2005; Krahmann 2011; 2018, see also Aradau et al 2008). What is more, a risk cannot be effaced, only mediated. Thus, one aspect of risk is that the ‘exceptional’ security measures put in place to counteract a risk are not exceptional at all. Rather, they constitute a new normal put in place to mediate an omnipresent, ever-present risk. In that way, risk enables government of the unknown, or government of non-knowledge (Aradau 2017). More data means the possibility of identifying more risks, it enables the assemblage of non-knowledge on the basis of too much knowledge. Risk identification and practice, therefore, is one example of the government of the unknown being exacerbated by big data, or the database.

James Shires (2018) notes that the increase in expert knowledge on cybersecurity entails an increase of the field of cybersecurity. That is, an increase in data, combined with the increase in expert knowledge to render that data legible, leads to an increase in ‘things’ that must be secured. Thus, there is an increase in identified potential risks, which again enables the enactment on more unknowns. A similar pattern is found in surveillance, as the increase of data means that more individuals are targeted. That is, the more data the sovereign has on its citizens, the more anomalies are identified. Here, the distinction between big data and statistics is relevant. If microtargeting is conceptualised as an equation, which the algorithm is in its basic form, it is a basic law of statistics that if a statistical equation is complicated enough, the model will speak for itself rather than the data (Christophersen 2018). As algorithms often evolve dynamically, starting from the source code but adjusting to the environment, an algorithm could potentially be close to infinite in complexity. As a generator of truth, it makes sense that this algorithm may express itself rather than the data when presenting an output. What is more, the more anomalies one looks for, the more parameters in place to identify outliers, the more one will find. Increased surveillance then, as a form of data collection and analysis, will provide the sovereign with more anomalies, and more unknowns. From the perspective of microtargeting, this is interesting. As already identified, microtargeting is both a technique of marketing, and a disciplining force. It becomes a threat to governmentality as it operates to reproduce anomalies, whereas microtargeting as a disciplining force is meant to govern anomalies. However, as a disciplining force, as a security practice, it is two-fold. On one hand, the greater amount of data, the more legibility of the populace for the sovereign. But, as already pointed out, the more data the sovereign has, the more they undermine stability; the more data one has for security practices, the more insecurity one will find; the more potential risks will be identified. As pointed out by Ferguson (2017) this does not only mean instability and insecurity for the state as such, as the state produces its own insecurity. It also means insecurity for very many humans, and especially humans who are already subjected to police profiling. Here, microtargeting arises again a security threat to liberal governmentality, as it produces those very anomalies as it wishes to discipline; microtargeting produces the subject of security.

Ansorge points out how the practice of singling out particular individuals through the exclusion of certain characteristics in the data was core in the German “hunt for the Rote Armee Fraktion (RAF) terrorists” in the 1970s (2016:95) This ability has been exacerbated by big data, and unlike Han who views digital power as significantly distinct from biopower, Ansorge argues that this constitutes “a new form of radicalised bio-power that is sufficiently distinct to warrant its own signifier”, namely digital power (Ibid.: 97) As such, digital power follows the same logic as biopower, and coexists with biopower, which the previous example on surveillance illustrate. Another example is to find in Amoore’s work on biometrics. Here, she argues that the use of “digital technologies, data integration and managerial expertise in the politics of border management” such as retina scanning and fingerprints means that the body itself becomes “inscribed with, and demarcates, a continual crossing of multiple encoded borders” (2006: 337). This means that for the immigrant, asylum seeker, or potential terrorist, the border does not end at the geographic boundary separating one state from the other. Rather, the border is continuous as it follows the body it is inscribed on. As such, there is not a clear distinction between digital power and biopower. Rather, biopower increases in that digital technologies enhance the ability of continuous surveillance. In a digital era, this means that the biopolitical border becomes a biometric border as the body itself become inscribed with digital knowledge. This also contrasts Han’s concept of psychopolitics, as he argues that the site of sovereign power is located on the psyche, rather than the body. For Amoore, as well as Ferguson and Ansorge, bifurcation of the two is artificial. The digital is better understood as a new technic of legibility; a new mode of knowledge-production, or a new mode of producing truth.

6.4) The global context

As outlined in chapter three of this thesis, governmentality comes with certain challenges on the international level. As pointed out by Joseph (2009) the subject of governmentality is the people, whereas the subject of global politics are states. In the context of Internet governance, however, this claim is somehow distorted. Although nominally the main actors in Internet governance are those of private actors or corporations, states, and civil society (Carr 2015; 2016), the non-territorial nature of cyberspace makes a multi-stakeholderism approach to the Internet just as complicated as an approach from the perspective of governmentality. Central to multi-stakeholderism is an idea of security, and in the context of Internet this idea is most clearly expressed in works on cyber-security. The field of cyber-security is vast, and a complete discussion on aspects of this field of security is beyond the scope of this section. Rather, I wish to explore whether the findings from the previous sections of this chapter; namely the inherent conflict within liberalism exacerbated by big data, can tell us something on the internal workings of multi-stakeholderism in the global context of Internet governance, and thus inspire future research.

This exploration is based on the premise that liberal institutionalism is the dominant ideology driving global Internet politics. Secondly, it is based on the premise that it is within this framework the liberal ambition for expansion – as formulated by Foucault – is best captured. Here, the conflict in expanding a liberal notion of Internet governance unfolds as a paradox: on one hand Internet is formulated as a 'free' space. However, this notion of freedom is inherently liberal – it builds on an idea of freedom as on one hand being freedom from state interference, and on the other hand as freedom in the form of fundamental rights of individuals. In multi-stakeholderism, a central point of contention arises as this formulation of freedom – freedom from the government – is viewed as an absolute and universal form of freedom. By this is meant that the vision of the free and open Internet is not only a Western and liberal formulation of what a free Internet is and should be, it is also an expansion of liberal jurisdiction into the realms of non-sovereign space (Mueller 2017). Although this is not entirely new to the Internet, as noted by Neumann (2011; see also Bartelson 1995; 2001; 2014) and others, the global ambition of liberalism puts it in a specifically paradoxical situation. Mueller (2017) points out this paradox in the liberal vision of the Internet: where Western states criticise especially China and Iran for expanding their sovereignty into cyberspace, that very criticism speaks from the premise that it is the liberal jurisdiction – notable for its freedom from government – that should govern in cyberspace. Likewise, the very notion of Internet as best governed by a tripod cooperation between private companies, states, and civil society is an inherently liberal idea of how and international space is best governed. These conflicts stick even deeper. Even the formulation of information technologies as 'cyberspace' is an inherently western conceptualisation. Branch (forthcoming) points out that the choice to designate this space as a *space* is a social construction. Rather than formulating the Internet as a tool for communication, cyberspace is formulated by spatial metaphors, which again subject it to territorialisation. One could have chosen, along Russian and Chinese terms, to designate the Internet with the signifier 'information technologies', omitting the contentions that spatial metaphors carry with them (Ibid.).

Biometrics is not the only way in which governmentality in cyberspace transgresses state boundaries. A focus on the Internet will always have to consider the supranational nature of cyberspace. Ansorge argues that there are four core issues making the digital mode of power and Internet governance a global question. Firstly, there is the global ambition of the U.S. in the political arrangement of the Internet. This is not new to the Internet as it visible also in previous arrangements of categorising databases, such as the Dewey system for categorising a library. Secondly, these techniques of categorising have spread across the globe, "to the point where they are increasingly used or aspired to by all states, leading to a progressively homogenous set of political tools and techniques in the international system." (2016: 96) This is also evident in fundamental arrangements of Internet governance such as the Domain Name System (DNS) that "translates between the alphanumeric names that humans use (…) and the binary addresses computers use to route information to its destination" (DeNardis 2014: 4) Third, big data analytics are increasingly used to make international phenomena legible, and thus "framing and sorting global human life." (Ansorge 2016: 96) Lastly, "these modern tools are used to maintain a complex international migration regime in which certain classes (…) circulate easily while others face a huge barrier to entry, both literally and metaphorically" (Ibid.) echoing Amoore's work on the biometric border. I would add to Ansorge's point on the global ambition of American or Western categorisation of the database, that this ambition is not only a technical one, but also a liberal and ideological one. It is also useful to add that Internet technologies are not only an application of a specific technique to render a database legible. They are also part of the ambition for a global virtual space, even if its creation is imperfect. As a global space it is also characterised by a specific idea of how space and freedom should be organised. It is a particular vision for Internet governance that is a liberal one; centred on a western idea of political organisation that claims global relevance. Hayek, as referred to by Foucault, captures this ambition:

> We need a liberalism that is a living thought. Liberalism has always left it to the socialists to produce utopias, and socialism owes much of its vigor and historical dynamism to this utopian or utopia-creating activity. Well, liberalism also needs utopia. It is up to us to create liberal utopias, to think in a liberal mode, rather than presenting

> liberalism as a technical alternative for government. Liberalism must be a general style of thought, analysis, and imagination (2004: 219)

Internet, in its starkest sense, pertains visions of a liberal utopia. It is to connect people across the globe; provide information and communication free from state interference. It is to nurture freedom of speech and freedom of organisation. This vision, of course, is not complete. Recent events such as the Snowden affair (DeNardis 2014; Mueller 2017; see also Byman & Wittes 2014; Verble 2014; Sprenger 2015) have shattered the vision of a free and open Internet, as the U.S. and with it other western states have come to realise the vulnerability inherent in a non-territorial space. Likewise, the Facebook-Cambridge Analytica scandal is situated in a landscape within which the combination of capitalism and social media has arisen as a threat to liberalism. The freedom inherent to a liberal vision of the Internet are also the dangers of that very Internet, both inside and outside cyberspace. This is not to say that these vulnerabilities should be 'fixed', rather, it is an argument that the mediation of the threat may well end up eradicating what it is supposed to protect. Additionally, Chinese and Iranian efforts to control information flows (see DeNardis 2014; Mueller 2017) have led to a fragmentation debate, that "is really a power struggle over the future of national sovereignty in the digital World" (Mueller 2017: 5)

Laura DeNardis (2014) refers to Internet governance as an oxymoron. As such, she argues along the same lines as Milton Mueller in the quote above: the supranational global of Internet is always in conflict with the national and sovereign. As such, Internet governance threatens the fundamental ideas of liberal institutionalism as first formulated by Keohane and Nye (1989) as a regime of complex interdependence leading to stability. Where supranational issues such as jurisdiction of oceans or pollution may be solved through international organisations, allowing for the mediation of causes through a complex architecture of niche institutions (e.g. Stokke 2011), cyberspace is complicated as it is a transcending 'space'. It is a domain with no sovereign, to put it bluntly.

The main purpose of Internet governance is the "design and administration of the technologies necessary to keep the Internet operational and the enactment of substantive policy around these technologies." (DeNardis 2014: 6) However, the establishment of these technologies and designs are far from apolitical endeavours and entail power-struggles in defining the architecture of these arrangements. DeNardis refers to the "control of names and numbers [as] a fundamental global struggle of Internet governance since the 1990s" (Ibid.: 8) She further argues that the struggle for power over the Internet is not only a matter of designing the architectures governing cyberspace. It also about using these designs to control global information flows. Here, intellectual property, probably most famous through the Stop Online Piracy Act (SOPA), is one example. The Online Piracy Act was a proposal represented before the U.S. House of Representatives in October 2011. The purpose of the bill was "[t]o promote prosperity, creativity, entrepreneurship, and innovation by combating the theft of U.S. property, and for other purposes." (U.S. Congress 2011) However, the bill would also have required all sites to block links to other sites with content that could potentially violate copyright laws. This was viewed as an infringement on freedom of speech as it "could have also created different possibilities for content mediation apart from intellectual property rights enforcement, effectively creating an infrastructure aimed primarily toward the blocking of content rather than the free flow of information" (DeNardis 2014: 8) On one hand, there is the liberal idea of property rights. On the other, there is the liberal idea of freedom of speech.

One of the main reactions in the U.S. following the Facebook-Cambridge Analytica scandal was allegations of Russian interference in the 2016 election. These were investigated in the Mueller report, stating that the Russian involvement in the elections were true, and that they happened through two operations. The first was that "a Russian entity carried out a social media campaign that favoured presidential candidate Donald J. Trump and disparaged presidential candidate Hillary Clinton" The second revolved around computer-intrusions, that is the hacking and spread of malware "against entities, employees, and volunteers working on the Clinton Campaign and then released stolen documents." (US DoJ 2019: 1) The campaign against Hilary was characterised by what the Mueller report refer to as "information warfare" which included "the purchase of political advertisements on social media in the names of U.S. persons and entities, as well as the staging of political rallies inside the United States" (Ibid.: 4) What is curious about the Russian involvement is its rather 'conventional' use of social media. That is, most of the influence happened through so-called 'troll-factories', where social media profiles were produced to impersonate a real person, and these ‘fake’ accounts would then be used to promote the content of other fake accounts, artificially creating echo-chambers (Ibid.: 29-31). The role of big data, as such, and microtargeting was limited. What was used was the ‘inherent vulnerability’ of free and open social media, as well as the liberal state, namely through creating social media accounts that would communicate certain messages and organise events. These findings from the Mueller report echo the findings in the report issued by Oxford University’s Computational Propaganda Research Project (2018), where they found that the most used technique of IRA for influencing the U.S. elections was that of producing organic content, and not advertisement.

However, the latter was also used as “[s]ocial media are particularly effective at directly reaching large numbers of people, while simultaneously microtargeting individuals with personalized messages” (Ibid.: 39) What is perhaps curious, is how both these reports found that although IRA’s influence was directed against Hilary Clinton, it was directed in favour on both sides of the political spectrum: both in favour of Trump and Sanders, both for and against Black Lives Matter. Both reports note how IRA controlled accounts organised events both against and in favour of an issue, as if the purpose was to increase disagreement rather than to tip popular opinion in one direction or the other. It is as if IRA’s involvement was all about abusing freedom of speech and freedom of organisation in the U.S. in order to upstir chaos and disagreement through reproducing digital (and analogue) echo chambers. As such, these attempts at influence bear some resemblances to the fundamental logic of microtargeted ads. They identify a weakness in liberalism; a weakness that when reproduced may destabilise the very system of liberal governmentality.

In the Mueller report, the threat representation is quite straight forward. The threat is Russia, and the action is political propaganda through new means. The threat representation of the Mueller report is therefore one of a geopolitical logic, neatly placed within a conventional view on security. This thesis, however, has argued that microtargeting, or in this case the use of social media in political campaigns, is not that straightforward. Firstly, it is subtle in nature. Secondly, it cannot be reduced to a ‘threat to democracy’. The legal question surrounding IRA’s involvement in the 2016 US elections is based on the creation of fake profiles, that is not identify-theft profiles, but profiles with an identity that does not correspond with the person creating the profile (US DoJ 2019), which is illegal in the US, but not illegal in countries such as Germany (Fioretti 2015). Furthermore, if the problem is fake profiles, what if a large group of Russians wanted, without being paid for it, to communicate political views to their American counterparts? Would that still be a threat to democracy, and in that case, why? Most of the work on microtargeting as a threat have focussed on how it threatens democracy (See Borgesius et al 2018; Watts 2018; Unver 2017). As already mentioned, I do not think this is a useful approach, for several reasons.

First, positing democracy as a referent object also presents us with already mentioned problems. The use of social media and big data has been prominent in American elections since the 2008 Obama Campaign (Hersh 2015) and is now common amongst all political campaigners in the U.S., as pointed out by Senator Tillis in chapter 5.3. Secondly, it does not capture the supranational nature of cyber, and liberalism and capitalism in cyber. One cannot reduce microtargeting to the technique itself; the whole spectre of collecting the data, manipulating the data, before communication is a whole array of practices underpinning the meaning-formation of the final message. And this array of practices transcends national borders, both in terms of the author of the message and the recipient. In the case of microtargeting in U.S. elections, for instance, the actors have proven to be American nationals such as Ted Cruz. But as we know from the hearings on Cambridge Analytica, the data used had been collected from around the world via a company that was registered in the UK with ties to Israeli military operators. A key point made in Internet governance is the global character of the Internet, and Internet is data, as well as algorithms and infrastructure. In order to understand the manipulation of that data one must approach the topic from a global perspective. Third, if one wants to counteract the threat posed by microtargeting from a global perspective, democracy is a dangerous referent object. This is not only because Internet is not per definition democratic, it is also because society utilising, and living, in cyber is not only people living in democratic societies. Furthermore, by positing democracy as referent object, one is inadvertently re-nationalising the Internet through an expansion of a liberal notion of democracy and societal organisation into the realm of cyber.

7) Conclusion.

In this thesis I have, among other things, attempted to demonstrate how the change in the episteme concomitant to the emergence of cyber, has come to threaten an analogue rationale of governmentality. This demonstration has followed microtargeting as logic and process from its situation within the wider context of computation in cyber, through its construction of meaning in Senate hearings, to its threatening position towards the liberal subject of governmentality, and the international level of Internet governance.

Microtargeting arises as a threat as the interest and rationale of private corporations or politicians diverge from the interests of the governor. When the governor uses microtargeting techniques; when governmentality governs the algorithm, it does so to govern the anomalous. When capitalism governs the algorithm, it does so to reproduce the anomaly, enforce the divisive; reproduce the echo-chambers. From a liberal perspective, this is particularly complicated as liberal governmentality is to a large extent defined by its position vis a vis the economy. In the context of cyber, the potential contentions between liberal governmentality and the liberal market are once again exacerbated. This conflict is also visible at the level of cybersecurity. McCarthy (2018) demonstrates a difficulty inherent in cybersecurity. As most critical infrastructure is owned by private actors, but security for the state depends on security of that critical infrastructure, this means that state security practices must be directed towards the private. This is not necessarily a problem itself, but what is a problem is that the private actors' ability to provide cybersecurity is a competitive advantage in a capitalist market economy. State interference would therefore undermine market competition. And lack of state interference would undermine state security. As many actors in the economy of cyber are multinational, not only is the distinction between private and public blurred, but also the distinction between local and global (Collier 2018). To provide a solution to these challenges is not an aim of this paper. However, these issues illustrate the need to move beyond state borders and to the level of epistemology when analysing issues pertinent to cyberspace. It also requires us to acknowledge that state and capitalist interests do not always align, although the privatisation of security provision seems to be built on a presupposition that they do (e.g. Krahmann 2011).

It should be emphasised that the limits to big data – that is, the fact that *n* does not equal all, and that there are measurement errors in big data as inn all kinds of statistics – also apply to microtargeting (see Kitchin 2015; 2016; 2017). The efficiency of microtargeting has also been disputed (see esp. Hersh 2015), and as pointed out by Hersh in the June hearing in the Senate; the promises made by psychographics to be able to manipulate behaviour are not necessarily scientifically grounded. Despite this, I believe microtargeting as communication should be analysed as a threat. Like all communication, it affects how we see the world. In an age of cyber, communication is increasingly individualised for each and every one of us. What effect that has on society should not go unexplored.

I have attempted to balance my analysis in on the borders of what a metaphorical cyberspace beholds. In doing so, I have avoided to engage in discussions on what cybersecurity is, or what security in cyber-times is, or should be. This does not mean that security has not been a topic in this essay. If I were to suggest future research building on this point, I would emphasise the relevance of studying the epistemology of cyber-technologies. Betz and Stevens (2018; Stevens 2018) argue against analogue reasoning in cybersecurity. I would also argue against digital reasoning in cybersecurity. If cyber-technologies are integrated in society; if critical infrastructure is the veins of society and binary code transforms our cognition of ourselves and the world, the digital can never be reduced to the analogue and vice versa. In order to balance the line between the analogue and digital, a focus on information may be a good start. As pointed out at the beginning of chapter two, the Internet *is* data. The Internet is information transmitted through electrons shaping the infrastructure of a communications network. The language of this 'computational regime' (Hayles 2002) is binary code. However, not all information is binary code, and not all information is transmitted digitally. What is more, most people neither see nor understand binary code. From a Foucauldian perspective then, understanding power will always entail understanding knowledge. And knowledge is more than information; it is ontology, epistemology, and infrastructures of transmission. As such it is everything from and beyond algorithms, art, scientific experiments, and speech. If understanding these knowledge productions and information flows is the starting point in an analogue world, I cannot see why it should not also be so in a cyber-world. As pointed out by Karl W. Deutsch: “The science of communication and control, which has been derived from this technology and which Norbert Wiener has called ‘cybernetics,’ is therefore a new science about an old subject.” (1966: 76) The question then, is both what epistemologies underpin this new science of an old subject, as well as the role of the old subject itself. It is a fine line to balance between old and new, and between banal and exceptional. I have attempted to balance on this line throughout these pages through an exploration of a metaphorical cyberspace by the means of microtargeting.

8) Bibliography

Adesina, A. (2018) “Data is the new oil” Published by Medium on November 13th 2018, url: https://medium.com/@adeolaadesina/data-is-the-new-oil-2947ed8804f6 (accessed February 27th 2019)

Adorno, T. W. & Horkheimer, M. (1997[1944]) *Dialectic of Enlightenment* (London: Verso Books)

Amoore, L. (2006) “Biometric borders: Governing mobilities in the war on terror” Political Geography 25: 336-351

Amoore, L. (2016) “What Does It Mean To Govern With Algorithms?” Antipode. A Radical Journal of Geography, Intervention Symposium – Algorithmic Governance Organised by Jeremy Crampton and Andrea Miller

Amoore, L. (2019) “Introduction: Thinking with Algorithms: Cognition and Computation in the Work of N. Katherine Hayles” Theory Culture & Society 36(2): 3-16

Amoore, L. & Piotukh, V. (2015) “Life beyond big data: governing with little analytics” Economy and Society 44(3): 341-366

Amoore, L. & Piotukh, V. (2016) “Introduction” in *Algorithmic Life. Calculative devices in the age of big data,* Amoore, L. & Piotukh, V. (ed.) (Routledge: New York)

Amoore, L. & Piotukh, V. (2019) “Interview with N. Katherine Hayles” Theory, Culture & Society 36(2): 145-155

Andres, R. B. (2012) “The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence” in *Cyberspace and National Security. Threats, Opportunities, and Power in a Virtual World,* Reveron, D. S. (ed.) (Washington D.C.: Georgetown University Press)

Ansorge, J., T. (2016) *Identify & Sort. How Digital Power Changed World Politics.* (Oxford: Oxford University Press)

Aradau, C. (2017) “Assembling (Non)Knowledge: Security, Law, and Surveillance in a Digital World” International Political Sociology 11: 327-342

Aradau, C. & Blanke, T. (2017) "Governing others: Anomaly and the algorithmc subject of security" European Journal of international Security 3(1): 1-21

Aradau, C., Lobo-Guerrero, L., & Van Munster, R. (2008) "Security, Technologies of Risk, and the Political: Guest Editors' Introduction" Security Dialogue 39(2-3): 147-154

Balzacq, T. & Cavelty, M.D. (2016) "A theory of actor-network for cyber-security" European Journal of international security 1(part 2): 176-198

Barbu, O. (2014) "Advertising, Microtargeting and Social Media" Procedia -Social and Behavioral Sciences 163: 44-49

Bartelson, J. (1995) *A Genealogy of Sovereignty* (Cambridge: Cambridge University Press)

Bartelson, J. (2001) *The Critique of the State* (Cambridge: Cambridge University Press)

Bartelson, J. (2014) *Sovereignty as Symbolic Form* (New York: Routledge)

Benkler, Y., Faris, R. E. L., Roberts, H. S. (2018) *Network propaganda: manipulation, disinformation, and radicalization in American politics* (New York: Oxford University Press)

Betz, D. J. & Stevens, T. (2018) «Analogical reasoning and cyber security" Security Dialogue 44(2): 147-164

Bevir, M. (2011) *The SAGE Handbook of Governance* (London: SAGE Publications Ltd)

Birkbak, A. & Carlsen, H. B. (2016) "The Public and its Algorithms. Comparing and experimenting with calculated publics" in *Algorithmic Life. Calculative devices in the age of big data* Amoore, L. & Piotukh, V. (ed.) (Routledge: New York)

Bohman, J. & William, R. (2017) "Jürgen Habermas" in *The Stanford Encyclopedia of Philosophy* Zalta, E. N. (ed.) (Fall) url: https://plato.stanford.edu/entries/habermas/ (accessed May 7th 2019)

Borgesius F. J. F., Möller, J., Kruikemeier, S., Faathnaigh, R., Irion, K., Dobber,T., Bodo, B., & de Vreese, C. (2018) "Online Political Microtargeting: Promises and Threats for Democracy" Utrecht Law Review 14(1): 82-96

Branch, J. (2011) “Mapping the Sovereign State: Technology, Authority, and Systemic Change” International Organisation 65(Winter): 1-36

Branch, J. (2016) “Geographic Information Systems (GIS) in International Relations” International Organisation 70(Fall): 845-869

Branch, J. (2017) “Territorial Conflict in the Digital Age: Mapping Technologies and Negotiation” International Studies Quarterly 61: 557-569

Branch, J. (Forthcoming) “Spatial Metaphors and the Territorialiszation of Cyberspace, preliminary draft

Brayne, S. (2017) “Big Data Surveillance: The Case of Policing” American Sociological Review 82(5): 977-1008

Bridle, J. (2017) “Something is wrong on the Internet” Medium (url: https://medium.com/@jamesbridle/something-is-wrong-on-the-internet-c39c471271d2, accessed January 30th 2019)

Bridle, J. (2018) *New Dark Age* (London: Verso)

Brodwin, E. (2018) “Here’s the personality test Cambridge Analytica had Facebook users take” Business Insider, published March 19th 2018, url: https://www.businessinsider.com/facebook-personality-test-cambridge-analytica-data-trump-election-2018-3?r=US&IR=T (accessed May 14th 2019)

Brooke, H. (2016) “Inside the Digital Revolution” Journal of International Affairs 70(1): 29-54

Bucci, S. (2012) “Joining Cybercrime and Cyberterrorism: A Likely Scenario” in *Cyberspace and National Security. Threats, Opportunities, and Power in a Virtual World,* Reveron, D. S. (ed.) (Washington D.C.: Georgetown University Press)

Bueger, C. (2015) “Making things known: Epistemic Practices, the United Nations, and the Translation of Piracy” International Political Sociology 9: 1-18

Bui, Q. & Wee, S-L. (2018) “China Rules. How China became a superpower” The New York Times, published November 18th 2018 url:

https://www.nytimes.com/interactive/2018/11/18/world/asia/made-in-china.html (accessed April 22nd 2019)

Butler, J. (1997) *Excitable Speech. A politics of the Performative* (London and New York: Rutledge)

Byman, D. & Wittes, B. (2014) "Reforming the NSA: How to Spy After Snowden" Foreign Affairs 93(3): 127-138

C-Span (2018a) "Facebook CEO Mark Zuckerberg Hearing on Data Privacy and Protection", published April 10th 2018, url: https://www.c-span.org/video/?443543-1/facebook-ceo-mark-zuckerbergtestifies-data-protection&live (accessed Dec 1st 2018)

C-Span (2018c) "Cambridge Analytica and Facebook Data Partners", published June 19th 2018, url: https://www.c-span.org/video/?447132-1/senate-committee-examines-cambridge-analytica-partnership-facebook (accessed February 10th 2019)

C-Span (2018b) "Cambridge Analytica and Data Privacy" Hearing before the U.S. Senate Judiciary Committee on May 16th 2018, url: https://www.c-span.org/video/?445621-1/cambridge-analytica-whistleblower-christopher-wylie-testifies-data-privacy (accessed February 10th 2019)

C-Span (2018d) "Foreign Influence and Social Media" Published September 5th 2018, url: https://www.c-span.org/video/?450990-1/foreign-influence-social-media (accessed February 21st 2019)

Cadwalladr, C. (2018a) "I made Steve Bannon's psychological warfare tool': meet the data war whistleblower" The Guardian, published March 18th 2018, url: https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump (accessed March 7th 2019)

Cadwalladr, C. (2018b) "Exposing Cambridge Analytica: 'It's been exhausting, exhilarating, and slightly terrifying" The Guardian, published September 29th 2018, url: https://www.theguardian.com/membership/2018/sep/29/cambridge-analytica-cadwalladr-observer-facebook-zuckerberg-wylie (accessed May 6th 2019)

Cadwalladr, C. (2019) “A digital gangster destroying democracy: the damning verdict on Faceook” The Guardian, published February 19th 2019, url: https://www.theguardian.com/technology/2019/feb/18/a-digital-gangster-destroying-democracy-the-damning-verdict-on-facebook (accessed May 6th 2019)

Cadwalladr, C. & Graham-Harrison, E. (2018) “Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach” The Guardian, published March 17th 2018, url: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (accessed February 7th 2019)

Cameron, D. (2018) “AggregateIQ Created Cambridge Analytica’s Election Software, and Here’s the Proof” Gizmondo, published March 26th 2018, url: https://gizmodo.com/aggregateiq-created-cambridge-analyticas-election-softw-1824026565 (accessed March 20th 2019)

Carr, M. (2015) “Power Plays in Global Internet Governance” Millennium: Journal of International Studies 43(2): 640-659

Carr, M. (2016) “Public-private partnerships in national cyber-security strategies” International Affairs 92(1): 43-62

C.A.S.E. (2006) “Critical Approaches to Security in Europe: A Networked Manifesto” Security Dialogue 37(4): 443-487

Cavelty, D. M. (2018) “Cybersecurity Meets Science and Technology Studies” Politics and Governance 6(2): 22-30

Chen, S. (2017) “Quantum Internet is 13 years away. Wait, What’s Quantum Internet?” published in Wired, August 15th 2017, url: https://www.wired.com/story/quantum-internet-is-13-years-away-wait-whats-quantum-internet/ (accessed March 3rd 2019)

Christophersen, K. A. (2018) *Introduksjon til statistisk analyse* (Oslo: Gyldendal)

Ciuta, F. (2009) “Security and the problem of context: a hermeneutical critique of securitisation theory” Review of International Studies 35:301-326

Collier, J. (2018) “Cybersecurity Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision” Politics and Governance 6(2): 13-21

Collins (2010) “Collins English Dictionary” url: https://www.collinsdictionary.com/ (accessed May 2nd 2019)

Corry, O. (2012) “Securitisation and ‘Riskification’: Second-order Security and the Politics of Climate Change” Millennium: Journal of International Studies 40(2): 235-258

Cukier, K. & Mayer-Schoenberger, V. (2013) “The Rise of Big Data: How It’s Changing the Way We Think About the World” Foreign Affairs 92(3): 28-40

Curran, T. & Hill, A. P. (2017) “Perfectionism is increasing over time: A meta-analysis of birth cohort differences from 1989 to 2016” Psychological Bulletin. Advance online publication. Available at http://dx.doi.org/10.1037/bul0000138 (accessed February 14th 2019)

Coles-Kemp, L., Ashenden, D. & O’Hara, K. (2018) “Why should I comply? Cybersecurity, the Security of the State and the Insecurity of the Citizen” Politics and Governance 6(2): 41-48

Dahl, R. A. (1963) *Who Governs? Democracy and Power in an American City* (New Haven: Yale University)

Deleuze, G. (1992) “Postscript on the Societies of Control” October 59(Winter): 3-7

DeNardis L. (2014) *The global war for Internet governance.* (New Haven & London: Yale University Press)

Deutsch, K. W. (1966) *The Nerves of Government. Models of Political Communication and Control.* (New York: The Free Press)

Dieter, M. & Gauthier, D. (2019) “On the Politics of Chrono-Design: Capture, Time and the Interface” Theory, Culture & Society 36(2): 61-87

Dunn, K. C. & Neumann, I. B. (2016) *Undertaking Discourse Analysis for Social Research* (Ann Arbor: University of Michigan Press)

Edwards, P. N. (1996) *The Closed World. Computers and the Politics of Discourse in Cold War America* (Cambridge: The MIT Press)

Elden, S. (2013) *The Birth of Territory* (Chicago: University of Chicago Press)

Elbe, S. (2005) “AIDS, Security, Biopolitics” International Relations 19(4): 403-419

Ericson, R. V. & Doyle, A. (2004) “Catastrophe risk, insurance and terrorism” Economy and Society 33(2): 135-173

Fairclough, N. (1992) “Discourse and text: linguistic and intertextual analysis within discourse analysis” Discourse & Society 3(2): 193-217

Fairclough, N. (2013) “Critical discourse analysis and critical policy studies” Critical Policy Studies 7(2): 177-197

Farrell, H. & Schneier, B. (2018) “Common-Knowledge Attacks on Democracy” The Berkman Klein Center for Internet & Society Research Publication Series 2018 7(October): 1-20

Ferguson, A. G. (2017a) *The Rise of Big Data Policing* (New York: NYU Press)

Ferguson, A. G. (2017b) “The Police Are Using Computer Algorithms to Tell if You’re a Threat” Time, url: http://time.com/4966125/police-departments-algorithms-chicago/ (accessed February 20th 2019)

Fioretti, J. (2015) “A German regulator just told Facebook it now has to allow users to use fake names” Business insider, published July 29th 2015, url: https://www.businessinsider.com/r-german-regulator-orders-facebook-to-allow-pseudonyms-2015-7?r=US&IR=T (accessed May 7th 2019)

Foucault, M. (1991) *Discipline and Punish. The Birth of the Prison* (London: Penguin Books)

Foucault, M. (1997) *Society Must be Defended. Lectures at the Collège de France 1975-1976* Bertani, M. & Fontana, A. (ed.) (New York: Picador)

Foucault, M. (2001) *The Hermeneutics of the Subject. Lectures at the Collège de France 1981-1982* Gros, F. (ed.) (New York: Picador)

Foucault, M. (2004) *The Birth of Biopolitics. Lectures at the Collège de France 1978-1979* Senellart, M. (ed.) (New York: Picador)

Foucault, M. (2007) *Security, Territory, Population. Lectures at the Collège de France 1977-1978* Senellart, M. (ed.) (New York: Picador)

Foucault, M. (2012) *On the Government of the Living. Lectures at the Collège de France 1979-1980* Senellart, M. (ed.) (New York: Picador)

Frenkel, S. & Rosenberg, M. (2018) "Facebook Sued by District of Columbia Over Cambridge Analytica" New York Times, Published December 19th 2018 url: https://www.nytimes.com/2018/12/19/technology/dc-sues-facebook-cambridge-analytica.html (Accessed February 21st 2019)

Frisk, A. (2018) "What is Project Maven? The Pentagon AI project Google employees want out of." Global News, published April 5th 2018, url: https://globalnews.ca/news/4125382/google-pentagon-ai-project-maven/ (Accessed March 12th 2019)

Fryer-Biggs, Z. (2018) "Inside the Pentagon's plan to win over Silicon Vally's AI experts" Wired, published December 21st 2018, url: https://www.wired.com/story/inside-the-pentagons-plan-to-win-over-silicon-valleys-ai-experts/ (Accessed March 12th 2019)

Ghosh, S. (2018) "The power players behind Cambridge Analytica have set up a mysterious new data company" Business Insider, published March 21st 2018, url: https://nordic.businessinsider.com/cambridge-analytica-executives-and-mercer-family-launch-emerdata-2018-3?r=UK (accessed March 8th 2019)

Ghoshal, D. (2018) "Mapped: The breathtaking global reach of Cambridge Analytica's parent company" Quarts, published March 28th 2018, url: https://qz.com/1239762/cambridge-analytica-scandal-all-the-countries-where-scl-elections-claims-to-have-worked/ (Accessed March 8th 2019)

Gibson, W. (1984) *Neuromancer.* (London: Gollancz)

Goldsmith, J. & Wu, T. (2006) *Who Controls the Internet? Illusions of a Borderless World* (Oxford: Oxford University Press)

Hacking, I. (1986) “Making up people” in *Reconstructing individualism. Autonomy, Individuality, and the Self in Western Thought*, Heller, T. C, Sosna, M., & Wellebery, D. E. (ed.) (Stanford: Stanford University Press)

Haggerty, D. D. & Ericson, R. V. (2000) “The surveillant assemblage” British Journal of Sociology 51(4): 605-622

Hall, H. K. (2017) “The new voice of America: Countering Foreign Propaganda and Disinformation Act” First Amendment Sudies 51(2): 49-61

Halpern, O. (2014) *Beautiful Data. A History of Vision and Reason since 1945* (Durham & London: Duke University Press)

Halpern, S. (2018) “Cambridge Analytica and the perils of psychographics” The New Yorker, published March 30th 2018, url: https://www.newyorker.com/news/news-desk/cambridge-analytica-and-the-perils-of-psychographics (accessed May 6th 2018)

Han, B.-C. (2015) *Psychopolitics: Neoliberalism and New Technologies of Power* (London: Verso Books)

Haraway, D. (2016) *A Cyborg Manifesto. Science, technology, and socialist-feminism in the late twentieth century* (Minnesota: University of Minnesota Press)

Harvey, D. (2005) *A Brief History of Neoliberalism* (Oxford: Oxford University Press)

Harvey, D. (2007) “Neoliberalism as Creative Destruction” The Annals of the American Academy of Political and Social Science 610(March): 22-44

Hayles, K. N. (2005) *My Mother was a Computer* (Chicago; University of Chicago Press)

Hayles, K. N. (2012) *How We Think: Digital Media and Contemporary Technogenesis* (Chicago: University of Chicago Press)

Hayles, K. N. (2014) “Cognition everywhere; The rise of the cognitive nonconscious and the costs of consciousness” New Literary History 45(2): 199-220

Hayles, K. N. (2016) “Cognitive Assemblages: Technical Agency and Human Interactions” Critical Inquiry 43(Autumn): 32-56

Hayles, K. N. (2017) *Unthought: The Power of the Cognitive Nonconscious* (Chicago: University of Chicago Press)

Hartzog, W. & Richards, N. (2018) "It's time to try something different on internet privacy" The Washington Post, Published December 20th 2018, url: https://www.washingtonpost.com/opinions/its-time-to-try-something-different-on-internet-privacy/2018/12/20/bc1d71c0-0315-11e9-9122-82e98f91ee6f_story.html?noredirect=on&utm_term=.63a5519b3f38 (accessed February 21st 2019)

Hearn, A. (2018) "Cambridge Analytica; how did it turn clicks into votes?" The Guardian, published May 6th 2018, url: https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie (accessed February 20th 2019)

Heawood, J. (2018) "Pseudo-public political speech: Democratic implications of the Cambridge Analytica scandal" Information Polity 23: 429-434

Heery, E. & Noon, M. (2017) *A Dictionary of Human Resource Management (3rd ed.)* (Oxford: Oxford University Press)

Hellevik, O. (2011) *Forskningsmetode i sosiologi og statsvitenskap* (Oslo: Universitetsforlaget)

Hobbes, T. (1998[1642]) *De cive* (Cambridge: Cambridge University Press)

Husserl, E. (1970[1936]) *The Crisis of European Sciences and Transcendental Phenomenology. An Introduction to Phenomenology* translated by Carr, D. (Evanston: Northwestern University Press)

Jackson, P., T. & Nexon, D., H. (1999) "Relations before states: Substance, Process and the Study of World Politics" European Journal of International Relations 5(3): 291-332

John, O. P., Robins, R. W., & Pervin, L. A. (2008) *Handbook of Personality. Theory and Research, 3rd edition* (New York & London: The Guilford Press)

Jorgesen, M. & Phillips, L. J. (2002) *Discourse Analysis as Theory and Method* (London: SAGE Publications)

Joseph, J. (2009) “Governmentality of What? Populations, States, and International Organisations” Global Society 23(4): 413-427

Kahle, L., R. & Chiagouris, L. (ed.) (1997) *Values, Lifestyles, and psychographics* (New Jersey: Lawrence Erlbaum Associates Publishers)

Kitchin, R. (2014) “Big Data, new epistemologies and paradigm shifts” Big Data & Society April-June: 1-2

Kitchin, R. (2015) “The opportunities, challenges and risks of big data for official statistics” Statistical Journal of the IAOS 31: 471-481

Kitchin, R. (2017) “Thinking critically about and researching algorithms” Information, Communication & Society 20(1): 14-29

Kitchin, R. & Dodge, M. (2009) “Software, objects, and home space” Environment and Planning 41:1344-1365

Kitchin, R. & Dodge, M. (2018) “Guest editorial” Environment and Planning 41:1283-1293

KNIME (2019) “About KNIME” url: https://www.knime.com/about (accessed April 5th 2019)

Knorr Cetina, K. (2006) “Objectual practice” in *The Practice Turn in Contemporary Theory* by Schatzki, T. R., Knorr Cetina, K., & Von Savigny, E. (ed.) (London and New York: Routledge)

Knorr Cetina, K. (1999) *Epistemic Cultures* (Cambridge: Harvard University Press)

Koopman, C. (2018) “How Democracy Can Survive Big Data” The New York Times, published March 22 2018, url: https://www.nytimes.com/2018/03/22/opinion/democracy-survive-data.html (accessed May 6th 2019)

Kosoff, M. (2018) “’Cambridge Analytica is just the tip of the iceberg’: Why the privacy crisis is bigger than Facebook” Vanity Fair, Published April 16th 2018, url: https://www.vanityfair.com/news/2018/04/why-the-privacy-crisis-is-bigger-than-facebook (accessed February 21st 2019)

Krahmann, E. (2011) “Beck and beyond: selling security in the world risk society” Review of International Studies 37: 349-372

Krahmann, E. (2018) “The market for ontological security” European Security 27(3): 356-373

Lakoff, G. (1993) “The Contemporary Theory of Metaphor” in *Metaphor and Thought* UC. Berkeley, url: https://escholarship.org/uc/item/54g7j6zh (accessed May 5th 2019)

Lapowsky, I. (2019) “Facebook exposes 87 million users to Cambridge Analytica” Wired, published April 4th 2018, url: https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/ (accessed March 29th 2019)

Latour, B. (2005) *Reassembling the Social. An Introduction to Actor-Network Theory* (Oxford: Oxford University Press)

Law, J. (2012) “The Materials of STS” Oxford Handbooks Online (DOI: 10.1093/oxfordhb/9780199218714.013.0006

Leander, A. (2005) “The Power to construct International Security: On the Significance of Private Military Companies” Milennium – Journal of International Studies 33(3): 803-826

Lemke, T. (2002) “Foucault, Governmentality, and Critique” Rethinking Marxism 14(3): 49-64

Lewis, P. & Hilder, P. (2018) “Leaked: Cambridge Analytica’s blueprint for Trump victory” published March 28th 2018, url: https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory (accessed May 14th 2019)

Libicki, M. C. (2007) *Conquest in Cyberspace. National Security and Information Warfare.* (Cambridge: Cambridge University Press)

Lin, H. (2012) “Operational Considerations in Cyber Attack ad Cyber Exploitation” in *Cyberspace and National Security. Threats, Opportunities, and Power in a Virtual World.* Reveron, D. S. (ed.) (Washington D.C.: Georgetown University Press)

Lin, H. (2016) “Attribution of Malicious Cyber Incidents: From Soup to Nuts” Journal of International Affairs 70(1): 75-138

Locke, J. (1988[1689]) *Two Treatises of Government.* Laslett, P. (ed) (Cambridge: Cambridge University Press)

Luhman, N. (1986) “The Individuality of the Individual: Historical Meanings and Contemporary Problems” in *Reconstructing Individualism. Autonomy, Individuality, and the Self in Western Thought.* Heller, T. C, Sosna, M., & Wellbery, D. E. (ed.) (Stanford: Stanford University Press)

Lury, C. & Day, S. (2019) “Algorithmic Personalization as a Mode of Individuation” Theory, Culture & Society 36(2): 17-37

MacKenzie, D. (2019) “How Algorithms Interact Goffman’s ‘Interaction Order’ in Automated Trading” Theory, Culture & Society 36(2): 39-59

Mayer, J. (2018) “New evidence emerges of Steve Bannon and Cambridge Analytica’s role in Brexit” The New Yorker, published November 17th 2018, url: https://www.newyorker.com/news/news-desk/new-evidence-emerges-of-steve-bannon-and-cambridge-analyticas-role-in-brexit (accessed May 15th 2019)

Manjikian, M. (2018) “Social construction of Technology. How objects acquire meaning in society” in *Technology and World Politics. An Introduction.* McCarthy, D. R. (ed.) (London and New York: Routledge)

Marshall, T. H. (1950) “Citizenship and Social Class” in *Citizenship and social Class and Other Essays* (Cambridge: Cambridge University Press)

Matzner, T. (2019) “The Human Is Dead – Long Live the Algorithm” Human-Algorithmic Ensembles and Liberal Subjectivity” Theory, Culture & Society 36(2): 123-144

Martinez, A. G. (2018) “The noisy fallacies of psychographic targeting” Wired, published March 19th 2018, url: https://www.wired.com/story/the-noisy-fallacies-of-psychographic-targeting/ (accessed May 15th 2019)

McCarthy, D. R. (2018*a*) “Privatising Political Authority: Cybersecurity, Public-Private Partnerships, and the Reproduction of Liberal Political Order” Politics and Governance 6(2): 5-12

McCarthy, D. R. (2018*b*) “Introduction” in *Technology and World Politics. An Introduction*, McCarthy, D. R. (ed.) (London and New York: Routledge)

McCarthy, D. R. (2018*c*) “Critical theory of technology. Design domination and uneven development” in *Technology and World Politics. An Introduction*. McCarthy, D., R. (ed.) (London and New York: Routledge)

Medium (2017) “SCL Group Joins the US State Dept.” Published March 19th 2017 by Medium, url: https://medium.com/textifire/scl-group-joins-the-us-state-dept-ad5cac8155ff (accessed March 6th 2019)

Meyer, J. M. (1986) “Myths of Socialization and of Personality” in *Reconstructing Individualism. Autonomy, Individuality, and the Self in Western Thought.* Heller, T. C., Sosna, M., & Wellbery, D. E. (ed.) (Stanford: Stanford University Press)

Mill, J. S. (2001[1859]) *On Liberty* (Kitchener: Batoche Books)

Mouffe, C. (2005) *On the Political. Thinking in Action* (Abingdon & New York: Routledge)

Mueller, M. (2017) *Will the Internet Fragment?* (Cambridge: Polity Press)

Neate, R. (2018) “Where is Huawei banned from working on critical networks?” The Guardian, Published April 19th 2019, url: https://www.theguardian.com/technology/2019/apr/19/where-huawei-is-banned (accessed April 22nd 2019)

Neumann, I. B. (2002) “Returning Practice to the Linguistic Turn: The Case of Diplomacy” Millennium: Journal of International Studies 31(3): 627-651

Neumann, I. B. (2011) “Entry into international society reconceptualized: the case of Russia” Review of International Studies Association 37: 463-484

Nexon, D. H., & Neumann, I. B. (2018) “Hegemonic-order-theory: a field-theoretic account” European Journal of International Relations 24(3): 662-686

Nietzsche, F. (2008[1887]) *On the Genealogy of Morals* (Oxford: Oxford University Press)

Nix, A. (2016) "The power of big data and psychographics" at the 2016 Concordia Summit, New York. Available online at https://vimeo.com/212373587 (accessed Sept 20th 2018)

O'Grady (2014) "A Politics of Redeployment. Malleable technologies and the localisation of anticipatory calculation" in *Algorithmic Life. Calculative devices in the age of big data,* Amoore, L. & Piotukh, V. (ed.) (London & New York: Routledge)

Ó Tuathail, G. (1996) *Critical Geopolitics. The politics of Writing Global Space* (London: Routledge)

Parisi, L. (2019) "Critical computation: Digital Automata and General Artificial Thinking" Theory, Culture & Society 36(2): 89-121

Peters, J., W. (2018) "Steve Bannon Steps Down From Breitbart Post" New York Times, published January 9th 2018, url: https://www.nytimes.com/2018/01/09/us/politics/steve-bannon-breitbart-trump.html (accessed March 7th 2019)

Porter, C. (2016) "Toward Practical Cyber Counter Deception" Journal of International Affairs 70(1): 161-174

Pouliot, V. (2015) "Practice Tracing" in *Process Tracing. From metaphor to Analytic Tool* Bennett, A. & Checkel, J. T. (ed.) (Cambridge: Cambridge University Press)

Reuters (2018) "Cambridge Analytica files for bankruptcy in the U.S. following Facebook debacle" bulished May 18th 2018, url: https://www.reuters.com/article/us-cambridge-analytica-bankruptcy/cambridge-analytica-files-for-bankruptcy-in-u-s-following-facebook-debacle-idUSKCN1IJ0IS (accessed April 16th 2019)

Rajan, A. (2018) "Data and the threat to democracy" BBC News, published March 19th 2018, url: https://www.bbc.com/news/entertainment-arts-43461779 (accessed May 5th 2019)

Reveron, D. S. (2012) "An Introduction to National Security and Cyberspace" in *Cyberspace and National Security. Threats, Opportunities, and Power in a Virtual World,* Reveron, D. S. (ed.) (Washington D.C.: Georgetown University Press)

Robertson, J. & Baker, S. (2018) "Meet the Psychologist at the Center of Facebook's Data Scandal" Bloomberg, published March 20th 2018, url: https://www.bloomberg.com/news/articles/2018-03-20/meet-the-psychologist-at-the-center-of-facebook-s-data-scandal (accessed March 6th 2019)

Rogers, K. & Kelly, C. (2017) "The Personal is Political" Encyclopædia Britannica, published May 1st 2017, url: https://www.britannica.com/topic/the-personal-is-political (accessed February 21st 2019)

Rose, N., O'Malley, P., & Valverde, M. (2006) "Governmentality" Annual Review of Law and Social Science 2: 83-104

Rosenau, J. N. & Czempiel, E. O. (1992) *Governance without government: order and change in world politics* (Cambridge: Cambridge University Press

Salesforce (2019) "Overview" url: https://www.salesforce.com/products/einstein-analytics/overview/ (accessed April 5th 2019) "Governmentality"

Schatzki, T. R. (2006) "Introduction" in *The Practice Turn in Contemporary Theory* by Schatzki, T. R., Knorr Cetina, K., & Von Savigny, E. (ed.) (London and New York: Routledge)

Schmidtz, D. (2017) "Friedrich Hayek" in *The Stanford Encyclopedia of Philosophy* (Winter) Zalta, E. N. (ed.) url: https://plato.stanford.edu/entries/friedrich-hayek/#JustImpaPoliEntrWithRest (accessed May 7th 2019)

Schneewind, J. B. (1986) "The Use of Autonomy in Ethical Theory" in *Reconstructing Individualism. Autonomy, Individuality, and the Self in Western Thought.* Heller, T. C., Sosna, M., & Wellbery, D. E. (ed.) (Stanford: Stanford University Press)

Scott, M. (2018) "Cambridge Analytica helped 'cheat' Brexit vote and US election, claims whistleblower" Politico, published March 27th 2018, url: https://www.politico.eu/article/cambridge-analytica-chris-wylie-brexit-trump-britain-data-protection-privacy-facebook/ (accessed May 8th 2019)

Sending, O. J. & Neumann, I. B. (2006) "Governance to governmentality: Analyzing NGOs, States, and Power" International Studies Quarterly 50(3): 651-672

Shires, J. (2018) “Enacting Expertise: Ritual and Risk in Cybersecurity” Politics and Governance 6(2): 31-40

Siegelman, W. (2018) “Cambridge Analytica is dead – but its obscure network is alive and well” The Guardian, published May 5th 2018, url: https://www.theguardian.com/uk-news/2018/may/05/cambridge-analytica-scl-group-new-companies-names (accessed March 8th 2019)

Singer, N. (2018) “’Weaponized Ad Technology’: Facebook’s Moneymaker Gets a Critical Eye” New York Times, published August 16th 2018, url: https://www.nytimes.com/2018/08/16/technology/facebook-microtargeting-advertising.html (accessed March 21st 2019)

Skeggs, B. & Yuill, S. (2015) “Capital experimentation with person/a formation: how Facebook’s monetization refigures the relationship between property, personhood and protest” Information, Communication & Society 19(3): 380-396

Skeggs, B. & Yuill, S. (2016) “The methodology of a multi-model project examining how facebook infrastructures social relations” Information, Communication & Society 19(10): 1356-1372

Solon, O. & Laughland, O. (2018) “Cambridge Analytica closing after Facebook data harvesting scandal” The Guardian, published May 2nd 2018, url: https://www.theguardian.com/uk-news/2018/may/02/cambridge-analytica-closing-down-after-facebook-row-reports-say (accessed March 8th 2019)

Sparke, M. B. (2006) “A neoliberal nexus: Economy, security and the biopolitics of citizenship at the border” Political Geography 25: 151-180

Sprenger, F. (2015) *The Politics of Micro-Decisions: Edward Snowden, Net Neutrality, and the Architectures of the Internet* (Lüneburg: Meson Press)

Stevens, T. (2018) “Global Cybersecurity: New Directions in Theory and Methods” Politics and Governance 6(2): 1-4

Stokke, O. S. (2011) “Environmental Security in the Arctic: The Case for Multilevel Governance” International Journal 66(4): 835-848

Strandsbjerg, J. (2012) “Cartopolitics, Geopolitics and Boundaries in the Arctic” Geopolitics 17(4): 818-842

Tarran, B. (2018) “What can we learn from the Facebook-Cambridge Analytica scandal?” Significance June: 4

U.K. House of Commons Digital, Culture, Media and Sport Committee (DCMS) (2018a) “Disinformation and ‘fake news’: Interim Report” Fifth Report Session 2017-19 url: https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/inquiries/parliament-2017/fake-news-17-19/ (accessed April 16th 2019)

U.K. House of Commons Digital, Culture, Media and Sport Committee (DCMS) (2018b) “Disinformation and ‘fake news’: Final Report” Fifth Report Session 2017-19 url: https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/inquiries/parliament-2017/fake-news-17-19/ (accessed April 16th 2019)

Unver, H. A. (2017) “Digital Challenges to democracy: politics of automation, attention, and engagement” Journal of International Affairs 71(1): 127-146

U.S. Congress (2011) “H.R. 3261” url: https://www.congress.gov/bill/112th-congress/house-bill/3261/text (accessed April 22nd 2019)

U.S. Department of Defense (U.S. DoD) (2017) “Project Maven to Deploy Computer Algorithms to War Zone by Year’s End”, published July 21st 2017, url: https://dod.defense.gov/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/ (accessed March 12th 2019)

U.S. Federal Trade Commission (U.S. FTC) (2014) “Data Brokers. A Call for Transparency and Accountability” url: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (accessed May 8th 2019)

U.S. Supreme Court (1976) “Buckley v. Valeo, 424 U.S. 1” Available online: https://supreme.justia.com/cases/federal/us/424/1/ (accessed February 14th 2019)

U.S. Senate Select Committee on Intelligence (SSCI) (2018) “The IRA, Social Media and Political Polarization in the United States, 2012-2018” Computational Propaganda Research Project, url: https://comprop.oii.ox.ac.uk/research/ira-political-polarization/ (accessed April 4th 2019)

U.S. Department of Justice (US DoJ) (2019) “Report On The Investigation Into Russian Interference In The 2016 Presidential Election Volume I of II” (Washington, D.C.)

Verble, J. (2014) “The NSA and Edward Snowden: Surveillance in the 21st century” Computers & Society 44(3): 14-20

Walker, J. (2018) “Facebook makes political advertising ‘transparent’ with information on buyers in UK” PressGazette, published October 16th 2018, url: https://www.pressgazette.co.uk/facebook-political-adverts/ (accessed February 21st 2019)

Wakabayashi, D. & Shane, S. (2018) “Google Will Not Renew Pantagon Contract That Upset Employees” The New York Times, published June 1st 2018, url: https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html (accessed March 3rd 2019)

Watts, C. (2018) “Advanced Persistent Manipulators and Social Media Nationalism. National security in a world of audiences” Aegis Series Paper No. 1812, url: https://www.hoover.org/sites/default/files/research/docs/watts_webreadypdf.pdf (accessed May 6th 2019)

Widiger, T. A. (2015) *The Oxford Handbook of the Five Factor Model* Widiger, T. A. (ed.), Oxford Handbooks Online, url: https://www-oxfordhandbooks-com.ezproxy.uio.no/view/10.1093/oxfordhb/9780199352487.001.0001/oxfordhb-9780199352487 (accessed May 14th 2019)

Wilson, D. G. (2017) “The Ethics of Automated Behavioral Microtargeting” AI Matters (3)3: 56-64

Wong, J., C., Lewis, P. & Davies, H. (2018) “How academic at centre of Facebook scandal tried – and failed – to spin personal data into gold” The Guardian, published April 24th

2018, url: https://www.theguardian.com/news/2018/apr/24/aleksandr-kogan-cambridge-analytica-facebook-data-business-ventures (accessed February 27th 2019)

Yeung, K. (2017) "'Hypernudge': Big Data as a mode of regulation by design" Information, Communication & Society 20(1): 118-136