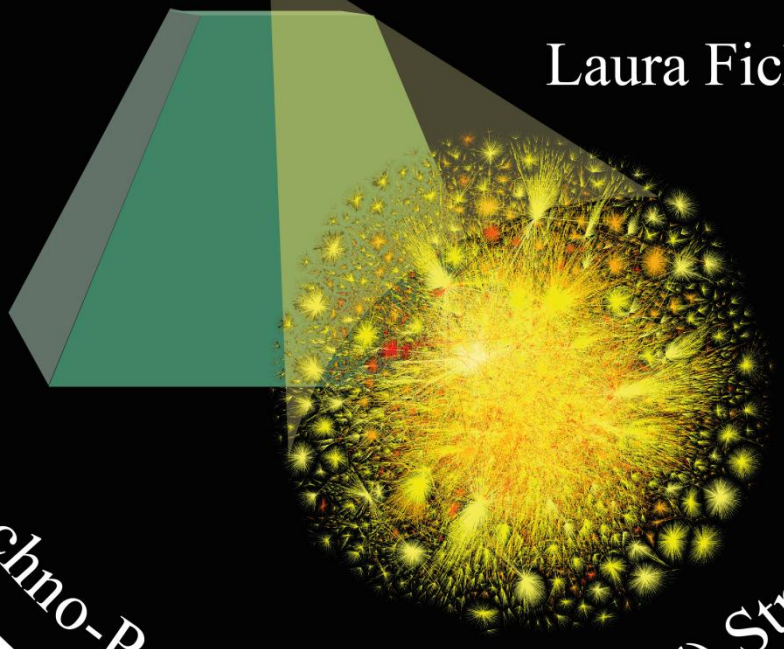
SCIENTIA EST POTENTIA

Laura Fichtner



Techno-Politics as Network(ed) Struggles

Credits for cover images:
The Opte project: http://www.opte.org/
Free under creative commons license for non-commercial use
Picture of NSA headquarters in Fort Meade, Maryland
Under creative commons license:
http://commons.wikimedia.org/wiki/File:National_Security_Agency_headquarters,_Fort_Meade,_Maryland.jpg

For her support for the cover: many thanks to Eva Müller!

Scientia est Potentia:
Techno-Politics as Network(ed) Struggles

Laura Fichtner

Master thesis:

Laura Fichtner, s1346946

Philosophy of Science, Technology and Society (MSc)

University of Twente

Dr. Michael Nagenborg (1st supervisor), Prof. Peter-Paul Verbeek (2nd supervisor)

Date: 09.10.2014

Abstract

Following 2013' summer of surveillance I investigate the technological operation of the NSA's internet surveillance programs Upstream, PRISM and Quantumtheory, which intercept strategically from within the United States. Moreover, I analyze corresponding counter-surveillance technologies. The research results show how internet techno-politics shape the contemporary political landscape. In the techno-politics of surveillance we see how particular technological structures become intrinsic to political forms, because they come with certain social structures. Acting through technological structures, political groups can govern and structure interactions in the way legislation traditionally would. I develop my framework out of the philosophy of pragmatist John Dewey, for whom technological networks and infrastructures played a significant role in politics. However, he still saw technological structures as extrinsic to political forms. I suggest expanding his framework and explore, based on the work of Susan Leigh Star and Geoffrey C. Bowker, how technological infrastructures can become intrinsic to politics. Because they give rise to flows which (re)organize spatial relations in what Manuel Castells has titled the new 'space of flows', different networks embed different socio-political structures. As Alexander Galloway has demonstrated, such structures can be characterized by (different) network diagrams. My empirical research on the operation of surveillance and counter-surveillance technologies shows how the two organize flows on the network differently. The NSA aspires a centralized structure whose hierarchy allows it to control the network; counter-surveillance movements aim at a distributed network with flat hierarchies. The two antagonists are hence opposed in a network struggle. This struggle is possible because the internet consists of different layers with different structures. The NSA operates through the physical layer, where it has a privileged position in a decentralized geography of data flows, while counter-surveillance operates through the distributed protocological layer. It is directed at strengthening protocols which protect from surveillance. Both network types are not inherently democratic, but would need democratic governance from outside. But since they operate through technological activity instead of public discourse, techno-politics happen outside the public's experience and pose a challenge to (Dewian) democracy. The NSA surveillance programs analyzed in this master thesis are particularly problematic, because they govern a global public in the interest of a nation state. They can do so because they have a privileged position in the internet's global geography.

Table of Contents

Chapter 1: Introduction

Not only in surveillance study circles has the summer of 2013 been titled the "summer of surveillance". It attained this glorious title after, in May 2013, former NSA contractor Edward Snowden revealed towards the journalists Laura Poitras, Glen Greenwald and Ewen MacAskill how the US-American *National Security Agency (NSA)* supposedly collects data comprehensively about nearly everybody around the world (Frontline PBS, 2014). Since then, information about sheer uncountable NSA surveillance programs has been published by the media. Many of the programs appear as a continuation of the US program *Total Information Awareness*, created by the Bush administration after September 11, which ran under the (infamous) slogan *Scientia est Potentia*: knowledge is power. Even though the program was officially discharged after a public outcry, we have now found out the NSA carried on with comprehensive data collection under different programs (Horgan, 2013; Poulos, 2013). Until today, publications continue to keep us out of breath – especially since most of the disclosed programs seem not to be only meant for finding members of (US-defined) terroristic organizations. Rather, they seem to aspire to carry out comprehensive surveillance of all communications around the world, those of regular people and those of internationally important persons and organizations. In fact , the NSA seems to be gathering signals intelligence about important international organization like the World Bank, the International Monetary Fund, the European Union and the International Atomic Energy Agency (all of which the US has not defined as terroristic organizations), and possibly even about journalists and human rights activists(Nakashima& Gellman, 2014). On top of this, the agency most likely uses its surveillance capacity to spy on political leaders, some of which are US allies, like the German government, important Israeli politicians and high officials of the EU squad and the head of the Economic Community of West African States. Journalists report in its surveillance efforts, the NSA did not even spare humanitarian "organisations such as the United Nations development programme, the UN's children's charity Unicef and Médecins du Monde, a French organisation that provides doctors and medical volunteers to conflict zones."(Ball & Hopkins, 2013).

Despite the great range of applications the spy programs appear to have, the US government, particularly Barack Obama, suggest the surveillance programs are part of the "War on Terror" and necessary to provide national security (Wall Street Journal, 2014). They emphasize the importance of the programs for providing security for US citizens and its allies. Nevertheless, the disclosures have subsequently caused wide spread concerns about surveillance issues. They stipulated discussions about freedom and security, privacy, international relations, the relation between markets and governments, people's growing dependence on information and communication technologies, the legal framework around surveillance and the trustworthiness of technologies, companies and governments. Citizens around the world were and still are concerned. On the other hand, the

persecution of whistleblower Snowden has furthered discussion on the growing number of leakages and the role of their initiators who make surveillance itself become vulnerable. Snowden's revelations presented a *disruptive moment* in the political discourse and stirred up international dispute. They follow a history of disclosures about NSA surveillance: for example in 2007, whistleblower Mark Klein had told the public about a secret surveillance room the NSA installed in the office of a big internet service provider (Klein, 2007). Still, the revelations and their scope and detail again caught us by surprise. The media attention the case continued to enjoy suddenly (re-)drew our attention to the use of technologies which have become so embedded in our daily routines their inherent potentials often become invisible. Edward Snowden[1] did not only offer us insights into the secret workings of (US') techno-politics, but gave rise to the opportunity to reflect upon the characteristics of the new spaces information technologies and in particular the internet can create. When coming to terms with the disclosures, we at the same time can gain a deeper understanding of the way ICTs structure communities of the globalized world and build hubs and networks.

Such a disruptive moment describes the becoming aware of being surveilled and encourages us to engage actively with the technological structures behind it. The disruptive moment introduces a new, formerly unnoticed, dimension to the technological networks we use and can change our experience of ICT infrastructures like the internet. In their essay *The Face of the Faceless,* Kirstie Ball, MariaLaura Di Domenico and Daniel Nunan (2014) investigated how the surveilled individual comes to terms with the experience of her own identity, her exposure, and also the faceless other, the surveillant, who disappears behind the technology. A scene from the movie *The Life of Others* they recounted described a similar disruptive moment. When explaining how the protagonist struggles with his experience of being surveilled, it is his conscious engagement with the surveillance infrastructure the authors described: "In the scenes where he *rips wires out from behind the wallpaper*, there is a profound sense of his exposure, with his vulnerability, horror and disbelief that even his bathroom and bedroom were bugged." (Ball, Di Domenico & Nunan, 2014, p.4, my italics) It is the confrontation with the *surveillance infrastructure* that introduces the relation between the surveiller and the surveilled, because it provides the interface where the two entities – surveilled and surveiller, face and faceless – enter into a relation. Thus the relation between the self and the surveillant other is experienced through the realization of the underlying infrastructure that connects

[1]A recent article (Bamford, 2014) which came out in the magazine *Wired* and featured an interview with Edward Snowden explained how not all documents and information leaked to the media might have come from Snowden. Other whistleblowers might have used (and still use) Snowden's name as a protection for leaking files and other information to the media. Until now this is all surrounded by secrecy. For the sake of convenience I will from now on assume leaks actually came from Snowden.

the two. Drawing our attention to the underlying technological infrastructure in which surveillance takes place is the power of the disruptive moment:

> Those moments of noticing – however momentary they are – become moments of connection, as the individual realises their place in a much larger infrastructure and notices the identity category to which they are assigned. They signify an involuntary entanglement within the infrastructures which constitute everyday life. (Ball, Di Domenico & Nunan, 2014, p. 17)

But when investigating into the state of surveillance studies I found they often move away from the technological dimensions which structure surveillance politics. For sure, many aspects surrounding comprehensive surveillance technologies transcend mere technological factors rapidly. The threat of terrorism and the wish for security, political aspirations and international relations and the involvement of governments with corporations are not merely technological conditions but developments that take place within broader social transformations. Thus it is not surprising that, even though they emerge from technological conditions, issues of privacy, visibility, cyber threats, vulnerabilities, exposure, enablement and autonomy are often discussed with a focus on concepts of the self or on new social forms and norms. Growing exposure of individuals' private activities leads people to be vulnerable to external forces and in consequence reduces their autonomy (Ball, 2009). It has been argued that control over what others know, the right to privacy, is essential for individual autonomy and for realizing our identities as persons (Solove, 2007; Warner, 2005). In the online world our understanding of identity changes and our presence in the virtual realm builds a major part of it. Participation in the infosphere has become, at least in the Western world, essential for participating in society (Floridi, 2001). Research has shown how exclusion from surveillance mechanisms leads to social marginalization (Hintjens, 2013). Due to these developments it has been argued we live in a *new culture of surveillance* (Pecora, 2002). Not only are we monitored by foreign governments, but also by companies, friends, relatives and colleges, and even by ourselves. There are uncountable parties who establish, with help of technologies, all kinds of different profiles about us.

Thus surveillance technologies provide a point of departure for understanding social and psychological factors which change our experiences. Surveillance seems to develop its own epistemologies and ways of acting in the world (Baijc, 2007). These provide a basis for talking about biopolitics, the excersion of power through visibilities, securitization (Baijc, 2007), transparency as a conscious, social and progressive way to live (Steiner & Veel, 2011), surveillance subjectivities (Ball, 2007), privacy as a societal license which excludes categories of acts from communal, public and governmental scrutiny (Solove, 2007), the essentiality of controlling what others know about one's

self for realizing our identities as persons, one-way communications of symbolic forms (Thompson, 2005), etc. But as the discussion moves on, the specific technologies that bring forth these phenomena often disappear into the background. They appear either as the enabler of new conditions or the medium for pursuing other intentions. In both cases, the technology itself then becomes only the background condition for subsequent discussion. A philosophy of technology aims to make these background conditions visible and bring them back into the focus of active inquiry. It takes a close look at technologies and their intertwinement with human experience and conduct. Technologies are found to be more than just tools but to display agency and carry moral implications. In this thesis, my aim is not to indulge in a discussion over abstract values like privacy and security, but to stay close to the technological structures to which they relate and fill these values with the meaning the material context gives them. The idea is to make the technological structures which guide interaction known and to escape dogmatic appeals. The approach I take reveals what technological structures in particular embed and, as I argue, can make important contributions to our understanding of surveillance[2] politics. In my work, the turn towards technological networks helps me to understand *if* and *how* certain politics operate through technological structures. This enriches our understanding of the transformation of politics, political activism and the experience of politics through the introduction of (new) surveillance technologies.

As both ICTs and surveillance technologies operate as networks, technological infrastructures and networks are the focus of my thesis. Rather than looking at the relation between an individual and a technological artifact, I consider the relation between social and technological structures. Today's dynamics take place within a global network. This network is both a potential threat and a potential point of control. As Cumbers, Routledge and Nativel argue "it is becoming increasingly difficult for ruling elites, usually located at the national scale, to play the gatekeeper role, through traditional territorialized hierarchies, with regard to information and communication flows across space" (Cumbers, Routledge & Nativel, 2008, p. 188). Because flows of communication are not bound to national borders but happen globally, control requires an "'empire' based upon a decentred and deterritorializing apparatus of rule that progressively incorporates the entire global realm – the social movements that emerge to resist it will also be decentred" (Cumbers, Routledge & Nativel, 2008, p. At the same time, there is a "'tendency for networks to create hubs as these provide more stability and robustness. Hubs establish a kind of 'hierarchy' within networks and this in turn gives a certain advantage to key positions of players'" (Cumbers, Routledge & Nativel, 2008, p. 189). We will see how the surveillance network does span the entire global realm, deterritorializing its apparatus of

[2] For me, surveillance is defined as the collecting and monitoring of people's data in order to control their behavior. David Lyon (2001) has suggested a similar defition: "any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered" (p. 2)

rule from the nation state, but it can only do so because the surveillance agency sits on the geographical hubs that emerged within the network, on top of a global hierarchy within the infrastructure. In this hierarchy, the surveilled are located on diffuse ends of the network while the surveillant has access to all information flows and can retrieve data unnoticeable. Thus relations of power, knowledge and control depend on the location within the network. As I find out in my work, power struggles over the network turn out to be struggles over the very network's structure itself. The two antagonists, surveillance technologies, here particularly the NSA surveillance programs, and counter-surveillance technologies and the corresponding movements like the collective Anonymous, are opposed in the way they use internet infrastructures and the way they try to organize the network. Turning towards these structures then makes clear what disputes over internet governance are (also) about – they are about the very technological design of a network. This design shapes how the technology functions, how we experience its use and in which political culture we find ourselves.

When I started my research, my ambition was to inquire into how we experience surveillance politics. I found the issue had not been fully addressed yet. I decided to start developing a tool for analyzing the transformation of political experience through surveillance technologies by filling the 'technological gab' in surveillance research first. This tool helps us explore the context which builds the fundament of this experience and can be used to infer conclusions based on the pragmatist understanding of experience. As a first step, in this paper I develop a notion of *techno-politics* which describes the intertwinement of technological and political issues and structures. I understand the notion as describing a process or activity in which politics are executed through technologies, while at the same time technologies make for certain politics. In the conduct of techno-politics, technological and political developments stand in a reciprocal relationship to the extent that technological forms can be become intrinsic to certain political forms. Techno-politics encompass the politization of technological issues and the technification of political issues: the expansion of technological problems into the political realm and the exercise of political agendas through technological structures. Recent discussions, many of which are centered around control over the internet (i.eg. surveillance, privacy, censorship), exemplify this: the right to internet access and privacy, a recent court ruling on the "right to be forgotten" (European Commission, 2014), the targeting of technological infrastructures for military purposes (cyber warfare), the documentation and publication of war crimes (exemplified by Bradley Manning), the emergence of programming as a form of political activism (hacktivism), and of course the international surveillance scandal Edward Snowden's leaks created. In this work I build on the latter and ask:

> *How do NSA surveillance and their corresponding counter-surveillance technologies, as a form of techno-politics, operate within the internet infrastructure?*

How do these techno-politics transform the contemporary political landscape which shapes our experiences?

In the first part of my thesis I do not talk about surveillance technologies in detail yet, but develop a philosophical framework on which I base my conceptualization of techno-politics and the role of technological structures in political conduct. I base this framework on the thought of American pragmatist John Dewey, who has provided important work on the relation between infrastructures and politics. Especially in his book *The Public and its Problems* (Dewey, 1927) he explored how material dimensions and especially technologies correspond with social practices, politics and democracy. Rather than single artifacts, he considered broader technological networks. It is interesting to see how many of the issues he had been discussing back then still continue to persist today and require to be addressed anew in the case of surveillance technologies. I place his political work within the broader methodology pragmatism provided. My reading of Dewey is inspired by the work of Larry Hickman (2001) and Alfonso Damico (1978). I then propose to expand Dewey's framework by taking a close look at how infrastructures are composed. This provides a methodology for researching surveillance practices and clarifies how techno-politics can be enacted through technological infrastructures. My conceptualization of infrastructures in the third chapter is founded on Susan Leigh Star's and Geoffrey C. Bowker's work on infrastructures and Manuel Castells' space of flows (Castells, 1996; Star & Bowker, 2006). I further explain how the ordering of components within infrastructural spaces can be described by network diagrams, and how these network diagrams can give information about the socio-political structure of the network. This builds on Alexander Galloway's *Protocol* (2004) where he provided an in depth analysis of parts of the internet infrastructure and their structural diagrams. The first part provides a methodology to research the technological practices, concrete surveillance and counter-surveillance technologies, in the fourth chapter.

In the second part of my thesis I dive into specific internet surveillance practices and analyze surveillance and counter-surveillance technologies, making use of the information provided by Edward Snowden and others, foremost the testimony from Mark Klein, a former AT&T technician, back in 2006. This research zooms in on how surveillance and counter-surveillance as techno-politics operate in practice. Due to the scope of this paper and the complexity and amount of the disclosed surveillance programs, I cannot discuss all of them in detail. However, my main concern is how internet surveillance operates in and through technologies and how it can transform the network structurally. To investigate this, some of the most comprehensive NSA internet data collection techniques can already tell us a lot. For understanding the structural operation of techno-politics, we

will see how some of the most significant programs – PRISM, Upstream, Quantumtheory[3] – offer a high explanatory power. I understand this research as empirical because I focus on concrete technological practices and base my analysis on an actual case. The idea is to demonstrate how pragmatism is a fruitful and relevant approach for making sense of the disclosed surveillance programs, while at the same time using the actual practice to expand and adjust the existing framework. In the last chapter I discuss the results of my research and their implications within Dewey's framework. I explore what the research has shown us about the operation of techno-politics, about how political struggles are carried out through struggles in the network, and how this changes our experience of politics.

The results of this research have to be handled with care, however. Not everything media reports should be taken for granted. Many facts are still in dispute and due to high political polarization it is difficult to report impartially. Additionally, because of both secrecy and actuality, there are little academic sources available about the specific case. In my empirical research I therefore had to rely on major news sources and technology websites. While my philosophical and methodological frameworks rely on academic sources, for much of my empirical research I had to consult organization websites and journalistic sources. Most of the information about the surveillance programs was leaked and accessible only to journalists. What speaks for their credibility is the fact that they are classified. But it is not clear how truthful these documents and testimonies are and any claim about them should be understood hypothetically. Even though some of the information might be inaccurate or some of the technologies only hypothetical, the sheer amount of surveillance programs leaked makes me feel something is going on. But the atmosphere of secrecy makes it hard to base a discourse on well-grounded facts. By now, different opposing camps have emerged and the issue has become highly politicized. The incident has again sparked a debate on whether journalism can be or should be impartial (Keller, 2013). Many journalists who report on surveillance issues are also activists. People like Laura Poitras, Glen Greenwald, Kurt Opsahl and Jacob Appelbaum, etc. are not only a computer experts and journalists, but also activists with a clear opinion. Ironically it also seems they are the people best informed about surveillance practices. That said, much of the specific information on the surveillance programs and technologies is everything else but uncontroversial. Some of the technologies might actually exist and work, while others might only be aspired, and yet some might be media hoax. But even though their status is unclear, the general argument of my work is valid. What I do is discuss how different technological forms impact

[3] With its program *PRISM*, the NSA managed to gain access to confidential information about internet users through collaboration with some of the world's biggest service providers like Google, Apple, Microsoft, AOL, Facebook, YouTube and Skype (Greenwald & MacAskill, 2013). The program *Upstream* on the other hand intercepts internet and phone communications through directly intercepting fiber-optic cables (Ball, 2013 a). *Quantumtheory* uses this technology in order to infiltrate and control devices on the internet.

on the social and political structure. My results show a general direction in which things are likely to develop. They should therefore be read as if-clauses: If we assume we have these surveillance technologies (and we have reason to believe so), then this is what it means.

Chapter 2: Pragmatism

To understand and analyze techno-politics requires a conceptualization of how politics, the purposeful organization of human beings in social structures, happen. At the same time it requires an understanding of how technology and its interaction with this purposeful organization can be understood. In this chapter I propose that the philosophical approach of *pragmatism* and the work of John Dewey provide an approach for understanding the techno-politics of internet surveillance. This approach can enrich the current discussion and help us focus on the concrete technological structures at stake. In this section I present my understanding of pragmatism and situate John Dewey's political philosophy within it. This builds the fundament for my subsequent research and provides us with important concepts for situating and interpreting the research results. Now I explain how, for pragmatism, human beings are fundamentally embedded in networks (environmental, social, technological) and how people can consciously shape these networks through technology in order to reach a given purpose.

As we will see, for Dewey politics is mainly concerned with the systematic organization of these structures of interactions which he saw implemented in the *technological forces making for consolidation.* These forces are responsible for bringing about political publics and demarcating political entities such as the state. They can embed undemocratic power structures or be governed democratically by the public. Interestingly for internet techno-politics, these forces of consolidation are embedded in technological infrastructures such as the internet. In the fourth chapter we will see how surveillance and counter-surveillance strategies are occupied with shaping those forces for bringing about a specific social order. In the work following this chapter I will clarify the notion of infrastructure, so important for Dewey's work, and explain how network diagrams and spaces relate to it. These concepts provide us with a methodology to examine the internet infrastructure and surveillance technologies. Falling in line with pragmatisms overall methodology, they provide me with an approach to systematically investigate the technological forces and their shaping – the techno-politics of internet surveillance. In the very last chapter of this paper I then discuss what the research results imply within my political and philosophical framework presented in detail in the present chapter.

As a basis for my practical research, I would like to use this chapter to show how pragmatists have provided a philosophy in which technologies and politics are deeply intertwined. They understand human beings as being intimately connected in a web of interrelations with others and their environment, and technology as the "intelligent techniques" (Hickman, 2001, p. 8) by which the energies flowing through this web are purposefully organized. Consequently, they give a significant role to networks and technological structures and see politics as being occupied with governing the

interactions of people in and through these structures. My understanding of techno-politics bases on this tradition's overall approach and Dewey's political philosophy. In this chapter, I start out with explaining the main features of pragmatism important for me, in dialogue with Hickman's book *Philosophical Tools for Technological Culture: Putting Pragmatism to Work* (2001) and some of Damico's *Individuality and Community* (1978). I introduce the major concepts of pragmatism that relate to techno-politics and explain the central role it gives to technologies within human communities and experiences. This provides a broader framework for understanding the particulars of Dewey's political philosophy, especially with regard to technologies. My exposé draws mainly from the work of John Dewey (1927) and his scholars Larry Hickman (2004) and Alfonso Damico (1978). While Dewey was part of the initiation of the movement in the early 1990's, Hickman, a professor at Southern Illinois University, works on fusing his ideas with a philosophy of technology. I then explain my reading of John Dewey's political work *The Public and its Problems* (1927). This work builds the philosophical foundation for my analysis of surveillance's techno-politics. I describe how John Dewey conceptualized politics and political organizations like institutions and publics, and I position infrastructures as technological structures of interactions in his political thought. From my reading of his work, they can be understood to form the basis for political organization, the emergence of publics and the scope of political actions.

The Pragmatist Framework

The word "pragmatism" itself derives its meaning from the Greek *praxis* which is dialectically opposed to *theoria*:

> Theoria and praxis are two terms used by Aristotle to distinguish between those activities where knowing is an end in itself and those which have as their purpose an understanding of how to live well. The contrast is not between knowing and doing but between practical science, which through knowledge influences conduct, and theoretical science, which stops at knowledge. Praxis also requires theory. To know how to live well demands a reflective and critical understanding of one's purposes and activities. (Damico, 1978, pp. 2-3)

Thus praxis describes the application of knowledge for purpose-directed activities and achievement of the good life, whatever this might mean in particular. Pragmatism as a philosophical discipline is concerned with the role of purposes and consequences in guiding human activity and in shaping human-world relations. It does not state that whatever works most efficient to whatever preconceived end is right, but that any critical reflection should be concerned with *actual conduct* in the world. In this spirit aligns the belief that the discussion of ethical values too is best informed when carried out with a focus on the actual context in which these values work. Context is given a

central role because pragmatists believe the meaning of concepts arises out of their application in practice and their role for guiding human conduct.

The human condition.

For them, the fundamental mode of human life is *action*, which functions as the binding element between an individual and her environment. Anything humans *do* and need to do in order to live and survive, involves bodily activity, motion and manipulation of the environment as well as accommodation to it. From the moment we are born, we need to breathe. This is involves a vivid interaction between our body and the environment. Even an activity as seemingly passive as seeing involves direct contact with a physical medium through which light waves are transmitted. All activity requires the *interaction with* and *connection to* an environment and results in a process of mutual adjustment (Hickman, 2001, pp. 38-39). Individuals become connected to others through interacting in a shared environment that they shape mutually. When individuals interact with the world and meet others, they soon discover they also have common goals and problems, possibly stemming from the interaction itself, and they can collaborate to effectively work on those. *Communities* emerge where human beings not only share an environment, but purposefully interact with each other to realize their conception of the good life. People communicate and corporate in order to achieve new developments. They organize themselves in communities in order to pursue common goals, solve common problems and enhance the well-being of its members. This happens as an ongoing process of adaption in which problems are solved and new ones arise, for example through and by technologies and through and by accommodation to and adjustment of the shared environment (Hickman, 2001, pp. 38-39). From this point of view social interaction is always a fundamentally *experimental* process, guided by the constantly changing conditions of the environment.

Therefore “productive pragmatism calls not so much for a ‘planned’ society as for one that is continually ‘planning’” (Hickman, 2001, p. 61). A community is an organization of people sharing an environment and building *networks of interaction, collaboration and communication* by which shared values are built. In the view of pragmatism, humans are thus deeply embedded in communities and environments with which they co-evolve together (Hickman, 2001, p. 46). In the process of co-evolvement, individuals, communities and environments constantly act upon each other, transforming, adapting and adjusting. Human beings are, to a certain extent, able to conceive of these processes and act upon them consciously. Through communication and information exchange they can purposefully organize and make their endeavors become joint activities. Here we can already anticipate the importance of networks for the pragmatist approach, because they structure interactions and communications. Technological infrastructures are channels of human interaction

through which different flows can happen. As they build the foundation for phenomena of large scale human organization, they give rise to (new) spaces of communication, interaction and exchange: the internet's infrastructure for example enables a virtual world where we can meet 'online'. According to Manuel Castells (1996), these spaces are in our time increasingly structured around different flows. As the case of surveillance and counter-surveillance technologies will show in the fourth chapter, humans can shape those channels to create specific spaces through which given purposes can be reached and society organized in a specific way. As technological structures give rise to interactions (or movements) and to the exchange of goods, they consequently lead to new political phenomena, or political facts, as Dewey called them. For Dewey it is the organizing of the channels, namely the systematic regulation of networks and infrastructures of interactions, with which politics are mainly occupied. Especially infrastructures like the internet transform the channels of human interaction, and also their scope; they lead to new political structures. In the chapter following this one, I propose a way of conceptualizing and investigating these channels and their effects on social structures. This will help us to understand the specific way techno-politics operate in practice (chapter 4).

Technology.

Pragmatism's concept of technology connects to this idea of consciously shaping the channels of human interactions, especially through governing technological infrastructures, in order to reach a given purpose. Technologies play a significant role in pragmatism's account of the human condition: any interaction with the environment, any manipulation of it basically, appears to us as *technological*. The definition of technology Hickman (2001) offers in his book is the following: technology is the "*invention, development, and cognitive deployment of tools and other artifacts, brought to bear on raw material and intermediate stock parts, with a view to the resolution of perceived problems*"(p. 12). He derives this definition from Dewey's characterization of technology: *"'Technology' signifies **all the intelligent techniques** by which the **energies of nature and man** [sic] are **directed and used in satisfaction of human needs**; it cannot be limited to few outer and comparatively mechanical forms*" (quoted by Hickman, 2001, p. 8, italics and emphasis mine). At first sight, these definitions might surprise. In colloquial language it is often (material) tools and artifacts themselves, rather than their employment, which are meant by the word *technology*. For Dewey and Hickman however, technology in the etymological sense of the word characterizes more than this: it is the *cognitive*[4] and novel employment of such tools and artifacts (Hickman, 2001, pp. 16-17). It can

[4] By cognitive employment Hickman refers to an activity which involves deliberation and and concious reflection, inference, on the tools themselves (Hickman, 2001, pp. 15-23). It is an activity in which we direct our attention towards these tools or technqiues in order to examine and influence them so they can function for our purpose. (An example would be learning how to drive a car.) Non-technological activity is then the automated use of the techniques and tools we aquired through technology. (I.eg. after driving for a while, the

be understood as iterative: the tools and artifacts employed by technology are most likely also technologies or at least the outcome of a technological enterprise (Hickman, 2001, p. 47). The employment of tools alone is not yet technology but *technique*. Techniques, in contrast to technologies, can be habituated and automated. For example an experienced typewriter is capable of directly translating thought and speech into text by using the keyboard without having to reason about her use of it – she masters the *technique* of typewriting. Typewriting as a *technology* however involves a *cognitive relationship* to the tool itself, for example the putting together of a typewriter in a new fashion or the apprenticeship of typewriting in which the learner engages consciously and actively with the keyboard and its parts. Generally said, activities which involve reflection and tools are *technological*, activities which involve the automated use of such are merely *technical* and can be said to have reached the status of *habits* (Hickman, 2001, pp.16-17).

According to this definition, technology is a reaction to a 'perceived problem', so to an issue which is considered problematic and prompts the purposeful application of tools with a specific *goal* in mind. This implies to things. First, technologies are only developed *if* people become *aware* of an issue; in negation this means if people are not aware of an issue or the cause of a problem, they will not try to tangle it through the application of technology. Secondly, the important factor is that people *perceive* an issue – this means technology can be a reaction to a real problem or the reaction to a pseudo problem they perceive due to indoctrination, false information or ignorance. Especially in the conduct of techno-politics we will see further on how it is important that issues are perceived, because only then can people correspond to those through purposeful political organization. Politics which operate outside's people's experience or change the channels of interactions secretly are then not subjected to the scrutiny of democratic discourse. In their application, technologies become part of the human-environment relation and the ongoing process of adaption. They can themselves turn out to give rise to new issues which again call for active inquiry, *technology* in a Dewian sense. In this way *technology* is a description of an ongoing process, of a social experiment that puts different entities into a certain relation to each other. Technology is part of the human condition that involves interaction with each other and the environment and is always already there where cognition is purposefully applied. As I show in my thesis, surveillance techno-politics operate through this purposeful application of technological activity, in which they react to new phenomena which arise from technological structures and at the same time, based on extensive knowledge of the internet infrastructure, actively try to shape the channels of interaction in order to achieve their aims.

---

activity itself, switching gears, stirring, accelerating, becomes routinized and automated.) This use becomes automated and habitualized – techniques as the outcome of technology can be embedded in daily routines which we carry out unconciously; they become transparent. These are habits.

Concepts & experiences.

For pragmatists like Dewey, Hickman and Damico, the function of concepts is also technological. Rather than describing an absolute essence or truth, philosophical concepts, including pragmatism itself, are considered tools for an inquiry or investigation. They do not present true meta-physical descriptions of the world but have a function for specific purpose-directed activity. Concepts are not 'discovered', but the outcome of inquiries. They are part of the experimental method at the core of pragmatism (Dewey, 1927, pp. 200 ff.; Hickman, 2001). They arise out of investigations and are subsequently employed in those: they are part of an ongoing process of interaction. The binding element which helps to make sense of the relationship between concepts and activities in pragmatism is *experience*. By relating the meaning of concepts to the actual function they fulfill in guiding activities, pragmatists like Dewey try to overcome the dichotomy between ideas or concepts as mental objects and actions as bodily activity. Instead they see them unified in experience. When one engages in an activity, one interacts with the environment (and/or others) and this interaction results in a particular experience[5]. Through the experience the experienced is also *known*. Before a certain novel activity has been carried out, it is at the same time not known and not experienced. But when one engages in it, the activity becomes an experience and through the experience becomes known. Uncertainty is not only perceived mentally but is a trait of the medium itself. It is inherent to the situation as a whole, in the combination of the experiencer and the experienced, in the lack of a specified relation between the actor and the material. Through the performance of an activity, this uncertainty is resolved by establishing a determined relation between actor and environment. Concepts describe this relation. They are abstractions or analytic tools for making sense of a situation as a "contextual whole" which is part of "an environing experienced world that has a certain dominant character or quality" (Hickman, 2001, p. 21).In the following part of this thesis, I suggest how network diagrams can, in the case of infrastructural networks at least, help to describe the character of such a contextual whole, and consequently the kind of values and social norms it comes with. As I explicate, the internet infrastructure is especially characterized by uncertainty when it comes to its social structure, because its different layers have different traits. Through technological activity on and in the network, techno-politics try to make one layer and its diagram dominant and hence create a space of flows which is signified by their preferred character.

[5] The definition of experience I, following Dewey and Hickman, put forward here is a very particular notion of experience that has nothing to do with our habituated every day experiences. Pragmatism puts an emphasis on (concious) activity – experience too for them is established by a cognitive process in the course of concious activity. Passive experiences which describe the unconcious automated exposure to obscure influences are, for pragmatists, not experiences at all.

So in pragmatism, concepts refer to an interaction with the environment and cannot be understood without such – to observe something or have it explained by someone else, to have an idea of the general properties of the medium, to have had former, similar experiences, etc. And the way something is conceptualized will depend on the way it is known. Thus for Damico, "experience is the result of interaction between organism and environment and […] knowledge […] is the result of some activity" (Damico, 1978, p. 14). Because experience takes place in interaction with the environment, through action it eventually becomes the experience *of* the environment and is shaped by its particulars. Knowledge then involves a reference between the individual and her environment. In an experimental manner, ideas emerge out of experiences and are subjected to test by them. As experimental activities, both experience and knowing are in a constant process of change and refinement. But knowledge also involves directed and deliberate cognitive activity. Ideas and deliberation function in the dealing with an uncertain or problematic situation and inform action and thus experience. By the power of deliberation, experience becomes deeply technological. It is when a new course of action or a new outcome to an action is desired, when there are some unwanted effects to an action that deliberation comes into play in order to find a new way. When deliberation informs a change in action, what it does is actually transform the experience itself. Because a difficulty was perceived in the pursuit of a (desired) action, ideas are the outcomes of deliberative or cognitive activity and emerge from the action in context. Because they help transform the structure of activity in context, ideas also have the power to *reorganize experience* (Damico, 1978, p. 12).In his book on the physical make-up of the internet, author Andrew Blum (2012) for example described how his journalistic inquiry into the internet's infrastructure reorganized his thinking about sending an e-mail and consequently his experience of the net. The disruptive moment Edward Snowden caused can lead to a similar reorganization; learning about surveillance programs can change our experience of the network and consequently our activities online. For example we might start feeling surveilled and be more careful about what we do or say online, or we might start to use encryption technologies. Moreover, we could be inclined to take political measures to influence the network or its governance. In this view technologies may be understood as providing a basis for bringing thinking and doing together, as a place where cognition and activity meet. They are bound up with experience. In this framework, experience is not *perception*, but perception of an uncertain situation leads to conceptualization and eventually to a specific action in which the concepts are tested through experience (Hickman, 2001, p. 29).

Values.

Values as moral concepts are then connected to the specific context in which they function and arise out of experiences. They do not come as manna from the heavens but are part of the social experiment. To clarify this, let me consider the concepts of "individuality" and "community", two of

Dewey's favorite dialectic poles. To speak about individuals and communities is a conceptual tool for understanding phenomena and solving problems, not for discussing a tension between ontological categories. They arise from making sense of experiences within a continuous environment and a specific context and are "not absolutes" (Hickman, 2001, p. 57). In his political work, Dewey describes how he believes the modern ideal of individuality was the outcome of a misguided communitarian politics and emerged from an experimental process in which governments and organized communities were perceived to hamper development (Dewey, 1927, pp. 100 ff). It was the result of a specific experience, the experience of a failed public or state-run organization where authorities came to be associated with oppression and traditions presented obstacles for realizing people's aims (i.eg. technological innovation). So values as concepts have a specific function for describing human activity in context and technological developments influence their meaning. Later on I will argue how we can see a similar context-dependence in the case of "security", a value often called out on to justify surveillance. However, both the surveillance and the counter-surveillance networks incorporate aspects of security – it is only when we become aware of the structural aspects of the networks that we can understand what the value means for our activities in practice.

ICTs.

Information and communication technologies (ICTs), and the internet as their prime example, impact on the way people interact and form communities and on the concepts that make sense of new experiences arising. They can provide whole new platforms that bring people together by providing a space where they can interact and communicate through the exchange of (data) flows. (And because these spaces work through the organization of (data) flows, Manuel Castells' notion of the space of flows will be interesting in the following parts of this work.) The internet offers people a medium upon which they can act, in which they can interact with each other, and which they can shape together. Within a pragmatic framework, ICTs can be seen as building a quasi-environment, a medium that connects people, lets them interact and experience the consequences of other people's actions. At the same time the internet can be employed as a technology when it is consciously influenced, designed and shaped to fulfill a certain purpose. As I discuss in detail in the next chapter, it provides an *infrastructure* through which flows of goods (data, information) are organized and transmitted and in which *spaces* are created. From the interaction within the ICT infrastructure, new communities can form and new problems can arise – at the same time people can use the technological medium to organize and together find solutions to the issues they share. ICTs allow them to establish relations and communities, to exchange information and to communicate. They work as networks not as single artifacts and gain their power through integrating different technologies. What an ICT network particularly does depends on the network type it is and the way it integrates its different – human and non-human – components. Such networks give rise to the

process of mutual manipulation Hickman described. ICTs can be shaped technologically, through the cognitive reflection on the way its components are employed. At the same time, the specific space that is created through this technological activity impacts back on its users, because it structures the way they interact and form communities. In the following chapters I pick up this idea and suggest that this is what surveillance techno-politics are about – they are about the shaping of a network which itself shapes a community in a certain way through regulating the modes of interactions people have. The design of such a network is crucial because the specific environment we interact with and our conceptual understanding of this environment determines our experience.

One of the crucial points I make in my work is that the values we talk about with regard to internet governance should be considered in their relation to the context – the network diagram – they describe. The experience of the modes of interaction that ICTs bring about forms the way we make sense of the concepts we connect to them. An example from surveillance practice can show this. The individualistic or 'customized' character of modern ICTs (i.eg. social networks) makes surveillance on a personal level easy. Through observing the internet activities of individuals, detailed profiles can be constructed and used as means of control. Effectively those technologies can group people and control their behavior. Individuality turns against itself and becomes a means of social cohesion. The internet activist group *Anonymous* with its slogan "we are legion" and the mask as representative for anonymity build a community in which single individuals dissolve. The power they claim for themselves is the power of the "99%", the power of a community as a whole. In a movie they have made about the movement, one member describes how the group enabled him to do things outside the norm (and legal framework), because he could not be identified within the mass (TheAnonMessages, 2013). This displays a paradoxical effect of inversion: community offers its members the freedom to be individuals. It shows how both individuality and community are tools to describe the interaction between people (and their environment) in the pursuit of a desired way of life. When the context changes, the concepts gain a new meaning and can possible reverse themselves.

Dewey's *The Public and its Problems*

The public.

By now I have arrived at the point where I have clarified the basic conceptualization of technology in pragmatism and its relation to the organization of human life and human experience. What is left to do to build an understanding of techno-*politics* is to frame the role and operation of politics, they way they work and their connection to technological structures. Together with the preceding part this provides us with a way of looking at the specific techno-politics of surveillance. It is when people perceive the consequences of interactions mediated by technologies that they start

to form groups which collectively try to cope with those. In a similar fashion, political organizations, institutions and publics come to be. According to Hickman, they are "artifacts created and maintained by human effort. One of the primary tools utilized to create publics is the dissemination of information" (Hickman, 2001, p. 58). Thus they are the conscious organization of individuals as a means to reach a given purpose and to structure community life. In *The Public and its Problems* (1927), his only work dedicated solely to politics, Dewey builds on the pragmatic approach and develops an understanding of politics and their working, mediated by technologies.

Dewey started out his work with going on the search for the political *public*. His aim was to find out what constitutes a public, how it comes about, what its function is and what distinguishes the public from the private. For doing this, he proposed to start with an analysis of political phenomena as they happen, with what he called *political facts*. By starting with an analysis of the internet infrastructure and actual surveillance and counter-surveillance practices, this is what I do in the fourth chapter. Because for Dewey concepts and ideas come out of experience and arise out of the very action their holder is involved in, he suggested not to generalize terms such as 'the state' and to find their essence outside actual political happenings (Dewey, 1927, p. 8). He critiqued classical political philosophy for its preoccupation with finding first causes or principles to the constitution of political phenomena, like a political or social instinct: "To explain the origin of the state by saying that man is a political animal means to travel in a verbal circle. […] Such theories merely reduplicate in a so-called causal force the effects to be accounted for." (Dewey, 1927, p. 9) A political fact is not a neutral objective statement of how things are and always will be, but a description of political phenomena which can be experienced. Political facts are intimately bound up with value judgments since they are *conditioned by human activity* (Dewey, 1927, p. 7). They are the outcome of the conscious ordering of individuals into political communities:

> Political facts are not outside human desire or judgment. Change men's [sic] estimation of the *value* of existing political agencies and forms, and the latter change more or less. […] Modifiable and altering human habits sustain and generate political phenomena." (Dewey, 1927, p. 6)

Because value judgments and desires shape the political landscape and these in turn are in steady process through their interaction with changing environments, political struggle is constantly emerging. This struggle then leads to reflection upon the issues and eventually the discussion of how the state *ought* to be (Dewey, 1927, p. 6).Also in the case of internet surveillance, we later on see such a struggle in form of a network struggle. As I discuss in the last chapter, identifying how the struggle is carried out and how it impacts on the organization of society can then help to reflect on current national politics.

Thus, according to Dewey, any consideration of the nature of political publics should start with a consideration of the facts and consequences of human activity. Consequences are perceived and judged and some of them are desired while others averted. Humans can reflect upon the consequences of their actions and those of others and will be inclined to take measures – to employ technology – for regulating the actions of people within a community. It is by means of the *nature of consequences* and their *regulation* that the distinction between the *public* and the *private* comes about (Dewey, 1927, pp. 12 ff.). A private act is distinguished from a public act by the *scope* of its consequences. When certain activities reach a scope that their consequences systematically and *indirectly* affect others and lead at least to the aspiration of systematically controlling them, the activities reach a public character. Public acts call for a *systematic regulation* of their *indirect* consequences on a broader scope by means of *indirect control of behavior*. Techno-politics aspire to indirectly control behavior, because they aim at shaping the channels of interactions in a specific way.

The demarcation between the public and the private is not sharply drawn – it is a matter of evaluation what can be considered as an indirect consequence. The most accurate definition Dewey gives is that "the essence of the consequences which call a public into being is the fact that they expand beyond those directly engaged in producing them" (Dewey, 1927, p. 27). A public then is a group of people who share an interest in the regulation of activities, because they are mutually affected by and interested in their consequences. It "consists of all those who are affected by the direct consequences of transactions to such an extent that it is deemed necessary to have those consequences systematically cared for." (Dewey, 1927, p. 16) Such a public needs to appoint a range of people who dedicate themselves to taking care of the systematic regulation of human interactions: *officials* (Dewey, 1927, p. 75 ff.). Their function is to represent the interest of a public drawn together by a shared concern around the consequences of certain activities. Concluding, a public needs the following to emerge properly: it needs a systematic organization aimed at regulating a type of activity with indirect consequences, and its needs to do so by indirect means through the establishment of suitable structures and appointment of officials who act on behalf of it (Dewey, 1927, pp. 28-29).

Infrastructures.

Dewey's understanding of politics is placed within pragmatism's overall approach, where people are deeply embedded in an environment and a community, with which they are in a constant process of mutual co-shaping. Purposes are important to understand human engagement in such webs of interactions, because humans have the ability to reflect on their actions and to consequently guide them to reach an intended outcome or to organize together to reach a shared goal. According

to Dewey's work, beyond structuring one-on-one interactions, politics are concerned with the regulation of the systems through which interactions propagate and through which actions and consequences stand in indirect relationships because activities are transmitted over several instances. Technologically, these systems are implemented in infrastructures. This means technological infrastructures and the flow of goods through them played an important role in Dewey's political thought, because he thought of politics as being mainly concerned with regulating the (technological) channels of interactions. For this reason, Manuel Castells' concept of the space of flows, which I explain in the next chapter, is closely related to Dewey's political thought: it describes the formation of a material constellation in which certain social relationships are entertained. For Dewey too, social relationships arise out of interaction in a shared environment that can be seen as a web through which flows are transmitted by channels of interactions. These channels of interactions are implemented in infrastructures through which different goods can flow. Through the flow and exchange of different sorts of goods people can interact with each other and experience the consequences of other people's actions.

So in the emergence of publics and political structures, technological infrastructures and the flows they entertain play an important role. Publics are matters of association and associations work through material manifestations and the exchange of flows through corresponding infrastructures. When people become aware of their associations and perceive consequences following connected activity within them, they reflect on the forms of association and act upon insights they gain (Dewey, 1927, p. 24). Human associations are cognitively reflected upon and consciously shaped. In this process, publics come to be technological enterprises in a Dewian sense. They present the cognitive employment of intelligence to the regulation of perceived consequences through for example the formation of plans, purposes, means, and measures and the purposeful organization of people (Dewey, 1927, p. 34). They are concerned with the implications of infrastructural networks and their flows. They try to regulate and systematically control the way the community interacts with its environment and aim at the conscious shaping of the way actions are translated into consequences and consequences are transmitted over several instances or channels. These translations and transmissions are often performed, mediated or altered by technologies. Perceived consequences – to which publics react – are conditioned by technological structures, because they might for one arise from technologies or their perception might change with the help of technologies (Dewey, 1927, p. 32). Especially ICT infrastructures such as the internet can change the character of former associations, weaken or strengthen them, and function as tools for the formation of new associations, for the translation of actions through new channels and the transmission of their consequences on a new scale. As I demonstrate later on, surveillance techno-politics concerned with ICT networks aim at the political governance of these associations *through* shaping the network.

Therefore Dewey argued that "industry and inventions in technology, for example, create means which alter the modes of associated behavior and which radically change the quantity, character and place of impact of their direct consequences" (Dewey, 1927, p. 30). He held that political institutions which once evolved as response to former modes of association are not apt to adapt timely and adequately to such changes. A new public which emerges around new technological infrastructures and the issues they bring thus "cannot use inherited political agencies" (Dewey, 1927, p. 31) and in a first phase is still quite unorganized and chaotic. Moreover old institutional forms may even stand in the way of coping with the new struggles or support unwanted consequences. The new public needs to "break existing political forms" in possibly even revolutionary manner (Dewey, 1927, p. 31). Such a break can be necessary since many things in the formation of institutions as regulative entities can go wrong – in fact they can become "more harmful than the consequences which they were originally intended to control" (Dewey, 1927, p. 30). These negative consequences themselves bring about the formation of a public directed against them. According to Dewey's understanding thus, the public is more a process than a static entity and changes constantly as the circumstances do. However they too become manifested and institutionalized as their representation takes on material forms in different resources such as buildings, property and funds (Dewey, 1927, p.16). But even though technological structures seem to be fundamentally intertwined with politics, for Dewey the technological changes which alter publics still appeared as "extrinsic of political forms which, once established consist of their own momentum" (Dewey, 1927, p. 30).

If we consider the NSA as an established institution and internet activist groups like Anonymous as a new public that reacts to this intuitional form and deems it inadequate, we can see this struggle in their interactions. It is interesting to note here that their struggle actually happens *through* technology and by technological activity – so by means of techno-politics. I therefore argue, with the support of my empirical observations in chapter 4, we should take Dewey's approach further and understand (techno-)politics not as only reacting to or organizing technological structures of flows and interactions, but as creating a specific social order through the technological employment of structural components. As we can see in the case of the NSA and other secret services, even though institutions might not be adjusted to the new public a new infrastructure brings about, they are still very apt to use the structure for their purposes. It is interesting to see that even though the NSA tries to cling to its traditional power through technological change, it actually uses latest technology to do so. The current political struggles over surveillance (both surveillance and counter-surveillance) might actually imply that in surveillance techno-politics, technology and politics are so intertwined that we can consider technological changes as *intrinsic* to politic forms.

The state.

For Dewey, the systematic organization of a public, and the whole of associations within a given community according to certain central principles, forms a *state* (Dewey, 1927, p. 38). A state's laws have the task to make the enduring and extensive consequences of actions predictable in a way that you know if you do X, Y will happen (Dewey, 1927, p. 56). This implied that obscure legal systems, which work through secret courts like the NSA FISA court[6] and make decisions according to their own internal but concealed logic, are misguided. The structures of the state function as infrastructures: they set out to produce channels along which actions and their consequences proceed, they "canalize action" and form the conditions upon which individuals interact and associate (Dewey, 1927, p. 54). This also means that new infrastructures, canalizing actions differently, can change states and their responsibilities and scope. States are not sharply demarcated from "other forms of social union" (Dewey, 1927, p. 43) and describe "the organization of the public effected through officials for the protection of the interests shared by its members" (Dewey, 1927, p. 33). To distinguish a state from other forms of association happens through demarcation. A family or a village, marked by the direct involvement of its members with each other, is not complex enough an organization to be considered a state. On the other hand, there "are social groups so separated by rivers, seas and mountains, by strange languages and gods, that what one of them does – save in war – has no appreciable consequences for another" (Dewey, 1927, p. 42). Different states take on very different forms throughout time and place. Their formation comes about in an experimental process. In their constitution, technologies and technological infrastructures play a decisive role. As Dewey said,

> the consequences of conjoint behavior differ in kind and in range with changes in "material culture," especially those involved in exchange of raw materials, finished products and above all in technology, in tools, weapons and utensils. These in turn are immediately affected by inventions in means of transit, transportation and intercommunication. (Dewey, 1927, p. 44)

Technological infrastructures transform the state because they influence the way in which associations are made and communities come about. Means of communication and transportation extend the types of interactions possible and the reach of their consequences. They draw together those affected by new complex supply chains and interdependencies (Dewey, 1927, p. 60). Moreover, science and technologies influence the way the world is perceived and what kind of consequences are accounted for. For example, they contribute to the transformation to the secular state, when the will of God is no longer seen as a causal factor in the coming about of events (Dewey,

[6] See for example Opsahl's talk (CCCen, 2013), Levison's testimony (Levision, 2014), and Cain Miller & Perlroth, 2013.

1927, p. 49). Different world views influence the way institutions are structured as to take care of the issues attended to at the time. For these reasons new innovations can trouble the mechanisms of old structures and institutions. Eventually, they can be perceived as breaking old habits and judged negatively by existing authorities. This definition of the state that Dewey has is very flexible and does not refer to the nation states as we know them today.

For Dewey, just as communities and associations change through new technologies, so do state organizations. If state structures function as the political organization of infrastructures, then new infrastructures call for new political forms. But within this framework it is still difficult to conceive of a political organization of a global infrastructure like the internet. Especially institutions like the NSA that emerged from our nation states do in their organization not correspond to these new associations. And even though Dewey saw a problem in the inability of institutions to adjust to the scope of new technological structures, he did not conceive of the possibility of a complex global infrastructure like the internet, which spans the whole globe but can be controlled from a single country. He also did not foreshadow the emergence of global public groups like Anonymous who organizes without living in a shared environment. He still based his idea of democracy on an understanding that saw comprehensive infrastructures and associations within boundaries that can be taken care of by a state. Even though he thought that states must change with technologies, he did not offer a comprehensive framework of how to understand the tension between national and global groups as those which I discuss later on.

Democracy.

For Dewey, a form of state which can be considered a *democratic state* is one which organizes its officials or representatives in a certain way, namely through election by the people who judge them based on their representative skill (Dewey, 1927, p. 82). In their dependence on the will of the people, the democratic election of officials is meant to make sure that they act on behalf of their interests. Officials are supposed to act upon behalf of the public body they represent. Decisions they make out of other reasons, for example personal advantage, are in the strict sense *not political*, even though they might be acted out through institutional channels. Political decisions are those which are made in the interest of the public. From this premises he concludes that states are actually relatively new or maybe rare phenomena, since it seems throughout history decisions in political offices have been made upon reasons of personal or kinship nature (Dewey, 1927, p. 77). Democracy in its political form actually is a response to such misdirected politics and appears as the best political form to regulate human conduct in a way that people mutually benefit and negative consequences are best taken care of. But it is not an absolute and does not present the highest political good. Rather it evolved through the interaction of publics with their governments: “political democracy has

emerged as a kind of net consequence of a vast multitude of responsive adjustments to a vast number of situations, no two of which were alike, but which tended to convert to a common outcome" (Dewey, 1927, p. 84).

These developments were fostered by technologies and infrastructures: "invent the railway, the telegraph, mass manufacture and concentration of population in urban centers, and some form of democratic government is, humanly speaking, inevitable" (Dewey, 1927, p. 100). Through technologies, interactions transcended people's immediate environment and reached a public character. As a consequence, organization on a state level was needed for systematic regulation, as those interactions could not be taken care of anymore within the family or other local communities. This was especially when production started to take place not on a local level but in a complex supply chain over great distances. At the same time information became distributed widely and people could learn about the networks they're implied in and communicate about the issues they share. In this way they assembled into a public, organized, and appointed officials. In order to have their interests represented democratic mechanism became of importance.

Political phenomena and especially publics are hence a response to a change to conditions of community life. This change can be introduced by new technological structures. Technological networks can lead to the sharing of consequences of interactions beyond former community borders (Dewey, 1927, p. 113). This implies that publics emerging around such new technological infrastructures also have to be new in character, as they have no institutionalized or pre-given forms of organizing. Instead, they need to build up those. The internet is such a technological structure because it offers people a new platform to connect (globally), bringing forth a shared environment that concerns people mutually. It also offers them a platform to organize beyond the structures available before. These are the "technological forces making for consolidation" (Dewey, 1927, p. 116) which allow formerly separated communities to now constitute a common public through their interaction and interconnection. In Dewey's framework then, new infrastructures bring about new publics because they come with new issues arising out of new causal relationships and because they bring together new communities or groups. In this way, infrastructures can be superimposed with Dewey's terminology of the technological forces making for consolidation. Politics ought to take care of the structures and to organize and regulate them. In a democracy, this regulation should be exercised by officials who represent the public and act in its interest. Consequently, the technological forces making for consolidation can be seen as the systems which channel flows and through this channeling organize human interactions. The technological systems which make for consolidation are created by and through infrastructures through which goods (finances, information, services, etc.) and people (airline system, railway) can flow. The way these flows are structured then structure

social interactions. Through governing these systems, through regulating their operations, politics aspire to systematically and indirectly control people's behavior and the way they interact with each other.

But when a new global network for example emerges at first, there is no political institution in place that regulates this global network and represents its global public. The question for Dewey is then if the public can become conscious of itself and give people the genuine political experience they need to execute their democratic agency. According to him, spatial separation fails to give people the chance to anticipate the consequences of their actions as they are transmitted through technological infrastructures and obscure the origin of the consequences which they experience (compare Dewey, 1927, p. 130). Interactions are no longer focal, based upon direct contact and face-to-face character, but become indirect and alienating. People can no longer recognize or understand the vast network, that is infrastructure, in which they become employed or make their voices heard. Due to this alienation, even though a "Great Society" – so a vast number of people connected by technological infrastructures, which Dewey believed was in his time "created by steam and electricity" – emerges, people fail to become a community with shared concerns, issues and values (Dewey, 1927, p. 98). After having taken a close look at the network, I discuss this idea further in the last chapter. I argue that such a lack of oversight over the internet can make surveillance seem attractive because it offers a centralized structure and gives people the comforting thought that there is a traditional institution (the state) they know and are experience with and which they can rely on to understand and govern the seemingly anarchistic network. But even though comforting, this form of governance is not democratic, because democracy would – in Dewey's framework – require them to understand and influence *how* it governs. Further, I suggest that understanding how consequences and interactions in the network are structured and organized by political institutions requires looking at the network diagrams of the consolidating techno-structures. Oversight over the network's internal organization is essential for people to understand how communities are organized and how publics correspond. In the fourth chapter I show how this can be done in the case of internet surveillance.

Lack of education or time can be some of the obstacles for laypeople to understand the new concerns which arise out of the workings of complex technological structures (Dewey, 1927, p. 124). Especially when these infrastructures operate outside the experienced space, they are not automatically known through everyday activities but must actively be investigated. To recognize one's interest and the issues at stake, one needs to understand the workings – the diagrams – which channel actions into consequences. This is also important for being able to appoint and judge experts. Another problem to understanding the network is its complexity. As Dewey pointed out,

even if the public organizes itself around one issue, the multiplicity of technical matters that call for political action is so diverse that people cannot overview all what is at stake and hence cannot take the right measures to deal with these systems (Dewey, 1927, p. 135). In the two coming chapters I suggest that thinking about network in terms of infrastructural layers can help tame this complexity. To understand and analyze these networks is necessary to create concepts that describe them and can be publicly discussed. If technological developments take place rapidly and outside the conscious experiences of people, they cannot develop the right concepts to deal with the new forms of life. As Dewey puts it,

> the trouble springs […] from the ideas and absence of ideas in connection with which technological factors operate. Mental and moral beliefs and ideals change more slowly than outward condition. […] Ideals and standards formed without regard to the means by which they are to be achieved and incarnated are bound to be thin and wavering (Dewey, 1927, 141)

Eclipse of the public.

These circumstance lead to an eclipse of the public, as Dewey called it, and impact on the way politics work. The main problem he saw was that people do not become aware of the underlying technological forces that draw them together, so they remain ignorant of the vast space of flows upon which they live. The political structures still control the infrastructures and their flows, and channel the flows of exchanges (information, goods, capital, etc.), fixing "the channels in which non-political, industrialized currents flow" (Dewey, 1927, p. 114). But instead of being appointed and checked upon by its corresponding public, their task becomes the management of vastly distributed populations. For example, institutions like the NSA aim at controlling global networks and thus at organizing a vastly distributed population. However, institutionally, they still correspond to a very different public and do not enjoy the democratic shaping of all those who they concern. In this way, politic actors and institutions, supposed to take care of the public's interests, become alienated. Due to the delocalization of the public, its officials become unknown and exchangeable and elective decisions lose their significance. For secret surveillance agencies, this is even more dangerous because democratic oversight is already low. Political decisions are then made outside democratic frameworks. As an effect politics do not work through democratic publics, but through inertia and power struggles. In the void of the public, the politic stage runs the danger of becoming a farce and leaves governance up to a few powerful forces (Dewey, 1927, p. 136). As political structures no longer work through representation, they maintain support through media campaigns. Either political actors appeal to some sort of general public sentiment ("time-worn slogan", Dewey, 1927, p. 132) or they create "a scare" (Dewey, 1927, p. 135). "Terrorism" for example can act as such a

threatening slogan to be used to justify political activities outside the democratic realm. Public currents are created through the media and flush the masses into one direction or another (Dewey, 1927, p. 122).

Dewey believed that this rather disastrous state of democracy can be overcome if people realize themselves as a public and actively overcome the obstacles which prevent this from happening. Then the public can find ways to deal with the new forms of interaction through scientific-like inquiry into the problems and remedies of its time. This implies that they form a political community and actively create shared values, because community is genuinely moral and must be learned and "emotionally, intellectually, consciously" maintained (Dewey, 1927, p. 151. For this, a functioning system of information and communication, and the creation of symbols through which experiences can successfully be shared and expressed, is required. If we remind ourselves that a public is bound together by shared interaction and interests, it appears logical that the recognition of this implies a system of functioning communication through which people can share experiences so that single experiences turn into a "general will and social consciousness" (Dewey, 1927, p. 153). Internet activist groups like Anonymous (even though they also like to motivate people through slogans) might present the attempt to build such a public: they inquire into the technological conditions that bring forth interactions, they create a system of shared symbols (the mask) and values ("freedom", "security"), they demand information on the workings of political institutions and democratic mechanisms to govern those and they integrate people over distances through the technological network of the internet.

On this note, the open sharing of information and the free flow of communication are of utter importance and needed for the shared inquiry into issues at stake. Secrecy and isolation are poison to democratic structures and fruitful community life: "there can be no public without full publicity in respect to all consequences which concern it. Whatever obstructs and restricts publicity, limits and distorts public opinion and checks and distorts thinking on social affairs" (Dewey, 1927, p. 167). Secret surveillance programs for example hinder the public they concern from finding itself because they obscure they way they influence interactions and the way people are mutually concerned by their techno-politics. But in order to find its interests represented in the politics systematically dealing with technological infrastructures, the public must first realize the workings of the consolidating forces. It becomes a problem when people only anticipate the change technological structures bring to their life, but "do not understand *how* the change has gone on nor *how* it affects their conduct" (Dewey, 1927, p. 165). "For them," he explained, "electricity is *known* by means of the telephones, bells and lights they use, by the generators and magnetos in the automobiles they drive,

by the trolley cars in which they ride" (Dewey, 1927, p. 164). But the underlying technical mechanisms which ultimately govern these applications remain poorly understood.

In the example, electricity is known by the applications through which it can be *experienced* because one directly engages with them. But the underlying structures that bring electricity to these applications remain invisible and outside of experience – only when they become the subject of an inquiry and are openly communicated can they move into the realm of people's experience. In this example we can already anticipate a possibly problematic layering of technological infrastructures that obscures networks of interactions. As a result, people cannot attribute consequences (i.eg. the non-functioning light bulb) to their origins (i.eg. a power blackout miles away) and accordingly not govern those responsibly (power grids). Thus if techno-politics operate on a level outside the experience of people, they cannot be properly understood, conceptualized and checked upon.

In order to provide an active inquiry that can elucidate these technological forces making for consolidation, Dewey believed the codes which govern or should govern scientific conduct should also govern social life – that is free information sharing, interdisciplinary cooperation and careful rational inquiry. Habits – that is automated techniques not reflected upon – are tough obstacles in the adjustment to technological changes and can only be overcome once people know the workings that underlie their life and the conditions on which they operate. To make this easier, problems must not be wrapped in abstract (technical) language, but must be made concrete, must be made able to be experienced. When US government officials for example use words in a way that actually obscures the technological applications they are referring to, it makes it very difficult for people to judge the desirability of technological structures and their implications. In order to support the public however, accurate information and the results of rational inquiries into technical systems should be shared and communicated within a wider audience. Here different media channels such as the press play an important role. They can translate complicated issues into understandable language and reach a broad audience. In the Snowden disclosure, we actually got an idea of how journalistic networks can help to share, explain and disseminate information, and consequently mobilize a public. They took a major part in making people conscious of the surveillance programs and to make clear to them in which hidden networks they are implied.

Power Structures

The present work is part of this process of making conscious the mechanisms which underlie human conduct and inform today's politics, the concrete practices regulated by institutions and through power structures. I propose that a Dewey-inspired account of techno-politics offers a way to deal with the critique that has been leveled against pragmatism, the critique that it does not pay enough credit to power structures which do guide political activity in effect (Hickman, 2001, p. 80).

But if we take Dewey's account further and recognize that technological and political structures do not only react to each other but are *fundamentally* intertwined – so that politics do not only try to cope with the effects of technological structures but actually operate *through* those – an analysis of the technological forces making for consolidation, an analysis of the technological channels which influence human interactions, can lay bare the hidden coercions and social relations that incorporate power structures.

In the coming chapters I make a case that the NSA's surveillance practices present a prime example of such a form of techno-politics and I explain how network diagrams can support us to conceptualize these social structures as embedded in technological networks, and to investigate the power structures surveillance politics exercise. When we investigate into these, we reach awareness of the networks we are implied in and their consequences for our interactions. Edward Snowden contributed to such awareness when he made public the technological mechanisms we are subjected to and the non-democratic power structures that govern them. In Dewey's eyes, such mechanisms hamper democracy and its joint inquiry into problems and remedies of social and technical nature which benefits the community as a whole and its members. Established institutions then fail to represent the public and function for furthering the interests of a few powerful elites. For Dewey, power described the ability to bring forward one's desired end through the interaction with others and the environment and should in democracy lie in the hands of the public. Power *inequality* is then the domination of one group over another group in enacting its interests through the conditions which shape interactions. *Power* thus is the "effective means of operation; ability to execute… It means nothing but the sum of conditions available for bringing the desirable end into existence." (Hildreth, 2009, p. 786) In my work I research on the *underlying effective means of operation* of a technological structure with which techno-politics reach desired ends. This means to ask what the *conditions* are upon which surveillance and counter-surveillance practices are executed and to show how concretely power is *enacted* within the network.

In order to have a genuine political experience, people must become aware of the channels through which politics are enacted and actively engage in shaping them – they must be able to understand and participate in techno-politics. But if policies are secretly carried out, people cannot reach this understanding and do not have the chance to actively participate in the shaping those policies. States then hinder the free development of ideas and exchange of information and consequently impede on the best possible development of society, through excluding the power of democratic inquiry and open discourse. This account is then not unaware of structural aspects of power entrenched in society and the manipulation of social relations to the advantage of the powerful, as critics have accused Dewey of (Hildreth, 2009). As they argue, such social relations have

the capacity to manipulate the 'perceived ends' to which human activity reacts and let power structures work themselves out through *hidden coercions* (Hickman, 2001, p. 80). Reacting to this, I later on show that actually, an inquiry into the technological forces can give us a clearer picture of the ends to which the internet infrastructures works and of the contextual meaning of concepts such as "security" and "freedom" which are used to manipulate perceived ends. Power structures are executed through the (material) channels of interaction, but they are also kept up through cultural values. Pragmatism provides us with a tool to investigate the role of power structures also with its conceptualization of values. In saying "let's see how values function in the organization of interactions within a community", the approach provides us with a tool for checking the validity of old concepts that can be used to maintain power structures culturally through the creation of shared symbols, and to examine their normative functions in the light of new technological developments. It is exactly to ask what the norms of a community imply also in terms of the structural power relations they carry along with. For example Daniel Solove (2007) has criticized the 'you have nothing to fear, if you have nothing to hide' argument, saying it suggests privacy means to hide evil intentions or criminal activities and ignores the fact there might be many reasons why one would want to keep certain things private. For him privacy is a term which denominates a family of issues and gains absolute meaning only in the situation in which it functions. This view is similar to Dewey's approach to investigate the meaning of values as they arise in context.

It is especially a disruptive event like the NSA disclosure that offers a chance to realize these hidden coercions and power structures. Such an event induces a cognitive (technological) reflection upon the tools which we use to carry out our actions and an anew focus on the consolidating technological forces; it gives us a novel political experience. This break challenges us to break with automated habituated techniques and establishes again a cognitive relationship to the technologies we are using. Habits can be vehicles of power since when they are internalized and automated they become invisible and might "arouse devotion without being felt as oppressive or external" (Hildreth, 2009, p. 793). Traditional institutions like the states we have today can be considered as habituated techniques that might require anew reflection and possibly redesign. They might appear incapable to offer a democratic basis for coping with the global character of the new publics ICTs draw together. They do not have the mechanisms and geographical scope to deal with this public and to represent it accordingly. They might even become antagonistic to it. A state surveillance program operating on a global level, especially one which acts on behalf of the interests of a small group of people, does not represent properly the global public drawn together around the shared consequences of technological activity. Following Dewey, one could actually make the claim these states do not anymore function in the way the organization of the state emerged and cannot be democratic since their control is outside the scope of the public they concern in many ways.

I have pointed out the free flow of information, the 'freedom of information' of such special value in the information society, is essential for a democratic system in Dewey's eyes. This makes a normative demand towards politics and asks for political participation of all members of society. But against the allegations of his critics, I believe it is not so that Dewey has to be read as proposing to put all emotions aside and let cold scientific inquiry guide politics (Hickman, 2001, p. 77). What he says is that if we want to understand the networks in which we are implied and consequently the power structures we are subjected to, we should do so by rational inquiry into the conditions through which they are enacted. It is exactly through this inquiry into the material conditions we can understand the issues at stake and then also how our perceived interests might be the outcome of the effective power structure in which we are embedded. This means rather than being subjected to opinion makers, people should have the chance to inquire into the structures underlying their life and reflect upon problems and solutions in a way that is informed by the actual facts of human association. It is opposed to a religious perception not because it takes religion as unimportant, but because it says in the organization of our lives – which is guided by material dimensions – we must deal with matters in a way allowing us to compare all possibilities and choose the one of which everybody benefits best (Hickman, 2001, p. 106 ff.). This inquiry works through the conscious experience of our environment, through reflection upon the modes of activity. It must be technological in the naturalistic sense in which Dewey employs it. It must put forward a cognitive or conscious relation to technological structures, and transcends technique. Only in this way we can actual identify the cause of problematic situations and reflectively come up with new ways of action which suit us better.

Chapter 3: Infrastructures

So far I have explained the pragmatist approach in general and Dewey's understanding of the relation of technological structures to political structures and political publics. The argument I presented went like this: associations are manifested by the interactions of different people in a shared contingent environment. Politics present the attempt to regulate these interactions through governing and shaping of their channels. The channels of interactions become materialized in the infrastructures of growing socio-technical complexes. So if Dewey is right that infrastructures are crucial for the rise of governance issues, it will be important to understand what an infrastructure is and how it works. Dewey himself however did not investigate the structural aspects of infrastructures in his political work. He did not discuss how the specific configuration of an infrastructure comes with specific social structures and political forms (centralization, anarchy, representation), because he believed changes in technological structures would be "extrinsic of political forms" (Dewey, 1927, p. 30). In the techno-politics of surveillance we shall see how particular technological structures can become intrinsic to political forms, because they come with certain social structures and control mechanisms. In techno-politics, technological enterprises can act as a form of governance, structuring interactions, in the way policies and legislation traditionally would. These are important aspects which the present work can add to Dewey's still very relevant political philosophy. I owe this enrichment to Susan Leigh Star's empirical work on infrastructures, Alexander Galloway's analysis of the internet's network diagrams and Manuel Castells' conceptualization of the space of flows, which I introduce in this chapter. These works build the foundation for conceptualizing and investigating, with help of the empirical material Edward Snowden provided, how surveillance techno-politics operate on and in the internet infrastructure, making the consolidating technological forces intrinsic to politics.

In this chapter I now propose a methodology for conceptualizing and analyzing technological structures and their implications – in a way I step into the footsteps of infrastructure analyst Edward Snowden. I describe how infrastructures give rise to new spaces, and how these spaces incorporate certain social structures to be described by network diagrams. This methodology will provide a basis for my inquiry into the internet infrastructure and the operation of surveillance and counter-surveillance technologies. It describes how we can approach the underlying technological forces making for consolidation, the infrastructural environment that draws people together. Hence, in this chapter I clarify what an infrastructure is specifically, how it can be investigated and described by different network diagrams and how it relates to the concept of space. I explain how Susan Leigh Star and Geoffrey C. Bowker (2006) conceptualize infrastructure as that was is riding underneath phenomena of social organization. They can be understood as Dewey's underlying technological forces, and they can embed social norms through standards. But they are not definite but inherently

contingent. For the internet infrastructure, this contingency lies in the different structures its layers display. As Alexander Galloway (2004) proposed, network diagrams can describe the specific communication structure of a given configuration. With the use of network diagrams, we can then shed light on the techno-political struggle being carried out in the network. These different structural configurations build certain spaces, or assemblages. Manuel Castells' (1996) notion of the space of flows then helps me to understand how spaces emerge and how they are transformed by new infrastructures.

Infrastructure

The underneath.

(Technological) infrastructures are the channels of human interaction through which different flows can happen. As such they play an important part in pragmatism's account of the human condition as being fundamentally networked, and especially in Dewey's account of politics. In his view these are concerned with the systematic regulation of networks and channels of interaction. Infrastructures build the substratum upon which human organization functions – spaces of interactions and communications emerge from the use of infrastructural systems. Infrastructures themselves do not yet describe particular spaces with defined social structures, but potential channels which can be shaped to bring about such a space. As my inquiry into surveillance and counter-surveillance technologies will show, the techno-politics of internet surveillance are concerned with shaping a social space by exploiting the potentiality the internet infrastructure comes with. They are concerned with resolving the internet's inherent contingency through technological activity. This allows them to pursue their purpose, because it can embed a dominant character into the space and establish defined power relations. These techno-politics are then technological in the pragmatic sense, because they intelligently employ techniques upon a contingent medium in order to reach a goal. This goal in their case is a specific social structure with specific norms.

The account of infrastructure Susan Leigh Star and Geoffrey C. Bowker have developed in their 2006 essay *How to Infrastructure,* explains how infrastructures are to be understood as inherently contingent. They define infrastructure as that "upon which something else rides, or works" (Star & Bowker, 2006, p. 230). As such it is always "relative to working conditions" (Star & Bowker, 2006, p. 231). Just as it happens with concepts in pragmatism, infrastructure only gets defined by the context and then describes the underlying (technological) structure of a given phenomenon or technological application. The word describes this feature in two parts: *infra* is borrowed from the Latin word for *below* (infra-,n.d.), while *structure* describes a given pattern or shape in which different entities are related and configured (structure, n.d.a; structure, n.d.b). The symbiosis *infrastructure* describes what runs below the operated configuration. Always being

underneath, infrastructure strives to be transparent, invisible and embedded (Star & Bowker, 2006). It seems to be one of its properties to retract itself from our awareness. Infrastructure only calls for active investigation and attention when conditions of usability are altered and prevent smooth use. No wonder then that Dewey felt that the technological consolidating forces, like the electricity grid, are not experienced and known through their applications but only when actively investigated. For him, it is when this investigation takes place that the issues these forces bring are thoroughly understood and political publics can react to them.

While invisible when in use, infrastructures become apparent at a breakdown or when actively investigated or designed. They then stop being a matter of technique – automated use – and call for the application of technology to find a solution to the problem perceived. At the same time, when a part breaks down or stops functioning, its placement in the infrastructural hierarchies draws attention to the larger system in which it is embedded. The architecture of the underlying infrastructure becomes important, as one investigates into the cause of the error along the lines of system-inherent hierarchies. Star and Bowker (2006) illustrated this by the example of a mal-functioning light bulb:

> When the switch fails, we are forced to look more deeply into the cause: first check the light bulb, then the other appliances on the same circuit, then look at the circuit breaker box, then look down the block to see if it is a power outage in the neighbourhood or city, and lastly, depending on one's home repair skills, consider calling an electrician. (p. 230)

The breakdown they describe is similar to the disruptive moment in surveillance techno-politics. The Snowden disclosures have introduced such a breakdown in the sense that they made us realize that the internet infrastructure is not functioning as we believe but that our privacy is gravely violated, our movements monitored and stored, and our devices possibly infected. It made us realize the network of interactions and consequences we are involuntarily and unnoticed part of. As I actually exemplify, a technological investigation into surveillance issues will then demand us to understand the larger network and its organization.

Infrastructures are part of the technological forces making for consolidation, to which Dewey gave a central role in his political philosophy. They describe the *technological ordering* of things, the organization of flows and goods within socio-technical complexes. They function in a similar way as the environment does in the pragmatist framework I described in the beginning. Infrastructure connects people and makes some experience the consequences of others' actions and it puts them in a process of mutual manipulation as they adjust the structure to their needs and accommodate themselves to the structure they use. It is then the *in between,* the interfaces and connections, the

technological ordering of human and non-human bodies, that enable these flows of goods. The internet, as the network of networks, has this inbetweenness literally in its name: the Latin word *inter* is translated as *between* (inter-, n.d.) – the *inter-net* is that which is *in between* different networks. Networks which lack any interface with the broader structure internet cannot meaningfully be said to be *part* of it. Infrastructures and their interface make possible the interaction between and co-action of different parts. Talking about infrastructure means talking about what combines and connects different, possibly categorically distinct, entities, about what makes the socio-technical complexes to be governed (Star & Bowker, 2006, p. 231). In the naturalistic view pragmatism puts forward, all entities are already part of a continuum and embedded in a web of interactions through their environment. Infrastructures then appear as the *conscious*, the technological, ordering of these human and non-human bodies with a certain purpose in mind, the organization of flows of information and goods. If Dewey saw politics as being foremost concerned with this ordering of individuals in communities, and their interaction, through the employment of intelligent techniques on society, then infrastructure should also be inherently political.

Contingency.

Infrastructure describes networks of a plurality of technologies, agents and sub-networks. In a technological enterprise, these can be assembled to create configurations serving certain purposes. Infrastructure is never completely undetermined, because there are certain conditions which have to be fulfilled in order to hook up to the infrastructure. But how the actual emerging configurations look like is contingent and depends on a number of different factors: “the emergent [configuration] itself represents one of a number of possible distributions of tasks and properties between hardware, software and people” (Star & Bowker, 2006, p. 234). Within one infrastructure, a variety of different entities (natural sites, humans, technologies, networks) can connect and communicate in a way that is contingent before it is actually implemented and which can change over time. Configurations are assembled in a technological enterprise and for reaching a certain purpose or establishing a specific social order. Consequently, this enterprise can function as a means of techno-politics. Star and Bowker (2006) referred to these possibilities for techno-politics infrastructures bring. They said that, because of the contingency of the infrastructure and the heterogeneity of its entities, problems emerging in a specific constellation can be solved in different ways – “there might be a political solution to a technical problem and so forth” (Star & Bowker, 2006, p. 234). As I will show in the following chapter, the infrastructure internet does not imply either surveillance or anonymity but potentially allows for both. Techno-political struggles drive on this contingency and are about inscribing a preferred social organization and the corresponding values into the internet infrastructure through both technological design and governance. What the NSA and Anonymous share is the internet as their infrastructure of choice, their object of desire, a tool for pursuing their

political aims and a resource to be employed. Even though the actual configurations they try to achieve differ, there is a shared infrastructure upon which they operate. Because they're ways differ and because these have political implications, they actually become involved in a techno-political struggle.

Standardization.

Standardization functions as a means to deal with contingency and allow many different networks or entities to connect in one infrastructure. Standards and agreed formats for communication are necessary for creating interfaces between different entities and an infrastructure connecting them. They are the tools for establishing communication and building up networks and are necessary to create technological infrastructures through which information can flow. Without standards – agreed rules applying to information transfer – communication would be impossible and the internet could not happen, just as linguistic rules are the precondition for a functioning language. These standards can be considered as the outcomes of the technological enterprise that made a specific infrastructural configuration – and as the result of this enterprise they can then be used without further contemplation, and become techniques. Through using this development for achieving their aims, techno-politics can operate and achieve systematic regulation. In his book on *Weaving the Web*, www-founder Tim Berners-Lee (1999) describes for example how the standardization process for designing the World Wide Web was a techno-political enterprise in which standards were designed in a way that they allow specific – distributed – forms of interactions. But later on, the standards were to be used without further reflection and became invisible to the users.

Because they organize interactions and define what is allowed and what is not, standards incorporate certain social values and types of organizations and exclude others. Because they organize how individuals can relate to each other in a community, they not only incorporate technical but also social norms. On the internet for example, there exist a variety of standards which co-exist and can translate into one another. The standards are very open and operate according to the motto: "be conservative in what you do, be liberal in what you accept" (Galloway, 2004, p. 43). This allows the medium to exhibit great flexibility and heterogeneity – these properties are in turn associated with a specific social norm, namely a democratic social order (Star & Bowker, 2006, p. 241). Thus in the design of infrastructures, ethical, political or social choices and assumptions can be translated into technological dimension (Star & Bowker, 2006, p. 236). They are negotiated through a social discourse and change over time, and they are subjected to techno-politics. This happens in the social experiment Hickman described: in order to create functioning interfaces between humans and technologies, human and technological practices need to adjust and people need to align themselves within certain standards in their practices (Star & Bowker, 2006, p. 238).Because of this power of infrastructures to align both technologies and humans in a certain way, breaking up infrastructures

through a sort of reverse engineering can shed light on the values and social order of a given society. For example, it is astonishing what the content of the telephone book, a technological ordering of individual human beings, can tell one about the values of its society at a close look (Star, 2002). If according to Dewey moral concepts are known by experiencing their meaning in practice, then in the reverse process understanding the conditions of this practice will help understanding the values they embed. This is what I described as the importance of context in the last chapter: knowing how values 'function', so to what purposes they work and which socio-technical configurations they describe, can elucidate their *situational* meaning.

Network Diagrams

Diagrams & flows.

This breaking up of the consolidating forces is the sort of inquiry Dewey called for and which he believed can make us understand the mechanisms we are subjected to and consequently take part in their governance through political publics. When it comes to the analysis of networks, network diagrams are a helpful means to analyze the way these technological forces consolidate modes of interactions and information exchange. The different network diagrams describe different organizational forms of aligning the network's participants and correspond to different social orders. As a remark to avoid further confusion: when speaking about the internet, (inter)action *in* the network can be considered synonymous to *communication* that is information exchange. Flows on the internet are always data flows that establish communication paths between technologies or humans – any interaction on the internet proceeds through establishing a communication and possibly providing or manipulating available information: this includes e-mails, Facebook pages, buying stocks, transferring money, ordering food, blogging, creating websites, and so forth. This is why, later on, I will talk about Manuel Castells' concept of the space of flows: on the internet, flows of all kinds of types (financial, informational, cultural, etc.) are translated into digital information and transmitted through communication paths. Moreover, as I will discuss in the next chapter when talking about internet protocols, participating in the network – interacting with it and its other participants – depends on the access to communication structures through sticking to protocols. Interaction *in* the network is different from action *on* it, which is aimed at changing the network's make-up itself that is its communication *structures* (even though sometimes one can act on the network through acting in it).

So following Alexander Galloway (2004), I propose that network diagrams can describe how infrastructures align people and technologies, that is how interactions in the network are structured, and the type of social order they bring about. Diagrams are a way of depicting the communication structure within network infrastructures or flows of goods within them. Different diagrams have different attributes which influence mechanisms of information exchange, control and reproduction. They provide an accessible way to understand the network properties of a specific configuration as it is created by the way in which its parts are assembled. And from these diagrams then, the technological and contextual meaning of certain social values can be derived – later on this is what I propose to do when speaking for example about freedom and security in the surveillance discourse. In his work *Protocol*, Galloway (2004) has demonstrated how the structural forms according to which different internet layers operate can also be described by (different) network diagrams. They can be understood as a description of the kind of consolidating forces that draw people together, and eventually make them become part of a general public, because they put them in a certain relation to each other and because they determine how interactions are structured and how communication and transmission of flows can happen. As I vividly demonstrate later on with the case of the internet, they can be used to reach certain purposes, for example surveillance and control, or anonymity and resistance against institutionalized power. If we follow Dewey's understanding of power, they incorporate different power structures because they distribute control over information and communication flows differently, express who holds the ability to execute actions in the network (over others) and who has the conditions available for bringing their desired end into existence, possibly overriding other participants' interests. There are many forms of network topologies, but for my (and Galloway's) work there are three significant ones (Figure 1): the *centralized*, the *decentralized* and the *distributed* network.

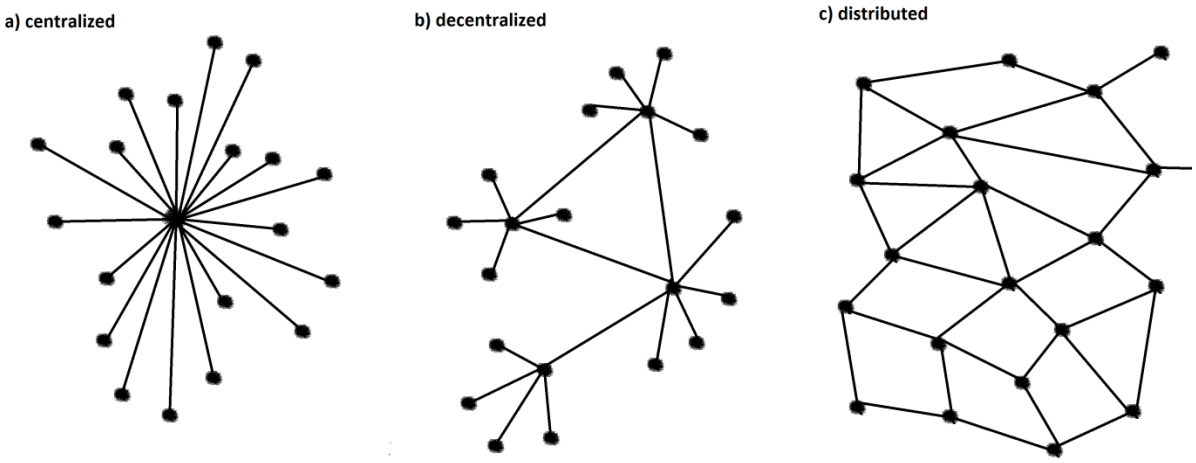


Figure 1: Three network diagrams

Centralized & distributed networks.

A centralized network (a) is a strictly hierarchical structure in which one central hub is linked to all subordinate nodes. Here it is always the top (the hub) which wields power over the bottom (the nodes) and information flows are organized one-directionally from the central hub to its peripheral nodes (Galloway, 2004, p. 30). A decentralized network (b) is the conjunction of several centralized networks. It lacks a single center, but instead consists of the connection of several superordinate hubs which rule over their own group of nodes (while one node may be connected to more than one hub). A distributed network (c) does not have any hierarchical distinction between hubs and nodes; each entity (or node) in the network functions as an autonomous agent and can communicate with any other node without having to consult a central authority (Galloway, 2004, pp. 33 ff.). Galloway described the distinction between the three diagrams as a distinction between the modes of interaction (so the modes of communication) of its different participants: "a distributed network differs from […] centralized and decentralized networks in the arrangement of its internal structure. A centralized network consists of a single central power point (a host), from which are attached radial nodes. […] A decentralized network, on the other hand, has multiple central hosts, each with its own set of satellite nodes. A satellite node may have connectivity with one or more hosts, but not with other nodes. Communication generally travels unidirectional within both centralized and decentralized networks: from the central trunk to the radial leaves. The distributed network is an entirely different matter. […] Each point […entity/node] is neither a central hub nor a satellite node […] each node in a distributed network may establish direct communication with another node, without having to appeal to a hierarchical intermediary." (Galloway, 2004, pp. 11-12) This explains how within the different networks, communication flows and internal power structures are differently organized. In the centralized network, power is condensed in the central hub which controls all nodes and the information flowing to them. As its ultimate representative, Galloway suggested the atomic bomb, certainly one of history's most radical means of techno-politics (Galloway, 2004, p. 29: it condenses power literally in a single nuclear spot from where, upon explosion, it is exercised over the periphery through the shock wave). The decentralized network on the other hand distributes power over several instances which consequently need to cooperate in order to keep the network up, but there are still hierarchical relationships between the different hubs and nodes. The contemporary airline system for example is such a decentralized network (Galloway, 2004, p. 31).

In the distributed network however, no hierarchical power relationships between the different nodes exist and anarchistic information flows occur due to the lack of one or more central authorities. Communication can be established bidirectional between any two nodes over several paths. The internet protocol, enabling peer-to-peer communication over a number of redundant

paths, works according to a distributed network. For understanding political power structures and surveillance politics, these diagrams, describing the organization of data flows through the networks, will be important. Centralized surveillance for example works best on a centralized network, since there is a single node through which all communication must flow and which is thus a perfect point of interception. In a decentralized network however, there is no one hub which communications need to pass; only if one intercepts all the hubs one can gather all communications. In a distributed network, all links or all nodes must be intercepted in order to monitor and control the total information flow through the network. This is because any node can communicate directly with its neighbors or with distant nodes through a high number of possible communication paths. It is the exponential number of possible communications made possible by its link structure which makes data surveillance here a complicated matter. While in the centralized and decentralized network it is enough for total surveillance to intercept at the number of superior hubs, in the distributed network total surveillance needs to intercept in as many places as participants exist. In Figure 1 this would be one point of interception for diagram (a), four for (b) and 20 for (c) with exactly the same number (20) of hubs/nodes within the three networks. The differences between the network structures explain what I mean by a 'techno-political struggle *over* the network': as I find out in my research in the next chapter, different political groups – surveillance and counter-surveillance movements – struggle over the design of the network as either a centralized (surveilled) or decentralized (unsurveilled) network. This struggle is perpetuated by the different properties different layers of the internet infrastructure display. Galloway (2004) exemplified this and used the different diagrams to show the way in which power and control are executed differently within separate layers (IP and DNS) of the internet. Following up on his insights, I find out how different internet layers have different network diagrams, some of which are readily exploited or even created by surveillance technologies, while others provide fertile grounds to counter surveillance.

Internet layers.

This points to an important characteristic of the (internet) infrastructure: its organization into different layers leveled on each other. In the following chapter, when I investigate how surveillance and counter-surveillance technologies operate in and on the internet infrastructure, I describe the significance of the different layers for techno-political practices. I find out that it is this layering that makes the social organization within the internet so contingent and opens up the platform for the techno-political struggle. The internet's contingency comes about because its different layers seem to have different and even opposed organizational diagrams. These correspond to the social structures about which current techno-politics struggle and which are then translated into moral language in the public discourse ("we need security/control" vs. "we need freedom/privacy"). Star described this incoherency as infrastructures having fringes, areas of contingencies that can change

their meaning in context and which are to be found at the edges of stable configurations (Star, 2002); some layers of the infrastructure might favor a certain configuration while others might impede it (Star, 2002, p. 116). Infrastructures can function for different things according to the way they are approached and employed by a certain technological enterprise; the fringes are resolved once it is agreed on a specific form of configuration (and thus social structure). As I demonstrate in this work, the infrastructure internet exhibits such fringes when it comes to networks of distribution and control. Technological hierarchies that allow for centralized surveillance might pose an obstacle to the preferred configuration counter-surveillance movements would like to establish. Therefore the configuration the NSA has in mind is a hierarchical unidirectional flow of communication, while the configuration groups like Anonymous envision is a distributed network of bidirectional peer-to-peer communication. It appears that for the NSA internet means control, surveillance and hierarchy and for Anonymous it means revolution and anarchy. It is not that one of them is right and the other is wrong, rather it is that the internet has contingencies which only gain definite meaning in a certain configuration, so through the use of a specific technological activity. When I say different groups struggle about the 'resource internet' I mean they struggle about how a yet very open infrastructure is to be configured so that incorporates certain practices and values – that the technological forces make for a certain form of consolidation. This is where techno-politics happen.

For my following research, I will make a distinction between three main internet layers: I call them the physical, the protocological and the user interface layer. As I take the pragmatic approach, I differentiate the layers by their function on different levels of organization. The physical layer describes the global internet infrastructure that provides the material substratum for the internet's virtual world, so the technological structure that actually carries, transmits and processes signals as optical or electronic impulses. The user interface layer is the interpretation of this transmitted data so that it can be understood by human beings and displayed on screens, showing the virtual world we can interact with when online (homepages, e-mail programs, etc). The protocological layer mediates between those two levels and describes the set of rules according to which data is to be transmitted, encoded and interpreted. I locate it in between the physical layer and the user interface because its responsibility is to encapsulate data in a way it can be passed on between the two. The *physical layer* thus describes the arrangement of the different tangible things that make the internet work, like servers, routers and cable networks, and the physical signals transmitted by them, like light waves or electronic impulses. The ranges of physical possibilities impact on which functions can technologically be realized and make certain demands as to their constitution and expression. Standards are then necessary for making explicit these demands and enabling interaction within the network. On the internet, standards are needed to create common rules for how to communicate and interact and for realizing a network which assembles all kinds of different entities. This is what

protocological layer does – it describes the standards needed to create interfaces between the different entities on the internet. It describes a set of formal rules which define how different participants can communicate digitally and how data must be rendered in order to be usable on the net. Its most important task is to guide the translation of an executed application or action, like the use of a web browser, into the transmission of signals and vice versa. Whereas the physical layer is concerned with the transmission of physical signals, the protocological layer is concerned with making sense of these in their function as digital signals. Whereas the physical layer is concerned with material interfaces, the protocological layer is concerned with communication rules.

And even though the internet needs its physical support, it is the protocols which *define* the internet. As Tim Berners-Lee (1999) puts it in *Weaving the Web*, the internet's "essence, though, is a set of standardized *protocols* – conventions by which computers send data to each other. The data are transmitted over various carriers, such as telephone lines, cable TV wires, and satellite channels [the old physical layer]. The data can be text, an e-mail message, an image, a software program – whatever [the semantic content]. When a computer is ready to send its data, it uses special software to break the data into packets that will conform to the […] Internet protocols that govern how packets will be shipped". (p. 18) Protocols are at the heart of the internet because, by defining rules for how data can be packed and exchanged, they make possible what the internet was meant for: enabling communication between all kinds of different networks and devices and of all kinds of different forms of information – as such they shaped our experience of the internet significantly. Thus the protocols are used to mediate the functions performed by the third layer, the *user interface layer*. This layer refers to the particular applications which users experience and interact with, like desktop surfaces, e-mail programs, browser web pages or YouTube videos. The user interface layer gives semantic content to information transmitted over the internet and actually makes it valuable for human users. While the protocological layer ought to find a way for communication to be established, and the physical layer a way for signals to be transmitted, the user interface finally displays signals as signs and formats information in a way understandable to the human senses. For most of us, the user interface layer will define how we experience the technology, or the internet, because it is the layer which we engage with and which offers us a tool to interact on the internet. In my framework, conceptualizations arise out of experiences and experiences come out of activities. This implies the way the function of the user interface layer is structured, and the way it lets us interact and establish social relations, will determine the kind space we experience and the way we conceptualize the technology.

The infrastructural layering of the internet plays an important part in the constitution of the experience of surveillance techno-politics, which I will outline in the last section of my thesis. This

layering is similar to Dewey's electricity example and Star and Bowker's light bulb. Dewey claimed electricity is 'known' by the applications (so the user interface layer) one experiences and engages with (light bulbs, telephones), because that is how pragmatists believe that knowledge about things is generated, namely through experience and engagement. But the broader structure, the consolidating forces (the grid) – the deeper, encompassing, encoding layer – remains hidden underneath and outside the scope of people's experience. The underlying structure is only experienced once one is forced to engage with deeper layers due to some sort of disruptive moment (disclosure, breakdown). The internet might not be any different from how Dewey described electricity: he said people may feel the changes which new technologies bring to their life, due to the consequences they experience, but would often "not understand *how* the change has gone on nor *how* it affects their conduct" (Dewey, 1927, p. 165). This is because the underlying technological infrastructures upon which the applications operate remain invisible. But if there is a hidden centralized structure through which dragnet surveillance creates a monopoly position for certain parties, this makes the internet a whole different socio-political network than if it is this space of free information and anarchistic communication flows often experienced on the user interface layer. Consequently, the impacts of such a network would only be perceived in terms of their consequences, but the consolidating forces which bring them about would not be experienced let alone understood (by the public). If state surveillance institutions operate on a layer outside people's experience – and through this even change the infrastructure's properties – then techno-politics operate outside people's experience and knowledge. This in turn has (negative) implications for the experience of techno-politics and especially for making the political judgments which, according to Dewey, democracy demands from people.

Security.

Because the term security plays a central role in the public discourse about surveillance, it should here be mentioned the different network diagrams I talked about all incorporate a specific kind of security. Pragmatism holds that the meaning of values can only be understood in connection to the specific context and social structure they function in and when one knows which kind of activities they describe. Through experience we 'learn' the meaning of values by engaging with their particular context. For pragmatism, values are relational properties that describe certain relations: *something* is good *for* something. Using terms such as "security" and "freedom" can be confusing, and meaningless, when applied outside the context and specific network form they correspond to. Security does not per se imply control or surveillance, and it does not by necessity imply a centralized network[7]. Security can also exist in a distributed network: this actually is the idea of network security.

[7] As we shall see in the section explaining the distributed protocological layer of the internet, the whole idea of creating the internet as a distributed network was to provide security, in the first place.

Thus, as a contextual value, the meaning of "security" differs in different contexts and networks. To play the dispute between the distributed and the centralized network out as a dialectical opposition of freedom and security, as it is often done in the public discourse, is misleading. Both diagrams – both organizational forms – come with threats and securities.

On the one hand, having a major control hub in a centralized network can protect the network better from certain threats, as it overseas its unity. Centralization can offer national security and use wiretapped information to defend a nation from a threat, possibly a cyber threat (Brey, 207). Through controlling communications globally, a central surveillance institution on top of such a network can provide a kind of cyber security which protects from threats that might be actualized outside the network but emerge out of its use, such as communications of violent groups (Nissenbaum, 2005, p. 64). Additionally, the centralized network can protect from a viral threat which can propagate and spread through the myriad of paths in the distributed network. It offers its members the freedom to live free from constant fear of the danger from within. On the other hand, the centralized network comes with the threat of a police state, of power abuse and of losing of autonomy[8]. Additionally, the centralized network is not very secure, and even less resilient, when it comes to centralized attacks. Due to the nodes' dependency on the central hub, any attack on it would shutter the whole network and destroy functional communication. It would at the same time target all nodes and leave them back in chaos, vulnerable to exploitation and external force. The distributed network on the other hand offers its members freedom from hierarchical control and surveillance; it can protect from dragnet surveillance or the control through a single power hub. It therefore can provide what Nissenbaum termed "technical computer security" which provides privacy and keeps up the integrity of devices, preventing for example attacks, possibly carried out by an agency like the NSA, from breaking in (Nissenbaum, 2005, p. 63). It offers them the freedom to act as equal and autonomous units within an environment of other equals. Moreover, the distributed network can diminish the effects central attacks can have, because the network does not depend on a central organizing authority and can recover and grow organically. But it also comes with the threat of an attack that shutters the system from within, through a distributed or even viral form of attack, propagating through the network's myriad of interconnections and causing system failure from within.

[8] Of course, autonomy as a concept is also ambigous and must, for a pragmatist, depend on specific context, too. In this thesis however I do not discuss different notions of autonomy. When I speak about the distributed network as offering autonomy, I imply that participants are not dependent on the control of a central authority. In the distributed network, new nodes can hook up at any point and without asking for permission and any two nodes can communicate with each other without having to ask for authorization. But there are still protocological rules which restrict the freedom of network participants, because they define what one can and cannot do. If a node does not compy with the protcological rules it simply cannot participate in the network and is forced to idleness.

The dialectical opposition of security and freedom, which has characterized the public debate on surveillance, is hence misleading in the sense that both network types provide a certain contextual freedom and come with a certain contextual threat. Both are in a way concerned with security. The major concern of the NSA is national security, as its priority is to protect the US from eventual (foreign) threats. The major concern of counter-surveillance is network security which protects the distributed network and the autonomy of its individual nodes. The context-dependence of security should still be kept in mind, because it helps us understand why the current techno-political struggle is not necessary a struggle between freedom and security, but between network diagrams. The internet's different layers build the condition for this struggle, because they offer the potential for creating both a centralized and a distributed diagram. Helen Nissenbaum has argued specific conceptualizations of security lead to different technological designs (Nissenbaum, 2005). Especially for infrastructures, this design influences the social structure in which we find ourselves and the way we interact. Inversely, looking at how the system is set up supports understanding its social norms. Because security is such a context-dependent term, the focus of this thesis is not on security, but on the specific network structures through which surveillance and counter-surveillance politics work. For future research, the results can then be used to provide contextual meaning and inform the public and academic debate.

Space of Flows

The notion of space.

The internet's different layers and their respective social structures can be conceptualized as different *spaces*, a notion sociologist Manuel Castells (1996) expanded on in his chapter on *the space of flows* in his work on *The Rise of the Network Society*. In analogy to infrastructural layers, spaces consist of interfaces with other spaces, plugging into a greater infrastructure. Functioning as pragmatic conceptualizations, they are looked at through a lens defined by the specific phenomenon one is interested in and depend on the type of relation inquired. How one will locate and analyze a space will depend on the type of question they ask and the type of inquiry they perform. When asking which kind of space the internet as a whole creates one will look for a certain interface – the one where on- and offline depart – and then analyze the internal structures demarcated by this boundary, while the question I am asking, namely which different spaces surveillance and counter-surveillance technologies create *within* the internet, leads me to look for a difference in their modus operandi and in the social relations which the configurations make for. Spaces ride on infrastructures and can be created through the purposeful use of technologies within them. The different diagrams we have seen above describe different spaces as they give an account of the way material

configurations guide societies by functioning for specific social relationships, or time-sharing practices as Castells (1996) called them.

Spaces describe particular configurations. Today, so Manuel Castells claimed, we find ourselves in a very specific type of space in which flows (and their socio-technical structures) become *the* defining element of societies. In this space of flows, places (geographical locations) do not vanish, but relations between them are transformed through the way these flows are structured. Castells (1996) exemplified this by showing new networks which connect global cities, but disconnect other maybe spatially closer areas which do not participate in the flows. To foreclose – the internet builds such a space of flows where spatial relations are transformed. This transformation comes with a tension: the internet's different infrastructural layers make for different types of spaces. While its protocols are aimed at structuring flows so that location becomes irrelevant as long as one is connected, the physical layer comes with major intersection points that have implications for political geography. Both layers however incorporate mechanisms of control but structure flows differently. Network diagrams help us to describe those structures and their mechanisms. Because they come with different social structures, the network struggle of surveillance techno-politics is about creating a dominant layer and hence a specific political space. By transforming, abstracting and virtualizing flows into digital data streams, ICT infrastructures in general can be seen as prime examples of the space of flows. And if we read Dewey's political work with a focus on his conceptualization of infrastructures and their role in structuring human conduct, we can come to the conclusion he already anticipated the importance of flows and their channels Castells would pick up in his work.

According to Castells, a *space* describes "a material product, in relationship to other material products – including people – who engage in […] social relationships that provide space with a form, a function and a social meaning" (Castells, 1996, p. 411). It is "the material support of time-sharing practices (Castells, 1996, p. 411). As a material *product* space is the outcome of an activity that created a specific configuration of different material entities. It is made through activity and could purposefully be created through a technological enterprise. Moreover, space is intimately bound to social practices and human relationships. It gains its form, function and social meaning through the social relationships it establishes and entertains. It is for this reason Castells said "space is not a reflection of society, it is its expression. In other words: space is not a photocopy of society, it is society" (Castells, 1996, p. 410). In this passage he pointed out how space and social relations are intertwined and together make up a society. Social relations cannot happen independently of space, while space cannot be established without social relations. I find this interesting for two reasons. First, it falls in line with Dewey's understanding of society as being made up by material connections

– he believed societies were created by a shared material environment in which people interconnected and interacted. Secondly, this interdependency of the material product and its social relationships reminds of the ongoing process of adaption in which Dewey and Hickman saw human beings and their environment constantly involved. While space (the material product) shapes the social relationships it entertains, human activity can change this material product at the same time and hence influence the constitution of a space.

Network diagrams as abstract spaces.

The different network diagrams can be understood as describing (and visualizing) the properties of certain spaces. They describe how a material product – a network – is configured and how the social relationships inside the network are structured. They can thus describe the function and form of a space. If the social relationships a certain type of space entertains are understood, this understanding could be used to exploit the space's properties and to strengthen the space and hence support its social structure. At the same time, through actively creating a space, one could influence social relationships. As we shall see in the empirical part of this thesis, it is these possibilities that make techno-politics, and surveillance politics, so attractive: a technological enterprise on the network can lead to a certain space, a certain configuration, which in turn leads to a certain socio-political structure. As spaces arises out of how a shared material environment that puts people into a relationship with each other, different network diagrams then describe different kinds of spaces. And if the different layers of the internet have different diagrams, and as I will show they do, the internet then consists of different spaces, with different properties and social relationships, leveled on each other. The notion of space can hence be used to describe the layer we experience – the experienced space – and the layers that remain underneath – the hidden spaces. The different spaces layered on each other together build the whole of the internet infrastructure. This entails that disruptive moments like Snowden's act of whistle blowing have the power to change the experienced space and consequently influence the political discourse. Such disruptive moments draw our attention to underlying infrastructural layers and open up the scope of social relationships we experience. Because spaces as conceptualizations depend on the way they are looked at, and because, in pragmatism, conceptualizations happen through experiences, a disruptive moment crucially transforms the space we experience and changes our view on the network's socio-political relationships.

Space & place.

The concept of space is hence different to the concept of *place* which describes a geographical or physical locale whose properties are "self-contained within the boundaries of physical contiguity" (Castells, 1996, p. 423). This means a place is determined by geographical location and boundaries. It can be understood as a sort of container and, in contrast to space, does

not change if the social relationships and practices inside the container change. But, as I argue, *space* and *place* are not independent entities, instead they are interrelated. Castells already argued how the space of flows still has significant places, but that flows can *reorganize* geographic relations. When we talk about the internet's physical layer, we can see how its hubs build their very own geography on the global map and hence transcended spatial relations. This has implications for Places can be thought of as part of the infrastructural allocation underlying the emergence of specific spaces. Even in the case of (governing) a global internet, where geographical location ought to be become less important over time, place still matters very much. In the next chapter I show how, within the internet's physical layer, geographical locations and configurations support the emergence of specific spaces corresponding to centralized network diagrams. As such, geographical locations within the physical layer co-determine social structures and their power relations because they can give advantage to key positions.

In the NSA programs, place has a distinct role to play. Because the servers of the companies NSA collaborated with were physically located on US territory they had such easy access to data in their program PRISM. Moreover, because many important internet hubs outside the US are located on the soil of their allies, they could run extensive surveillance programs together with foreign agencies. It is significant how PRISM slides leaked by Edward Snowden contain maps and references to places such as countries and continents, as shown in the example below (Figure 2). Even on the internet, places still do matter and it is part of this thesis to investigate their role in the creation of the new techno-political spaces of the surveillance society. As I will show, they are crucial for organizing a hierarchical organization of data flows, which is why they play such a great part for surveillance. Counter-surveillance programs, like the Tor network, on the other hand work through confusing physical boundaries to reduce the significance of places in order to both fight surveillance and strengthen the distributed network. On top of this, places are also important for understanding the implications techno-politics have for democracy and the emergence of political publics. If a network draws people distributed over the globe together in a shared environment of interactions and consequences and consequently into a common public, but this network is then controlled and governed from a specific place, that is a single state, which has democratic legitimization only from its citizens and whose institutions are governed on a national level and supposed to take care only of the concerns of its own citizens, then it cannot be said to correspond, in a democratic sense, to the global public it governs.

Figure 2: NSA slide showing the significance of places for the PRISM program

The space of flows.

According to Castells, the information age creates a new type of space he calls the space of flows. For him, different flows – be they financial, informational, organizational, technological, symbolic or else – are *the* structuring element of today's societies. They are the "purposeful, repetitive, programmable sequence of exchange and interaction between physically disjointed positions held by social actors in the economic, political, and symbolic structures of society" (Castells, 1996, p. 412). But actually, for Dewey flows were already the defining element for society and politics. He believed that societies changed through new technological infrastructures that extended and changed the scope of flows, and he believed that politics and publics happen as a responds to these new structures and mainly aim at the systematic regulation of these structures (even though he believed institutions weren't so good at it anymore). And infrastructures exactly organize these flows of goods between people and let them interact through acting on the flows they then transmit. Additionally, Dewey believed flows of information and shared symbols were necessary for the public to become aware of itself, to communicate and to organize politically. What Dewey did not talk about explicitly though, was the possibility to shape the technological structures in a certain way in order to *achieve* political goals or structures (for him, technological structures came first and then politics responded to them). But Castells said, flows are the "purposeful, repetitive, programmable

sequence of exchange and interaction" which means they can a) be employed for a certain purpose and b) they can be influenced and shaped – programmed – in order to do so: this is techno-politics.

But when Castells said that the space of flows lets "physically disjointed" actors interact, he did not talk about the whole internet. Just because different communities on the internet are often scattered around the globe and do not live in the same place, this does not mean they are physically disjointed. The physical layer of the internet infrastructure combines different actors into one network because it physically joins them and, even though they might be in quite remote places, puts them into one shared network of interaction. It is a crucial characteristic of the internet's physical layer's technologies to create physical joints between different places, emancipating the emerging spaces from local or national boundaries. The internet is not a way to describe a physically disjointed community – something impossible in pragmatism anyways – but it is a material technological infrastructure capable of *overcoming* former physical separation. Nevertheless, on the internet, the physical layer only transmits data flows, sending physical streams around the globe, but the protocological layer ought to determine how it does so and ought to organize the structures of the flows; these can be detached from places. Network diagrams help to understand the organization of spaces around flows, because they depict the hierarchical relationships to which flows between nodes are subjected. Comparing these with geographical borders can offer valuable clues about the role of place and geographical location. Thinking in terms of flows offers a (pragmatic) tool for understanding the altered landscape of global techno-politics. The notion of flow is a good way of capturing the dynamics transforming this landscape. For example, recent political developments, be they in Turkey, the US, UK, Syria, Somalia or India, have shown an essential struggle for political actors, aiming to maintain or gain power, is the control over data flows through the internet and to the people.

According to Manuel Castells, the space of flows consists itself of three layers. Due to his different approach, these layers differ slightly from my way of layering, but they do correspond. The first layer corresponds to what I have coined the physical layer and describes the collection of technologies, technological structures and interfaces which provide the material support for the creation of spaces with distinct properties and communities. It describes the internet's infrastructural components (Castells, 1996, p. 412). The layer's reach and boundaries can define the scope of networked spaces "like railways defined 'economic regions' and 'national markets' in the industrial economy" (Castells, 1996, p. 413). The second layer basically describes the outcome of a technological ordering of these components and emerges from the organization of the networks' parts into the hubs and nodes. It is this ordering, network diagrams express. Because they should prescribe the rules according to which data can flow between the network's participants, this

ordering of the network's participants should be expressed in its standards and protocols. So the layer describes how the components become "hierarchically organized according to their relative weight in the network. But such hierarchy may change depending upon the evolution of activities processed through the network" (Castells, 1996, p. 413). In the case of the internet, its hierarchical order depends on the activities performed in the network (i.eg. techno-politics) and by the functions of its hubs and nodes, and can be influenced by activities both on the physical and on the protocological layer, as I explain in the next chapter. For example, on the PRISM slide above (Figure 2) the US was defined as the "world's telecommunication backbone". But the creation of another big telecommunication backbone avoiding US soil could weaken this position on the network. Castells' third layer then articulates techno-political power relations expressed in the second layer and the governing of the network from outside. It describes "the spatial organization of the dominant managerial elites" (Castells, 1996, p. 415). The elites consist of the rich and powerful decision makers who – so Castells – are not themselves situated within the flows but control them from the outside. As he says,

> the elites do not want and cannot become flows themselves, if they are to preserve their social cohesion, develop the set of rules and the cultural codes by they can understand each other and dominate the others […] the real social domination stems from the fact that cultural codes are embedded in the social structure in such a way that the possession of these codes opens access to the power structure without the elite needing to conspire to bar to its networks […] the space of flows is made up of personal micro-networks that project their interests in functional macro-networks throughout the global set of interactions in the space of flows. (Castells, 1996, p. 416)

As we shall see later on, the NSA tries to put itself in such an elitist position by creating a centralized network on top of the distributed network the internet protocols create. By aiming at a unidirectional information flow, it at the same time stays outside the internet's regular space of flows. Instead, it tries to control the space of distributed flows and its participants from outside and without participating in it – and in the best case it would like to do so in secret.

Surveillant Assemblage

Kevin Haggerty and Richard Ericson (2000) proposed the notion of *surveillant assemblage* to describe how the space of flows translates into a surveillance space and how the surveillant and the surveilled are related to each other. They derived the notion of *assemblage* from Gilles Deleuze and Félix Guattari who used it to describe the concert of a *multiplicity* of different entities, themselves consisting of assemblages in a sort of eternal loop (Haggerty & Ericson, 2000, p. 608). What connects these different entities of sub-assemblages into one single, shared assemblage is their functional

incorporation into a working system. In this sense, the notion of assemblage is reminiscent of Dewey's notion of the technological forces making for consolidation. The emergence of political publics as a response to these forces then seems to correspond to the power of assemblages to introduce "breaks and divisions into otherwise free-flowing phenomena" (Haggerty & Ericsson, 2000, p. 608). Assemblages describe spaces as the organization of technologies and bodies into certain configurations and allow distinctions between them by differentiating their working conditions. To function for surveillance and control, assemblages need to incorporate certain functions that can capture and compare data flows in order to make use of them, fixing them in time and space. When surveilljng, the surveillant needs to abstract "human bodies from their territorial settings and [separate] them into a series of discrete flows. These flows are then reassembled into distinct 'data doubles' [that is the data representation of the surveilled] which can be scrutinized and targeted for intervention", so which can then be used to systematically surveil and process information (Haggerty & Ericson, 2000, p. 606). In order to unravel their functions fully, surveillant assemblages need to create a specific type of network, one in which centers and hierarchies exist where the captured multiplicity of flows can be collected and compared, and used to exert control on the network and subordinate nodes (Haggerty & Ericson, 2000, p. 613-614).

But just as we can conceive of *surveillant assemblages* we can conceive of *counter-surveillant assemblages*. It is only when an assemblage takes on a specific form that it becomes a surveillant assemblage – assemblages are made in a technological enterprise in which different raw parts are put a relation and which can serve specific ends. Haggerty and Ericson acknowledged this contingency. For them, assemblages work through "potentiality, one that resides at the intersections of various media that can be connected for diverse purposes" (Haggerty & Ericson, 2000, 609). That means they arise out resolving of an inherent contingency, which they call potentiality. I have proposed the internet as infrastructure holds such a potentiality, which is aimed to be resolved by techno-political struggles. In the next chapter I give practical examples of how this happens. The surveillant assemblage helps us to understand how surveillance is not a matter of a specific technology or technological application, but emerges from the formation of a surveillance space, of a specific network, through the interfacial integration of different bodies and technologies into a functioning whole. Assemblage is then a pragmatic notion, looking at the function or activity a system performs. The assemblage we will find depends on the function we are looking for (i.eg. surveillance). Whatever our functional point of entry is will give us the assemblage as the whole performing the function. In the following chapter I will go on the empirical search for both the surveillant and the counter-surveillant assemblage. The material collection of entities underlying a certain manifested assemblage – the potentiality – is the infrastructure. Because new comprehensive surveillance unfolds its power by the sheer number of communication channels it controls, the

surveillance society works through the interconnection, comparison and integration of different distinct data flows into a surveillant assemblage. Its central focus lies on the control of infrastructure as a whole. In this sense techno-political struggles about the internet are power struggles about controlling the internet not as a technology but as a resource.

Chapter 4: Internet Surveillance

In this chapter I research and analyze how techno-politics *operate* in practice, how surveillance and counter-surveillance politics are *done*. I start out with an analysis of 'political facts', political phenomena as they happen in practice. I show how NSA surveillance and counter-surveillance technologies operate as a form of techno-politics, because they organize the channels of human interaction in a specific way and strive to systematically regulate the structures of interactions and communications, and how they do so by technologically acting in and on the network. As I argue, they are concerned with organizing infrastructures in order to systematically bring about a specific social structure – they actively shape the technological forces of consolidation. They do so by exploiting and operating the internet's infrastructural layers differently. This research answers to my research question of how surveillance and counter-surveillance techno-politics operate within the internet infrastructure. In the following chapter I subsequently discuss what the results of this investigation tell us about the operation of techno-politics and their democratic legitimization. But before this, I now examine *the operation of surveillance and counter-surveillance technologies* within the internet's infrastructural layering.

As I show, the inquiry into the concrete technological forces elucidates which structural diagrams are at the basis of the surveillant and the counter-surveillant assemblage and consequently how they structure interactions between the network's participants. We will see how the internet's different layers, which are at the heart of its contingency, follow different structural diagrams; both parties aim at making a specific social structure prevalent by strengthening the corresponding layer. This explains why there can exist both comprehensive surveillance programs, such as executed by institutions like the NSA, which manage to create huge databases with information about each one of us, while at the same time there a plurality of groups, like Anonymous and the Chaos Computer Club, who escape those mechanisms successfully and operate anonymously. These phenomena show how the internet's contingency gives rise to a new form of politics – surveillance techno-politics. To see how surveillance happens technologically is crucial for understanding how political aspirations are – often invisibly – translated into technological infrastructures and how technologies and politics co-shape each other. The insights provide a basis for understanding how techno-politics work in the case of internet surveillance. With the tools Dewey's political philosophy has provided us with, this understanding can in turn help us to evaluate the implications surveillance techno-politics have on the current political structure, and their democratic justification.

In this chapter I specifically look at what I have defined as the internet's first and second layer, as this is where surveillance and counter-surveillance technologies mainly operate. The first layer I titled the physical layer. I use it to describe the material implementation of the internet, its

physical structure which connects devices, cables, routers, exchange points, etc. and through which data can flow in form of signals. We will see how this layer, by the way components are jointed and physical data flows happen, developed to build a decentralized network. Through setting rules for communication flows, the second, protocological layer then operates the physical layer in a specific way and aims at organizing the internet's components into a distributed network. I explain how it does so by logically assigning the same weight to all nodes in the network and by letting information hop from router to router throughout the network. My third layer, the user interface layer, will not be a main part of my analysis of techno-political practices. It is mainly responsible for bringing about the experience of the network we can have when using an end device. It should be kept in mind that it can both make invisible or visible certain structures: for example, with a chat program we would have the experience of finding ourselves in a distributed peer-to-peer communication situation. We would not recognize however how on their way our communications flow through certain hubs on the physical layer and get copied and fed into NSA servers.

The Internet's Physical Layer

In June 2013, Edward Snowden's revelations to the public made us conscious of at least some of the comprehensive surveillance programs the NSA appears to be executing. In their aftermath the most commonly heard names were *Upstream* and *PRISM*, two data collection programs run by the US' secret agency. Both collect vast amounts of internet traffic but appear to differ in their methodology. According to the leaked information, PRISM cooperates with big US internet companies like Facebook and Google to gain access to information stored on their servers and data about users and their activities (Greenwald & MacAskill, 2013). Such information can contain pretty much anything which the companies store or process such as e-mails, search requests, websites visited and cookie information. How the NSA can get to this data, either by direct access to the servers, secretly or in cooperation with the companies, as Guardian-verified NSA slides claim, or if the companies only hand them over once a legal request has been issued, cannot be said with confidence (Miller, 2013; Rushe & Ball, 2013). In their other big surveillance program called Upstream, the NSA seems to collect internet traffic directly from the cables and intersection points of the internet's backbone infrastructure. What it does is sit on major internet traffic hubs and passively collect and analyze data as it is flowing by (Ball, 2013 a). One of the leaked slides shows both programs and their distinctions (see Figure 3).

On the slide it is interesting to see – in a truly infrastructural way – what lies underneath the graphic. The background of the slide shows a map of North America, depicting the undersea cable networks which connect the US to the globe and the location of the ISPs with whom the NSA is likely to cooperate. But why does the map appear of such importance? Another leaked slide provides an

answer and tells NSA employees why they can expect most data will flow through interception points on US soil: because it will take the cheapest, not the physically most direct path (The Washington Post, 2013). In the language of the internet, cheaper means a higher bandwidth available – therefore the very same slide shows the bandwidth of every intercontinental cable connection. Because the cables connecting Europe and the US and the US and Asia both offer a greater bandwidth and are cheaper than a lower bandwidth direct connection between Europe and Asia, a communication between the two might not pass through a direct cable but via an intersection point in the United States. So apparently, the NSA slides themselves already reveal which layer is most important for their surveillance programs, namely the layer that organizes the flows of physical data signals, the physical layer. It is the layer which creates the physical joints upon which the dynamics of internet traffic can unfold and Castells' space of flows enables sequences "of exchange and interaction between [seemingly] physically disjointed […] social actors" (Castells, 1996, p. 412). The physical layer attaches the internet to places and gives rise to NSA's geopolitical advantage on the network. Its structure plays a crucial role for global dragnet surveillance.

Figure 3: NSA slide explaining the programs Upstream and PRISM

Internet geography.

The physical layer is so important here because it determines the traits of the internet's geography. In his description of the new space of flows, Castells (1996) pointed out how places are still important because they host hubs in which flows come together. In the introduction I said networks have the tendency to build hubs, and as I am about to find out, it is the internet's physical layer where these can be found. The hubs are important to understand the structure of the internet's physical data flows – this structure is crucial to the NSA's surveillance. The internet's physical structure transforms global geographic relations and makes it possible for a national agency to act upon the global network, performing global surveillance. Hence it embeds certain power relations in a network that makes people around the globe part of the shared environment. Because this possibility influences the reach and responsibility of a nation state's institution, and because these new consolidating forces draw together a different (global) public than before, the geography the internet's physical layer creates has implications for the political justification of an institution like the NSA. As we shall discover later on, counter-surveillance technologies are actually keen to weaken the position certain (national) players have on the physical layer and try to create a distributed network which can make location become irrelevant. But before getting to these points, let us first find out how the internet's physical layer is structured and how this structure supports surveillance techno-politics.

A company called TeleGeography has dedicated itself to mapping the internet's data flows and the underlying physical structures since 1989 and sells those as customized maps, compiling the desired information well-arranged and visually appealing. What they do is collect data about internet traffic with help of a computer program called *Traceroute* and information they receive from various internet providers (Blum, 2012, p. 31). They use the collected data to compile maps showing the geography of the internet's data flows. Their map in Figure 4 depicts the global network connections in 2012 – the thickness of the connecting lines represent bandwidth (the thicker, they higher the bandwidth) and the numbers rank cities according to their share of global internet capacity (the number 1 is connected to the most capacity). As we can see, cities in Europe, London Frankfurt, Paris and Amsterdam, build some of the major internet hubs, providing high capacity connections and high internet traffic throughput. But already from rank five US cities, especially New York, Miami, Los Angeles, Washington and San Francisco, also provide internet major hubs. The map is a tool for identifying the routes most communications take. For example, most data arriving in the US from Europe comes from intersection points in Paris and London, but not from those in Frankfurt and Amsterdam, and reaches the continent in New York and Washington, but not in Miami which rather functions as the intersection point for connection to the South American continent. The map does not order cables and their bandwidths according to the geographical location, but orders

geographical locations according to their connection to and function in the global network. It follows the geography of the physical layer that transmits data flows and highlights the domination of the bandwidth. In analogy to Castells' space of flows, data flows here become the dominant ordering principle. Geographic places do not become irrelevant, but instead the way data flows transforms geographic relations. The ordering principle of this space of flows is still fundamentally material, namely the course and quality of the fiber optic cables connecting each place. This makes clear how geographical relations in the internet are determined by the capacity of the physical network connecting different places.

When one considers that after all, the virtual space of the internet is created by the transmission of very real signals, signals that need a reliable medium to be transported by, it becomes clear connection paths are not random but dependent upon the global cable network. Location in the internet's physical geography depends on the routes where internet operators have laid out high capacity undersea cables, crossing wide intercontinental distances via the ocean floor (Figure 5). The cables are crucial for the internet as infrastructure, because they have the power to connect smaller networks (for example intracontinental or national ones) to the whole network. They allow for example a European end user to access a US site or use the services of companies like Google, whose main servers are on US territory. The make-up of the physical layer is crucial for surveillance technologies which intercept at geographical access points. As we will find out below, the US with its big internet hubs has a geographical advantage for global surveillance in the space of internet flows, because it can indeed label itself as a major part of the "world's telecommunications backbone" (The Washington Post, 2013) and expect most traffic to cross its borders. As they clarify on their own slide, it is the fact that so much data flows through the US via the cable infrastructure which helped them to make their surveillance program Upstream, which collects data from the cables, work on a large scale. The PRISM program too uses a geo-political advantage. Since they depend upon the infrastructure, many globally operating internet companies are based on US soil and store their data there. As in our current world order geographic locations are tied to nation states, the internet's geography gives key positions to a country like the US. This will be important to consider when discussing the political implications of state surveillance. Because of the location of hubs and servers in the US, the NSA had legal and political force when it approached companies with surveillance plans.

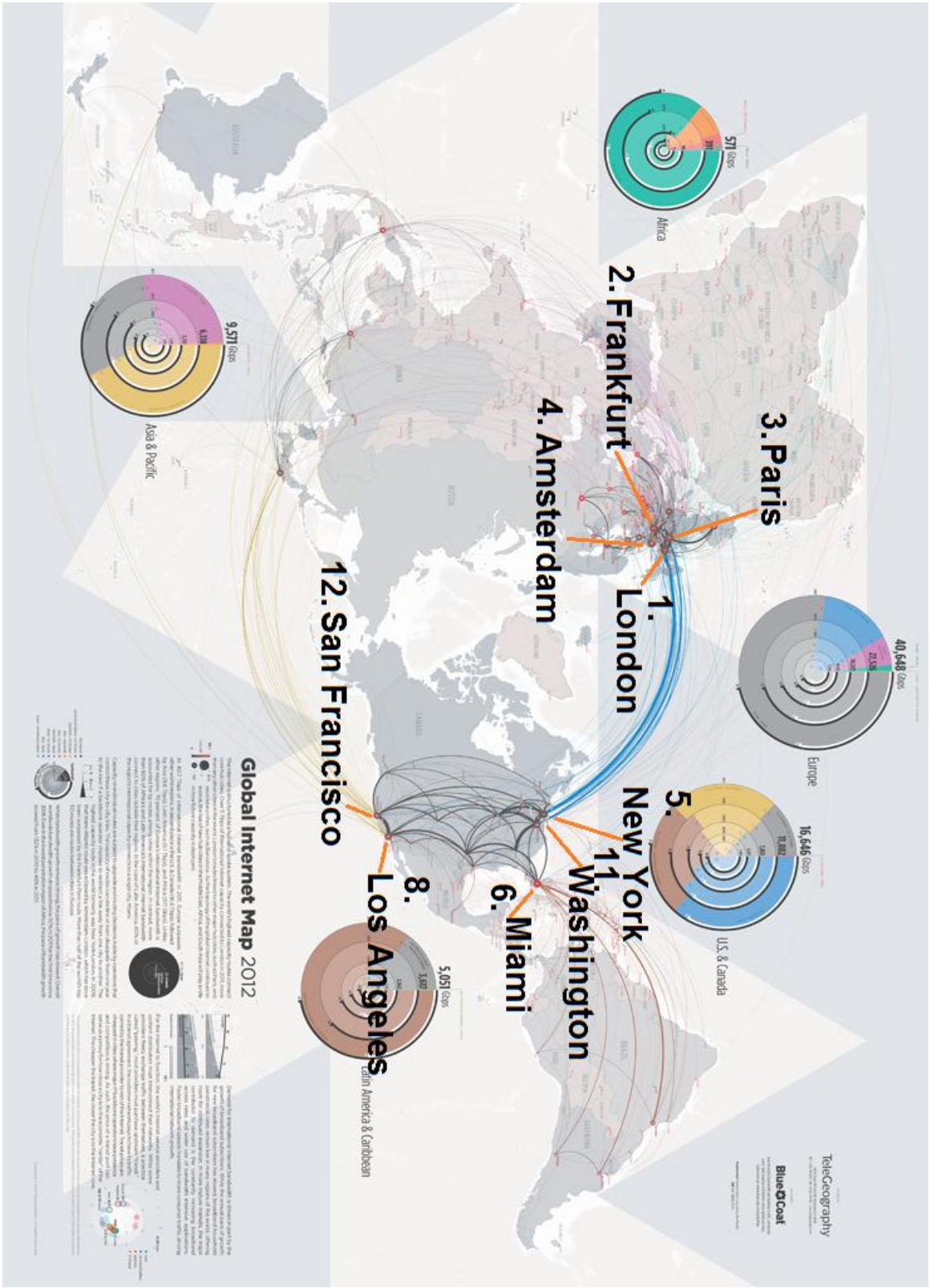


Figure 4: Global internet routes in 2012 mapped by TeleGeography

Figure 5: TeleGeography's map of the global undersea cable network in 2014

Internet exchange points.

So how exactly does the NSA (and other surveillance agencies) make use of its geographic advantage? How does it actually intercept data in order to surveil, how does it execute surveillance techno-politics? When it comes to actually intercepting the world's internet traffic, exact location becomes even more important – down to the level of single buildings. New York's 60 Hudson Street, the former Western Union building in lower Manhattan, is one such a place. It is a location where the internet actually happens. Here different sub-networks interconnect and hook up to the broader network and providers interconnect and (Mendelsohn, 2011). In this building, the cables of internet providers, companies and others come together and are intersected (Figure 6). These intersection points then build hubs in the internet's network. When one imagines the internet as the network of networks, it becomes clearer how all data flows, wishing to use its entirety, need to go through certain intersection points on their journey to get to a different part of the network. They are crucial for the physical functioning of the internet, but at the same time they are great points of entry for mass surveillance. Such a place where the different networks come together, connect and exchange their traffic is called an Internet Exchange Point (IXP/XP). The nodes we have seen in Figure 4 are examples of such IXPs' locations. With its hubs and cable structures, the physical layer is organized as a decentralized network. Within this network, the IXPs build hubs in the physical layer's structural diagram. It is not a centralized network: there is no one major hub or single center to which all communications flow or from which all data travels. Instead, there are several major hubs, and those are mostly the major IXPs, through which internet traffic flows (as the multiplication of a centralized network).

The intersection points are a crucial part of the internet's *backbone*, a vital part of its physical layer. It binds together different (sub-)networks into a single network and signifies the crucial structure for creating a *network of networks* (the internet). Data traffic has to pass the backbone in order to interconnect with other networks around the globe. A major part of the internet backbone is run by so-called 'Tier 1' networks. These are often huge ISPs which own such big global networks they do not need to pay other ISPs to transit their traffic; they connect directly to other networks and Tier 1 providers. Usually, the Tier 1 networks have agreements amongst themselves where they exchange their traffic free of cost and thus can connect to the whole of the internet without having to buy data transit from other internet providers (van der Berg, 2008). One of the world's largest Tier 1 networks is owned by the company AT&T, one of America's biggest internet providers (CAIDA, n.d.). Its globally owned network (Figure 7) is so broad it roughly resembles the internet's major transit routes (Figure 4, Figure 5). In 2014, AT&T's backbone carried 67.0 petabytes on an average business day (AT&T Inc., 2014) and its network includes more than 1 014 000 worldwide fiber route miles, 38 globally distributed data centers and services available in 182 countries (AT&T Inc., 2014). One of its major offices in the United States is located in *611 Folsom Street, San Francisco*. In this office AT&T not only processes the traffic of most of their customers, but also data from other providers who pay Tier 1 networks like AT&T for transit. At the same time, they host an exchange point for intersection with other Tier 1 networks. Consequently, their office functions as a major IXP similar to the one in Hudson Street. This makes it most probable a lot of internet traffic not necessarily only processed by AT&T flows through this location. Alas, the office building handles both domestic (US) and global internet traffic on a large scale.

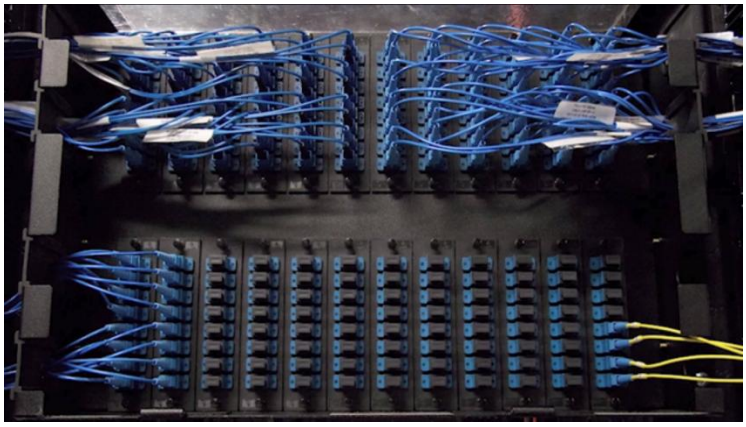


Figure 6: Where the internet happens – intersection point at 60 Hudson Street

Because the office, as a hub in the internet's decentralized layer of physical data streams, is a place where you might be likely to find a lot of the world's internet traffic flowing through, it appears an interesting target for surveillance technologies. For a *national* agency like the NSA, such a hub offers the perfect chance to intercept and maybe *control* a global network by operating on a national scale. Thus, by performing techno-politics on a national scale, it can then intercept a global public. Many of the details of how the NSA de facto collects data are unknown, especially since there seem to be a myriad of different intersecting programs and applications. But if someone were to intercept the world's internet traffic as comprehensively as possible, using a global Tier 1 provider like AT&T

would bring them really close to that goal. If surveillance targets a huge IXP of a Tier 1 network in for example New York or San Francisco, it retrieves data from a major hub in the global network and is hence much more likely to get not only local communication but global traffic which needs to flow through there in order to connect to the whole internet. But how could data then be gathered and used for surveillance, once a suitable access point is identified? Most internet communications are transmitted through fiber-optic cables. In terms of surveillance these need their very own method of interception. For gathering data from fiber-optic cables, physical interception into the cable structure itself is necessary because in contrast to electro-magnetic fields measurable from the outside of common copper wires, light waves stay within the medium and cannot be accessed from outside the cable (Hepting vs. AT&T, 2006). This shows how in ICT surveillance, material dimensions matter all the way down to the level of the physical medium. Surveillance techno-politics need to take these conditions into account and react to them with the suitable technological applications. *Room 641A* of AT&T's office in San Francisco is an example how this might look like. Already in 2006, whistleblower and former AT&T technician Mark Klein claimed he had found out NSA had instructed his former employer to install a secret room in the building in Folsom Street (Hepting vs. AT&T, 2006).

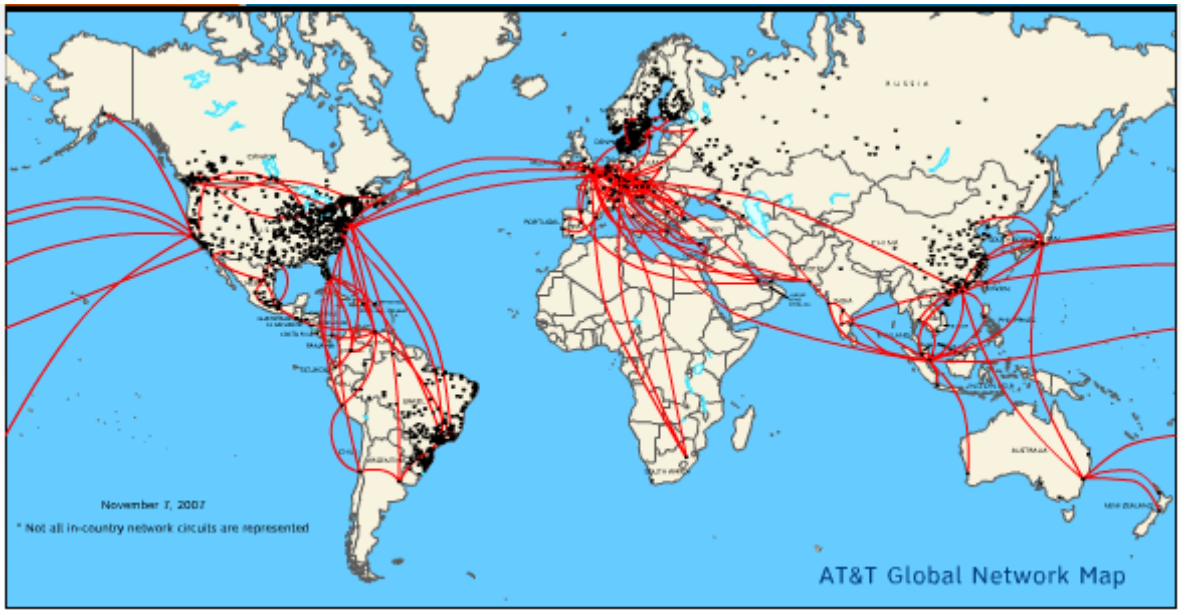


Figure 7: AT&T's global Tier 1 network

NSA's Surveillance Technologies

Room 641A.

Most likely, this room is a NSA facility operating under high secrecy and accessible only to few top rank AT&T employees (Hepting vs. AT&T, 2006). As Klein gradually found out, it was connected to AT&T's internet room, where an optical splitter installed by the NSA made a copy of all the internet traffic, of all the information encoded in light waves, running through AT&T's fiber-optic

cables (Klein, 2007). As a company, such a splitter is not what you would like to have switched in between your cables, because the copy of the data the splitter compiles from the physical light stream technically sets down the light waves' intensity and consequently distorts the signal and impacts negatively on signal quality (Klein, 2007). If and how AT&T has been compensated for this loss is not clear. However, there have been other reports stating the NSA has been spending "millions of dollars to cover the costs of major internet companies", caused by other surveillance programs (MacAskill, 2013). In response to these reports, criticism as to whether these a tax dollars spent wisely has been sparked.

In any case, it appears the NSA managed to get its splitter device installed and laid fiber-optic cables inside the facility to transmit an exact copy of the passing data to Room 641A. From company documents Klein eventually got to look at, it seems the NSA installed the splitter device in the beginning of 2003 (Hepting vs. AT&T, 2006; Klein, 2007) and had put it in a logistically smart place, namely at the intersection point where AT&T connects to other networks and to other major IXPs in the country. In an interview, Klein described what he believes had happened:

> So they took 16 high-speed peering links which go to places like Qwest [Communications] and Palo Alto Internet Exchange [PAIX] and places like that. … These circuits were working at one point, and the documents indicated in February 2003 they had cut into these circuits so that they could insert the splitter so that they can get the data flow from these circuits to go to the secret room. So this data flow meant that they were getting not only AT&T customers' data flow; they were getting everybody else's data flow, whoever else might happen to be communicating into the AT&T network from other networks. So it was turning out to be like a large chunk of the network, of the Internet. (Klein, 2007)

This description of NSA's activities on AT&T's network, which as Klein observed targeted a large part of the internet traffic, is an indicative example of internet techno-politics. The choice to intercept at AT&T's San Francisco office was surely not coincidental, but a conscious choice that presupposed extensive knowledge of the internet infrastructure and its properties, and especially its physical layer's organizing principles. This includes awareness of the social structure the network implies and knowledge about the fact that a lot of data from people all over the globe comes together and is processed at this interchange point, and therefore relies and depends on AT&T's technological services and, when it comes to data privacy and security, their integrity. Installing the splitter device in Room 641A was a technological enterprise on behalf of the NSA. It was founded on active reflection and inquiry into the internet's structure, on which it operates intelligently and organizes flows in order to advance the pursuit of its political aspirations. At the same time, the NSA operated on the network and used technologies to change it physically and to create new channels of

Figure 8: Room 641A at 611, Folsom Street, in San Francisco

data flows non-existing before. As I argue below, this operation goes as far as creating a centralized surveillance network which, on top of the internet network, is able to control data flows and thus interactions. In order to do so, the NSA has to be able to process, store and analyze huge amounts of data, and they do so through the use of up-to-date technological devices.

Narus STA 6400.

Also inside the NSA's room at AT&T's office, the traffic intercepted and copied was probably stored, processed and analyzed with latest high speed technology. A crucial device Klein talked about is the *Narus STA 6400*, a device made for high speed semantic analysis of huge amounts of data traffic. It is manufactured by the company Narus, a subsidiary of the Boeing Company since 2010 (The Associated Press, 2010). Next to selling their devices to governments publicly perceived of as oppressive in the Western world, such as Egypt and Saudi Arabia, they appear to have strong ties to the NSA, having made William P. Crowell, the NSA's former Deputy Director, a part of their Board of Directors (Lloyd-Jones ,2005; Narus, 2004). Their device installed in Room 641A, part of the NarusInsight series, is a high tech data analysis device which can analyze and process huge amounts of data in real time. The device is called a semantic analyzer, because what it does it is analyze data and look for certain (flagged) content, exceeding simple buzzword analysis. In this way it does not just intercept data flows but already makes sense of them and processes information (Klein, 2007). As the company puts it,

> the NarusInsight […] Intercept Suite (NIS), [is] the industry's only network traffic intelligence system that supports real-time precision targeting, capturing and reconstruction of webmail traffic. Narus technology has long been recognized for its ability to identify and track almost all network and application protocols across very large networks. (Reuters, 2007)

As Narus' marketing vice president Steve Bannerman said, "anything that comes through (an internet protocol network), we can record" and then "we can reconstruct all of their e-mails along with attachments, see what web pages they clicked on, we can reconstruct their (voice over internet protocol) calls." (Poe, 2006) According to Wired.com, Narus therefore advertised their device by praising its unique surveillance qualities: supposedly it "captures comprehensive customer usage data ... and transforms it into actionable information.... (It) is the only technology that provides complete visibility for all internet applications." (Wiretap Whistle-Blower's Account, 2006)

Splitter function.

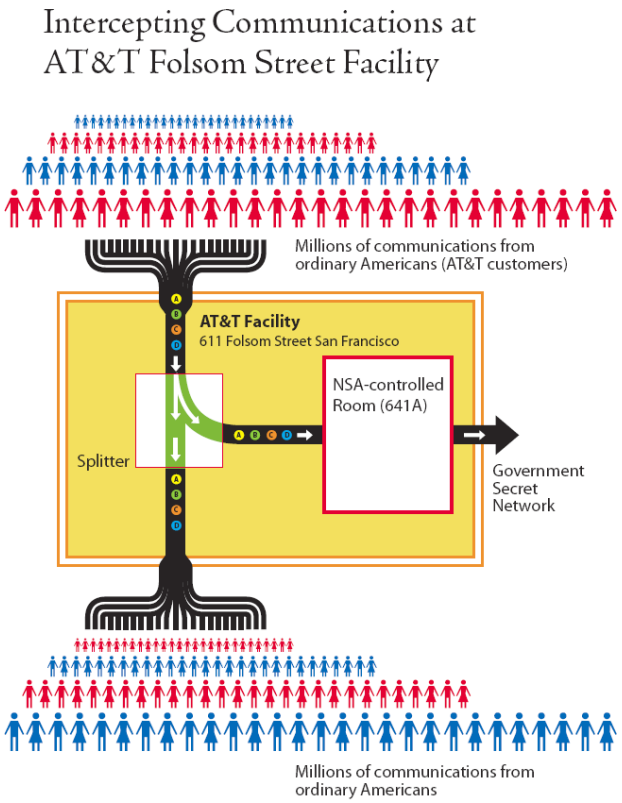


Figure 9: Graphical explanation of the functionality of Narus STA 6400 and Room 641A

When we now understand how the NSA attains and processes signals they need for their signals intelligence, we can also understand the meaning of their code names. Interestingly, the code names resemble pragmatism's framing of concepts because they refer to the function and technological context of the surveillance programs. Upstream points to the fact they intercept at major upstream lines, namely where global internet flows come together. The name of PRISM also symbolically refers to the actual technological practice. Normally, a prism is an optical device which splits a single light beam into different wavelengths. In this function it can be used to 'analyze' the beam for its different spectral components. This basically is exactly what the NSA is doing in AT&T's office – they physically split up a single light beam into two (or more) beams carrying identical information, but with reduced signal strength. Then they examine this beam for its different components. In this way, the term "prism" attains meaning in the language of the diagram. It metaphorically represents the function of the hub: it is a major node through which all information flows. The input (in the case a single light beam) needs to meet the hub (the exchange point/the splitter) from where it is distributed into different channels, according to certain laws, and a determined output is created – as such the prism has its very own diagram. The image in Figure 9 depicting the splitter's function in the network visualizes this. Here we can see how a single data beam is divided into two identical copies and from there directed into two different output channels. The placement of the Narus STA 6400 in a

strategic place aims at creating such a prism function and shows how the NSA's techno-politics use the make-up of the internet's physical layer strategically and technologically. It is well aware of the technological forces which make for the network on a layer often invisible, or made invisible by the protocological layer. For the NSA however, this invisible layer is crucial. Through employing technologies like the STA 6400 on it, the NSA can invisible build a new network and execute techno-politics beneath the user's surface. This kind of strategic operation impacts on the network as a whole and is hence able to affect it globally.

The Surveillance Network

But how does this new network look like? What kind of assemblage do the NSA surveillance programs create? And which position does the NSA have on the global network? The NSA's surveillance programs use the decentralized structure of the internet's physical layer through targeting and intercepting the major hubs. To this end they employ their strategic position on the internet's geography. Surely helpful also are the so-called 'five-eyes collaboration' they had with the secret services of Canada, Australia, New Zealand and the UK, as well as collaborations with other (Western) countries like Germany, and joint programs like the program *MUSCULAR* which operates together with Britain's GCHQ and intercepts data links to Yahoo and Google servers physically at the cables (Gellman & Soltani, 2013; Snowden, 2014; "Spying together", 2014). Even though it can physically access nearly all internet traffic, the NSA still also shares signals intelligence with other secret agencies like the German BND, who might employ similar techniques in their country. Hence, the NSA can even get a hand on the small amount of data traffic it does not itself intercept (Gude, Poitras, Rosenbach, 2013). In this way the NSA can intercept at the major hubs or IXPs of the internet's physical layer, on US soil as well as those abroad (Figure 4).

Centralized surveillance.

By intercepting these hubs and creating unidirectional data streams of intercepted and copied data to their servers, a new and centralized network emerges. The network has been called a *shadow network* (Appelbaum, Rosenbach, Schindler, Stark & Stöcker, 2013), because it operates in secret and because it copies data, which means it does not (per se) change the data streams as they flow through the common network, but creates an additional dimension – a shadow – which works through doubling data. Here, data flowing through the common network, the internet's infrastructure, becomes, in exact copy, part of a new network of unidirectional, centralized data streams which flow from peripherical nodes (the intersection points) to the central hub (the HQ) but not the other way around. Cooperating with AT&T was a way to achieve such a shadow network for the NSA. As Klein had reason to believe, they not only had a splitter cabinet in San Francisco, but also in Seattle, San Jose, Los Angeles and San Diego (Hepting vs. AT&T, 2006). This new dimension the

NSA surveillance adds to the infrastructure's physical layer transforms the layer from a decentralized into a centralized network and happens through hooking up additional technologies and communication channels to the hubs of the formerly decentralized structure. This leads to the creation of a central hub above the hubs it connects to and to which all information flows.

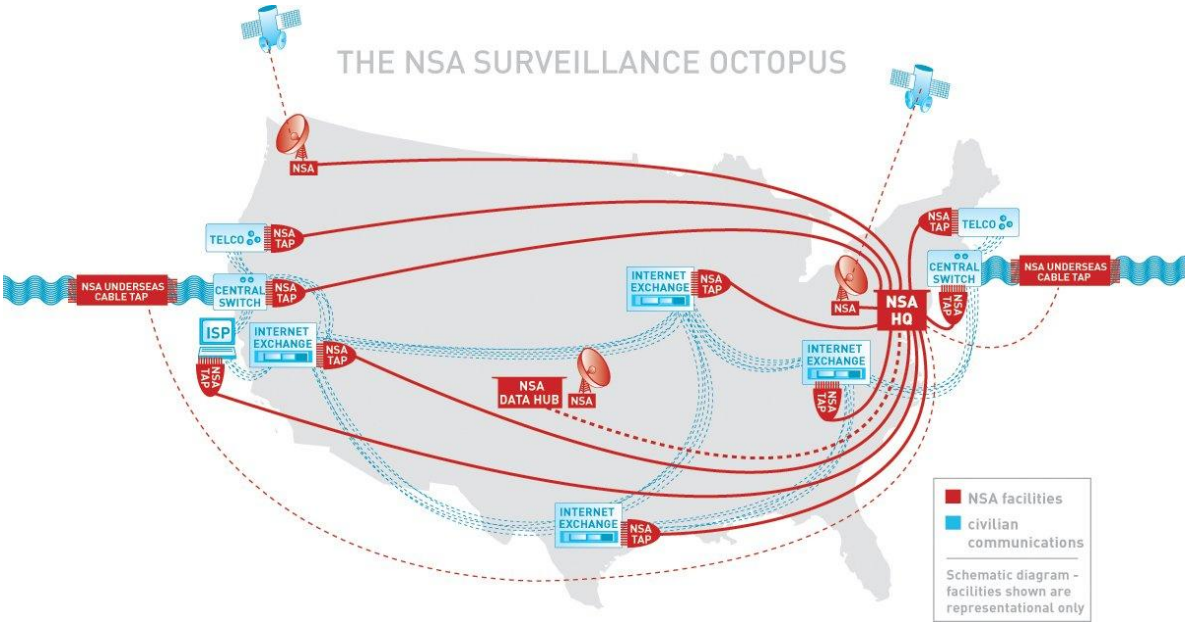


Figure 10: The NSA surveillance octopus

The network now resembles a centralized diagram. A graphic of the "surveillance octopus" is helpful for understanding how this works (Figure 10). The map was compiled by the American Civil Liberties Union and incorporates interception points from different programs. It shows how, through intercepting major hubs, a formally decentralized network (the blue connection lines) turns into a centralized one with the NSA headquarters as the central node (the red connection lines). Now, the map only shows the United States and not the internet's geography of the whole globe. But when we expand the graphic and add the importance the interception points in the US have within the global physical infrastructure (Figure 4, Figure 5), we realize this surveillance network has the capacity to span the whole globe and its internet traffic. This then allows inference of the public the network assembles, because it concerns people around the globe mutually and structures their relations and interactions. The octopus illustrates how techno-politics operate globally from a local basis, and how they use infrastructural conditions to create a new dimension to the space of flows. Because a new dimension of communication flows is added, the consolidating forces change. We see this change visualized in the transition from the decentralized to the centralized network. Because the transition incorporates global data flows, it concerns a global public, and because it systematically impacts on the channels of communication, it is – according to Dewey – part of the political realm. It is however

outside democratic frameworks, because it happens invisibly and without public discourse. Working through data copies helps it keep up this invisibility.

NSA's surveillant assemblage.

The public building up around NSA surveillance is assembled by all those who become part of the NSA's global surveillant assemblage, so by all those whose data get doubled, retrieved, stored and analyzed. Due to the global scope of NSA surveillance and its strategic position on the physical layer, this is nearly all internet users. This phenomenon questions a conceptualization of publics as being bound to organizations on state levels. Dewey believed such a concept was feasible, because he could not conceive of social groups "so separated by rivers, seas and mountains, by strange languages and gods, that what one of them does" would have, except for the case of war, "appreciable consequences for another" (Dewey, 1927, p. 42). The internet, amongst other international infrastructures, however challenges this assumption because on its physical layer it creates a new geographic distribution of connections and power structures. As Castells has argued new infrastructures give rise to new flows which can reorganize social relationships so as to create a new space. This space can for example allows social groups spatially very separated to become part of a network of intimately bound up associations, part of a common space, and at the same time the structure of its flows can change former geographic relations. Under the influence of comprehensive NSA surveillance, this space then becomes a surveillant assemblage. And even though Haggerty and Ericson said the surveillant assemblage works through "abstracting human bodies from their territorial settings and separating them into a series of discrete flows" (Haggerty & Ericson, 2000, p. 606), rendering them as delocalized data, the practice through which the assemblage itself works is tied to the internet's very own geography and the NSA's position in. Here the surveillant assemblage creates a specific space where social relations are manifested materially by the NSA's operation on the physical layer and its geography. The institution NSA resides at the top of the centralized network its surveillant assemblage creates and of which its headquarters are the command center. From there it has overview over the nodes, the internet's sub-networks and regular users, and can also exert power and control as I explain further below.

At first sight, this surveillant assemblage appears not to disturb the regular internet upon which it resides and operates. Instead, it seems to create a space with a centralized diagram of *copied* information flows which only *connects* to the internet's decentralized physical layer. This space differs in its properties from the common internet's organization. Whereas on the internet information flow is always bidirectional, within the surveillance network the flow of identically copied information is unidirectional within a centralized network. This means through the way it is configured, the NSA's internet surveillance creates a new centralized network riding upon the internet. It creates a new infrastructural component with a different informational network diagram,

working through data copies. A common internet user, in the belief she is interacting with the common internet and its infrastructure, remains unaware of this additional space because she remains unaware of data being copied, processed, analyzed and eventually used against her. In order to create this additional network dimension, the NSA works by means of techno-politics and employs techniques and technological devices purposefully, like the placement of Narus STA 6400 devices at big interchange points. This techno-political enterprise supports the ordering of the technological forces in a way which benefits the control function the NSA aspires to hold globally. Through intercepting the global network at strategic points, the NSA can reach the scope of a global network, as in the space of flows the boundaries of shared spaces are made by the reach of the first layer's dissemination. This is what Castells meant to express by the first layer he attributed to the space of flows. Like railways for him "defined 'economic regions' and 'national markets' in the industrial economy" (Castells, 1996, p. 413), the dissemination of internet infrastructures defines the internet's public and those who are included in and affected by it.

The NSA itself however appears to be outside the internet's regular space of flows, because it does not hook up to the internet like normal users (or even companies) would, but appears as Castells' elite which aims at controlling the space of flows from outside and, in this case, through techno-politics. Its headquarters, the highest command center within the NSA's internal network of facilities, represents the most superior hub of its centralized network, where the elite is located to exert power through surveilling the space of flows below it. Appropriately then, the headquarters located in Fort Meade, Maryland, have become a common icon used by the media to symbolize or picture the NSA (Figure 11). The symbolic meaning it emits speaks volumes. The HQ are located within a huge rectangular block building, completely coated by a black reflecting glass façade and surrounded by parking lots full of seemingly tiny cars arranged in near-circles around it. The block has symbolic expressiveness: it mysterious massiveness and closeness evokes the impression of a centralized power hub, the building embodies its own symbolic function. Its massiveness procures respect, its closeness smoothness and secrecy. Its black and reflecting façade does not divulge its interior. It does

Figure 11: NSA headquarters in Fort Meade, Maryland

not convey any substantive information about its inside and the work done there. It symbolizes the opposite of transparency, the opposite of communication, and gives the contemplator back only herself. It *is* literally a blackbox. Its surface absorbs and reflects the sunlight shining on it, the information travelling *towards* it, but it only shows what is already 'out there' and does not emit any light of its own, does not reveal any information from inside. The massiveness of the building makes it tangible, makes it a material artifact and emphasizes its geography, its materiality, its physical presence – it is anti-virtuality and anti-information. As a function it stays obscure – outside the space of flows – but as a physical object, an obscure part of the internet's physical layer, as an all-powerful hub in all its symbolic power, it is ever more visible.

Data centers.

Despite their symbolism however, in practice the headquarters do not have enough capacity to store, process and analyze the huge amounts of data the NSA appropriates. To solve this, the NSA has recently built the Utah Data Center, located in Bluffdale, Utah, at a cost of over 1.5bn US dollars and over an area of a million square feet (9.3 ha) (Carroll, 2013; Bamford, 2012). The center, which will provide a site where great amounts of data can be stored and handled, is hierarchically directly inferior to the HQ (Figure 12). Estimations of how much data the center will be able to process and store go up to a yottabyte (1 000 000 000 000 000 000 000 000 bytes), but even low estimations still speak of 12.000 petabytes (12 000 000 000 000 000 000 bytes) (Hill, 2013). Global internet traffic is expected to reach 62.5 petabytes per month in 2014 and 91.3 in 2016 (Cisco, 2014). According to estimations of people familiar with NSA programs, the data center is not only meant to store the huge amount of data the NSA captures but also provide a facility for breaking code (encryption) (Carroll, 2013). The data center is not only needed to store data but also to process the physically captured data and make semantic use of it. The physical data streams alone, as light waves or electrical signals, do not per se provide any information useful for surveillance and population control. In order to employ the sheer infinite amount of information flowing through the physical medium, vast amounts of digital bit streams must be processed and analyzed. The information the NSA is interested in is encoded within those streams and wrapped by the protocological layer. The Naurus STA 6400 for example is a device which can process and analyze data streams for significant content on site and in real time. However, in order to analyze the data they physically catch comprehensively and in depth, the NSA itself needs facilities to where it can conduct data flows and analyze them. The information they retrieve is stored in huge data banks and fed into programs, helpful tools to make analytic use of them. These tools help interpret the data meaningfully in accordance with the protocols. Some of them will probably analyze data for suspicious activities automatically, while others let human agents search for what they wish to know. Since Snowden's revelations, two programs have especially gotten media attention: *Marina* and *XKeyscore* (Ball, 2013

b; Greenwald, 2013). Both of them allow NSA agents to sift through captured data and monitor targets. While Marina mainly focuses on meta-data, XKeyscore also allows for reading content. Thus the NSA does not only have programs to capture data, but also to read, sort and analyze the content they wrap. They do this by unraveling encoded data according to the protocological rules which guided their encoding. It is this *reconstruction* of content from captured physical data and its transformation into "actionable information" Bannerman spoke about when praising the Narus STA 6400 (Wiretap Whistle-Blower's Account, 2006). The NSA does exactly this on a large scale inside its own facilities, like in the center in Utah.

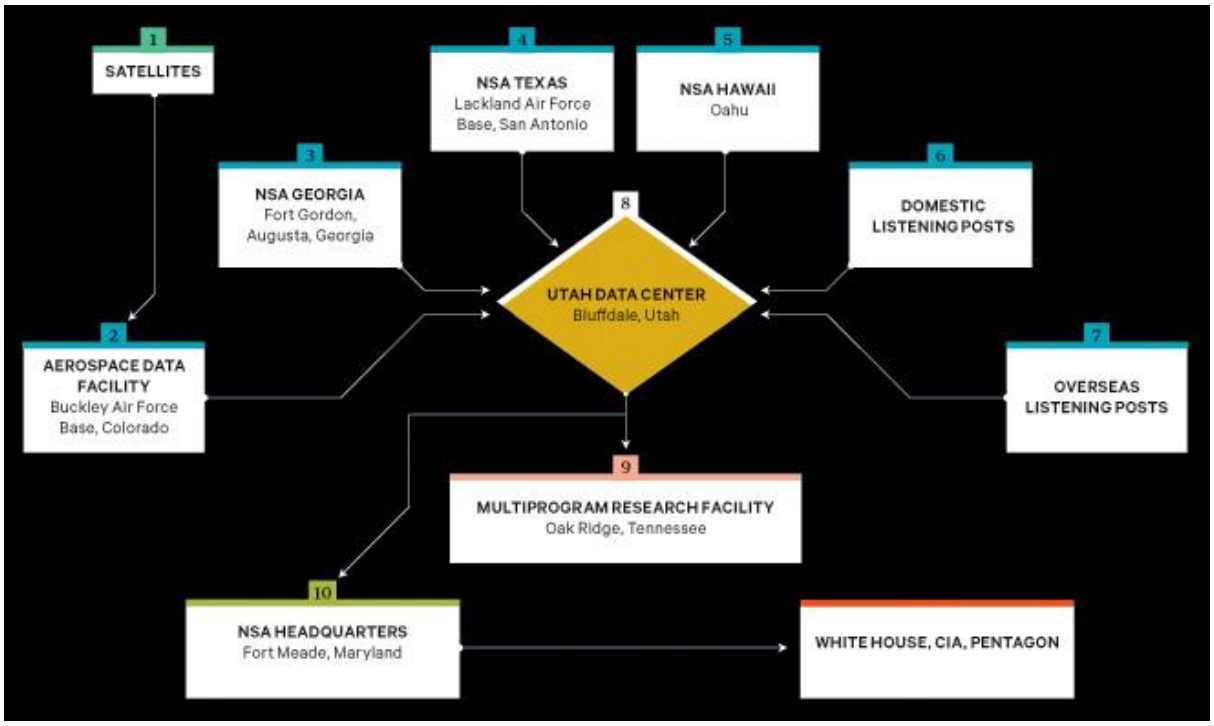


Figure 12: The NSA's own internal (centralized) hierarchical network

Network Control

Until here I have mainly been talking about the decentralized network of the physical layer and the centralized network of NSA surveillance, which operates through copying and eventually analyzing data streams captured at major hubs. This monitoring, storing and analyzing of communication flows however does not (yet) act upon the communication structure which the protocological layer creates on top of the physical layer and still allows for bidirectional peer-to-peer communication within the internet's regular network. How the protocological layer makes this possible is the subject of discussion in the next section. Connecting to this regular network now, the NSA establishes a parallel centralized network as it retrieves data copies flowing to its central hub. Even though it adds an additional dimension to the technological forces making for consolidation, it does not (yet) appear to *change* the existing data flows throughout the regular internet.

But despite unidirectional communication flows, a major characteristic of the centralized network is that the major hub, here the NSA, can (in principle) wield power over the global network and its nodes, here the regular internet users, and can control subordinate communication flows. This means the centralized network makes for a specific hierarchical form of social relations and places the NSA in a special position in the internet's geography. (A discussion of the implications of this hierarchical structure on political structures will be the subject of chapter 5.) The question now is how the NSA uses its position and the surveillance of captured data for population control. After all, the original slogan of the Total Information Awareness program, the precursor of many of the surveillance programs, was 'knowledge is power' (Horgan, 2013). This section investigates how the centralized network, which was established based on extensive knowledge of the internet infrastructure, can exercise power on other network participants. Talking about the Narus STA 6400, Bannerman spoke about "actionable information" because the semantic analysis of captured data streams the device performs should guide the surveillant to reach their purpose. However, so far we have only seen how the NSA uses techno-politics to establish a centralized network, but we have not seen how it makes use of this network for its purposes. Here I will discuss how control exerted outside the network and, as the main focus, inside, through data flows.

Control outside the network.

We have seen how the NSA copies and monitors information through a centralized network, but not how it acts upon these insights. Often it appears as if the NSA is only collecting comprehensive data for the sake of it – I discuss the impact this seemingly purposeless data collection alone can have further below. However, in certain programs the NSA does use monitored data to control, as we shall see below, or to have a political or strategic advantage over others. The information could be used for political or economic advantages – Snowden has actually claimed economic espionage to be a major part of the NSA's activities (Snowden, 2014). Using surveillance insights for political and economic advantage appears as the traditional way of using espionage, in which the NSA is also most likely involved in[9].The classical way to use surveillance for population control could be to use intercepted information to act upon people outside the network and in this way coerce them into desired behavior. In theory people's awareness of being monitored could coerce them to comply with what is expected or tolerated behavior, because they expect measures outside of the network such as legal persecution, detention, etc. This presupposes general awareness of surveillance, and the will of the surveillant, because only then can people react to and comply with

[9]In an interview with German news reporter Hubert Seipel, Snowden claimed the NSA is extensively involved in economic spying in order to advantage the US economic interests over others (Snowden, 2014)./In the beginning of this year, another high profile news story spread how leaked NSA slides seem to show the agency used its capacities to spy on participants of the Copenhagen climate summit in 2009 beforehand, in order to have a strategic advantage over other countries in the negations (Vidal & Goldenberg, 2014).

it. But if surveillance happens outside people's experience, it cannot influence them in future activity. Due to its secrecy, the NSA seems not to be interested in this form of coercion; its national scale also does not give it the ability to exert control globally through legal means. Another possibility however is to use the data to find and arrest potential criminals[10] or to identify national security threats more easily, to provide (national) cyber security – this is actually what the NSA claims it needs the programs for.

Control inside the network.

Whereas the above was a brief outline of how the NSA could use surveillance for control outside the network I would now like to investigate some if its programs where it actually exerts control *in* the network. In principle, the NSA's favored position in the centralized surveillance network allows it to control communication flows in the network. Its position comes with power as it is conceived of by pragmatism, because the central hub potentially holds the most effective means of operation – within the network it is bestowed with the effective means to reach its will, possibly overriding others' interests. The NSA's surveillance techno-politics not only strategically use the internet's geography, technologies like the Narus STA 6400 and facilities like the Utah data center to create a centralized network on top and attain information, but they make use of these activities to act *in* the network itself and to directly manipulate data flows and computers hooked up to the internet. By performing these activities the NSA's servers actually becomes *part* of the regular internet, of the space of flows. However it exploits its position of being connected to the network from outside and by a unidirectional data flow, to be able to do things other participants cannot do. Because of its authoritarian position within the network, the NSA can initiate data flows to the periphery when it feels the need to exert power. It has the possibility to intervene in regular communication flows on the network when it is deemed necessary.

Recent claims made by Snowden, saying it was a covert NSA attempt to build a surveillance backdoor into one of Syria's IXPs which eventually took the internet in the country down, shows what grave effect NSA's activities can have directly on the internet (Bamford, 2014). But moreover, the NSA uses its privileged position and technological resources targeted to directly influence data flows and computers on the internet. For example, in its alleged program *MonsterMind* it uses information it attains to identify potential malware or cyber-attacks and then 'fires back' automatically through attacking the supposed originator of the attack, for example a specific country's infrastructure (Bamford, 2014). In this program it seems to use the oversight over the network its central position provides it for providing security, protecting from cyber threats. The

[10]Torin Monahan and Priscilla Regan (Monahan & Regan, 2013) have demonstrated how in so-called data fusion centers, the NSA shares the data it gathers by counterterrorism surveillance programs with multiple other (national) law enforcement agencies which use it to persecute all kinds of crimes.

backfiring works through initiating or inserting data flows into the internet's regular space of flows – it is a sort of cyber-attack, compromising the network security of another system. Here the NSA uses the physical interface it has created with the network in order to participate in the network and reach its aims through communication flows. This shows us how the NSA changes the consolidating forces, the diagram of physical data flows, through hooking up its own network to the internet and then uses this advantage to exert power in the network, to gain the ability to execute on the technological structure that binds us together.

Next to MonsterMind, another essential program is called *Quantumtheory* (Horchert, 2014; "NSA-Geheimdokumente", 2013). While the surveillance programs I have discussed so far only capture and read data but do not change actual data flows or their content, Quantumtheory is more aggressive and actively manipulates communications. The program combines information the NSA's attains through its geographically strategic position on the physical layer with operations in the protocological space of flows itself. In contrast to PRISM and Upstream, the program is not meant for dragnet surveillance of all traffic flowing through the net, but uses gathered information to attack and infiltrate potential suspects through flows. First, it searches internet traffic flowing by exchange points to identify data packages coming from suspects in who the NSA is interested. In order to correlate data with suspects, the program requires the target to use unencrypted information. However, it seems likely even people who take great measures to secure sensitive internet traffic might at some point use normal web services, for example to check the weather or the news. Once such traffic is linked to a target, Quantumtheory activates one of its sub-programs. Upon the protocological layer, this program sneaks itself into the normal internet communication. What it basically does is wait until a connection with a server has been set up (most popular seems to be Yahoo) and then it intrudes the connection, sending an exact copy of the requested data to the client computer (Horchert, 2014; "NSA-Geheimdokumente", 2013). On top of this data it adds a secret program running in the back. By making the browser address a special URL in the background, the program establishes a connection between the target's device and a NSA server called *FoxAcid*. Because the NSA here participates in the space of flows and communicates bidirectional with another computer, the FoxAcid server needs to part of the normal infrastructure. However it is configured such that when one (accidently) addresses it, it disguises itself and pretends to be a regular internet server (Schneier, 2013). Invisible to the device's user, through this secret connection, the NSA site can then infect the personal computer, load software and take remote control. The connection can be used to search the target's private files, monitor all the user's actions through making screenshots or switching on the camera, and infect up-and downloads or cut the internet connection (Appelbaum, Rosenbach, Schindler, Stark & Stöcker, 2013).

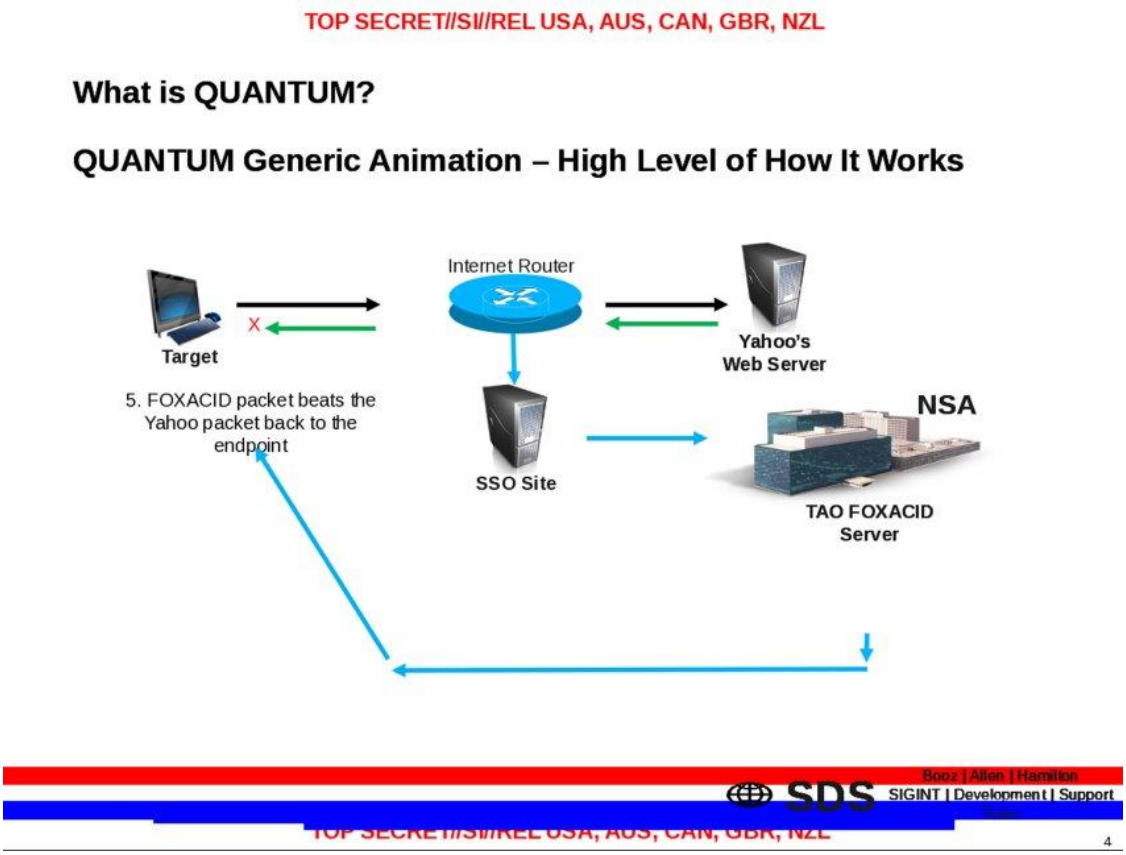


Figure 13: Alleged NSA slide about Quantumtheory

Quantumtheory involves both deep packet inspection (identifying the target and the request) and deep packet injection (infecting the package with malware). In performing these actions, Quantumtheory needs to fulfill the so-called *race condition* (Schneier, 2013). This means the data package sent from the FoxAcid server has to beat the package sent back from the actually addressed server (i.eg. Yahoo) and reach the target's computer first. Due to the race condition, the NSA needs to send its data package over strategically fast routes of the internet. When the originally requested data package then arrives, it is stopped from reaching its destination. Such activities are called "man-on-the-side" attacks, because there is another party sneaking itself into a communication between two hosts (Schneier, 2013). In general man-on-the-side attacks are difficult to execute because "they require the attacker to have a privileged position on the internet backbone" (Schneier, 2013). This means, even though Quantumtheory manipulates data content according to the protocols, it is the position on the physical layer which is crucial for the NSA to carry out this attack. The attack depends on the geographic location on the internet's physical layer, because it depends on the speed of physical data transmission. It appears, in order to be able to achieve the race condition more successfully, the NSA has actually installed "secret servers, codenamed Quantum, at key places on the internet backbone" (Schneier, 2013). So it is again the geographic position of NSA sites within the cable and router network which gives them an advantage over other network participants. And once the NSA has succeeded to establish the secret connection between the client computer and the

FoxAcid server, counter-surveillance efforts become useless. From now on the NSA has a secret and direct link between the client and its data processing sites and does not need to rely on unencrypted traffic. By exploiting this method it has succeeded to create a centralized shadow network also *within* the regular internet, despite a user trying to avoid this through tools like encryption and onion routing. At the moment, it seems impossible for the NSA to infect every single computer on the internet and hence the program alone cannot achieve to a complete centralized network by connecting to all nodes. However, the more (physical) processing and storage capacity becomes available the closer it can come to this point – new data facilities like the Utah Data Center surely contribute to the progress. To counter such a network would require then require enormous technological effort to protect oneself from surveillance and control.

Obscurity & rhetoric.

The analysis of surveillance technologies and the centralized network they create by using their position in the internet's geography showed how technological forces can make for specific consolidations and imply people in a particular network – like Dewey proposed. Investigating into the technological forces can help us understand underlying (global) power structures and the invisible forces we are subjected to. What NSA's surveillance seems to do, especially with Quantumtheory, goes against many of the internet's most important rules (Galloway, 2004, pp. 61 ff.)[11]. First of all, it deceives, claiming to be someone who it is not (i.eg. Yahoo), and secondly it sneaks in an additional, invisible and unintended connection. Through it centralized network it holds oversight over all information flows and can exert control when it wants to.

The surveillance network operates on deeper infrastructural layers whose structure and ordering principles are unbeknown to us. It is secretly created, underneath the user interfaces with which we usually engage. Unless we actively investigate the underlying physical structure – this is basically what Blum (2012) has done in his book – we can use the internet without being aware of the deeper infrastructure. Similar to Dewey's electricity example, we know the internet infrastructure by the applications it offers us, but the underlying technological mechanisms remain invisible. This is not surprising, since, according to Star & Bowker, infrastructures ought to be transparent. Only at a breakdown they give rise to active investigation – pragmatism's technological activity. The NSA's shadow network operates outside our awareness and obscures the technological forces upon which we interact. We have seen how NSA's surveillance works through monitoring and compiling data *copies*, through hooking up additional information flows. It does however not change the internet's regular space of flows in a way that would recognize (i.eg. censorship). After all, even a program like Quantumtheory which infiltrates computers is, as far as we know, only meant for

[11] For this and other reasons, Bruce Schneier, an internet security specialist at Harvard, has claimed what the NSA does in fact undermine s "the very fabric of the internet" itself (Ball, Borger & Greenwald, 2013).

surveilling more data better. We have not heard of any cases where the NSA actively censors the internet, which would be a classical way to use its power in the infrastructure. Up to this day it is unclear to what exact purposes the NSA collects information about nearly all communication flows. In any case, it seems to share its information with other legal institutions in the states, in order to persecute (US) persons within the US national legal system (Monahan & Regan, 2013). But we have so far only become aware of a small fraction of potential applications, at least on a global scale, like spying on political leaders, economic organizations and eventual terrorist networks.

This absence of executed power on the network suggests we usually do not experience NSA surveillance, because it does not influence regular communication flows. For pragmatism, experience was constituted by the reflective engagement with a subject matter. It presupposed the conscious making sense of a situation in which we act. But if certain forces withdraw from our awareness, we cannot reflect or consciously shape and investigate them, and consequently not experience them. This seemingly purposeless data collection could gives rise to another aspect: maybe it is not even so important for the NSA to actually be too successful in technological surveillance – it might be enough if we believe it is. As we have seen, Snowden's information provide us with material that gives rise to the suspicion that the NSA is surveilling the global network, and we have seen this perspective ascribes enormous power to it. Because, without knowing what it actually expects, it appears to us that the NSA is in this most powerful and privileged position on the network, we are subjected to a sort of superior ideology. If the NSA would want to use its surveillance to coerce people with the rules it sets, it would make sense to have these rules clear cut. Instead, the obscurity it creates around its activities seems to require us to submit to its absolute authority. In short: there might be a purpose for which the accurate functioning of actual surveillance might be irrelevant, for which it would be enough for people to think the NSA was at the top of this omnipotent centralized surveillance network: intimidation[12].

However, this is only a speculation. The fact that the NSA actually tries to keep its programs secret and the government heavily persecutes whistle blowers seems to suggest it is not interested in people being aware of its power on the network. Apparently it would prefer to keep the shadow network invisible. Because we cannot ourselves engage with the technological infrastructure itself, we cannot check upon claims made either by Edward Snowden or by Barack Obama. Instead we have to decide who to trust in the public discourse. Because of this obscurity, we do not know the exact status of the surveillance programs, let alone *why* the NSA does everything to gain total information

[12] This perspective might shed some slightly conspirative light on Snowden, the former CIA agent who comes from a family of government officials (Mitchell, 2013). Even though the revelations contributed to global public resentment, they also took a major part in conveying the feeling that there is this centralized network which ultimately intimidates us.

awareness. We have no way of evaluating the way it handles data. Because we cannot experience surveillance technologically, we are forced to trust what its officials say. This is the case Dewey described: when the technological forces making for consolidation operate outside people's experience, they cannot democratically shape the institutions which handle them. Instead, they are subjected to "hired makers of opinion" (Dewey, 1927, p. 136). In the case of NSA surveillance, we can see how officials use a rhetoric which obscures what they are actually doing technologically. With the help of Snowden's documents and the results of an inquiry into the internet infrastructure, we can only know analyze the accurateness of these statements.

On 12th December 2013, Kurt Opsahl, attorney of the Electronic Frontier Foundation, gave a talk at the *30th Chaos Communication Congress* in Germany where he tried to clarify the underlying implications of what had been said to defend NSA programs (CCCen, 2013). For example he explained when the NSA administration points out they only collect about 1.6% of internet traffic, even though this sounds little, it is actually a lot. Given the huge data flow on the internet, a lot of which is video streaming as Opsahl said, the percentage of traffic that constitutes the meta-data and communications needed for surveilling individuals comes pretty close to this number. This implies that even though the percentage of total internet traffic surveilled is little, the amount of collected information about people's interactions on the web is incredible. Additionally, the persistent argument that NSA's comprehensive surveillance activities exclude American citizens is more likely the outcome of a word game than a state of fact. Due to the redefinition of what it means to "intercept", "acquire", and "collect" data this might very well imply that as long as no NSA employee has actually taken a look at the stored data, data has officially not been collected. And if they do happen to look at data, it appears they have the power to define whether it concerns American citizens or not. The selection criteria for making the decision whether a communication belongs to an American citizen are more a matter of interpretation than a matter of fact. Despite their huge capabilities, it appears in practice the NSA is not able to say, with full certainty, whether information exchanges happen only within US borders. In order to legitimize the search for information about a target, a NSA operator can simply select a reason from a dropdown list for why he suspects the target to be outside the USA (CCCen, 2013). According to the NSA regulations on targeting foreign suspects, so Opsahl, the criteria for deciding whether someone is foreign are that the likelihood is judged higher than 50%, while all nodes are assumed to foreign if not proven otherwise and encrypted data is stored in any case.

The Internet's Protocological Layer

We have now arrived at a point where we have found out how the NSA's internet surveillance programs analyzed in this paper operate strategically on the physical layer's geography. The distributed network on the other hand speaks a completely different language. As we shall see, the internet's protocological layer creates a whole different network upon the physical infrastructure. Whereas the physical layer gives significance to certain places (hubs) and hence key positions to certain players like the NSA, the protocological layer tries to create a network of equal autonomous entities and bidirectional information flows. Therefore its consolidating forces bring about a very different social structure. This structure is in a sense more global, because it aims at making geographic locations and consequently national borders irrelevant. In the distributed protcological network, no one node has oversight over the whole network or can yield power over other nodes. Communication is established through mutual agreement between any two equal nodes and data flows bidirectional. Location on the network becomes meaningless as every node is interconnected through a myriad of paths – the distributed network in fact is anti-geographic. As such it presupposes a totally different space with different social relationships, in which entities are in mutual exchange and equal. It is this kind of network which the protocological layer ought to establish on the physical infrastructure.

In the next section I explain how it is supposed to do so and subsequently how counter-surveillance techno-politics operate. Not surprisingly, they try to defeat the centralized network the NSA's techno-politics aim at and exploit the possibilities for distribution the protocological layer gives. After having understood this antagonism, we can then discuss the network struggle in which current internet techno-politics are involved in. As counter-surveillance technologies try to strengthen this distributed network, they stand in direct opposition to the centralized surveillance network. But they also carry out techno-politics by intelligently operating protocols on the physical layer. Through this they try to bring about different channels of interaction than NSA surveillance does. This is where the political network struggle happens. The way information is wrapped and transmitted around the globe through the physical layer is organized by the protocological layer which determines the rules according to which the virtual space of the internet is created. It determines both how information is wrapped and encoded, and how communication circuits on the internet are established. Due to this, it can (potentially) transcend the physical organization, as we shall see, and create a *distributed network* (Figure 14).

Distribution & hypertext.

Creating such a distributed network, without hierarchies but high redundancy, which could withstand a nuclear attack – a powerful symbol of the centralized network – was the original

imperative for designing an internet at all (Galloway, 2004, pp. 29 ff.). This actually is a good example for the experimental process so central to pragmatism: a threat (a technology that is) leads to a reaction and a technological enterprise (creating a distributed internet), while the outcome of this enterprise can in turn then lead to another perceived issue (to which the NSA seems to react to). In a process of mutual adaption and co-shaping, people then try to change the network again in order to reach a new purpose. The techno-political struggle between surveillance and counter-surveillance shows exactly this constant process of adapting to new issues brought about by the opposition's techno-politics. The most famous civil application of the internet, the World Wide Web, picked up the idea of distribution the internet promised and implemented it in its Hypertext Markup Language (HTML). As its founder Tim Berners-Lee (1999) described it, the vision was to create an application which would allow users to share and access information through the internet, and would do so in a much more distributed way than traditional library systems. Anybody who would want to hook up to and participate in the network should be able to without having to ask for permission, without having to consult any hub or authority, and users, similar to jumping from node to node in the distributed network, should be able to move through information by means of hyperlinks, non-hierarchical inter-text references which directly link to another related resource (Berners-Lee, 1999, pp. 4-5, p 16). In this way a distributed system open to all would emerge which would consist of a web of hierarchy-free connections. There would be "no central computer 'controlling' the Web, no single network on which these protocols worked, not even an organization anywhere that [would run] the Web" (Berners-Lee, 1999, p. 36).Thus the World Wide Web was consciously created to avoid hierarchical power structures.

This hypertext world early internet pioneers envisioned could have impossibly been implemented by hardware connections since it would have needed "tens or hundreds of cables running from" each computer to each other computer (Berners-Lee, 1999, p. 17). Above we have seen how the physical layer depends on geographic locations, interchange points and economic resources, and emerged to represent a decentralized network. The solution to transform this network into a distributed diagram was to design the communication structure so that it weighs all nodes in the network the same, and to use a network of links between the different nodes through which an uncountable amount of virtual connections could be established between any two computers on the net. It was meant to create a space in which connection and communication can be established independently between any participants. Not surprisingly then, in his book recounting the development of the web, Berners-Lee dedicated practically no thought to the evolvement of its physical structure. Rather finding a way for universal sharing of information *independent* of the specific wiring of various technologies was the challenge – to find a way around the constraints of the physical media. The project's aim was to get to a situation where the web would not have to be a

"physical 'thing' that existed in a certain 'place' [but only] a 'space' in which information could exist" (Berners-Lee, 1999, p. 36), to create a space similar to Castells' space of flows where physically disjointed actors come together. The design of protocols which would establish hierarchy-free communication circuits, and consequently distributed social relationships, independently of specific locations, was supposed to create such a space. Internet protocols therefore can reorganize or rather overcome the hierarchical structure of the decentralized physical layer which developed out of practical necessities. In Castells' space of flows, the protocols are then located on the second layer as they organize technologies – the nodes – and the communication flows between them into hubs and nodes, and specifically into a distributed network. They give rise to the emergence of the internet's virtual space in which the space of flows becomes realized as a physically disjointed meeting place. So the development of internet protocols and HTML challenged physical barriers and the web's properties soon became detached from the physical medium upon which it operates. This task is accomplished by the protocological layer. Without having to establish direct physical connections and instead following a path of connections throughout the vast physical layer, protocols create a virtual peer-to-peer connection for exchanging information between any two participants on the net.

Protocols & control societies.

The internet protocols let different characteristically distinct sub-networks connect through setting "an agreed-upon standard of [inter]action" (Galloway, 2004, p. 7). They describe how information must be wrapped and transmitted and enable "a system that […accepts] the autonomy of the network's members" by establishing peer-to-peer communication upon mutual agreement (Tim Wu quoted by Blum, 2012, p. 54). But even though in the distributed network all nodes are equal and autonomous, as there is no central hub which can exercise control over information flows, the distributed protocological layer also incorporates control mechanisms. These are inscribed into the protocols all network participants must stick to for initiating communications. The formal protocological layer described the rules required for participation in the system: every network participant has the same opportunities and but also the same restrictions. People are forced to stick to the protocols, not because disobedience will lead to punishment but because it will simply disable communication and prohibit access to the space of flows. In Protocol (2004), it is Alexander Galloway's overall point to make that distributed protocols also exercise control, but locally not globally. For him, protocols are the symbolic archetypes of Gilles Deleuze' (1992) *Societies of Control*, which he sees chronologically following Foucault's disciplinary societies (Galloway, 2004, p. 83 ff.).In control societies, so Deleuze, control is free-floating, continuous, and works through passwords and codes, genetic codes that allow and disallow by architectural necessity. Whereas in the disciplinary society, discrete bodies run through discrete institutions (schools, factories, hospitals) with discrete systems of rules and functions, in the control societies one is always in a "continuous network" of

flows where transitions are fluent: “one is never finished with anything” (Deleuze, 1992, p. 6). Control societies are hence implemented in a space of flows. Whereas the disciplinary societies depend on surveillance, punishment and self-censorship, the control societies can do away with that. They embed discipline within the system’s protocological rules of conduct. Their form of control is so advanced that breach of rules implies direct disconnection, idleness, expulsion from the space of flows.

IP/TCP.

The shared standard protocols of the internet are bundled in the *TCP/IP protocol suite*, introduced in 1983 (Blum, 2012, p. 52 ff.). It is designed in such a way that it accommodates diversity and lets different networks, with different internal structures, technologies and capacities, connect (Galloway, 2004, p. 46). Within this communication structure, no central authority exists.TCP/IP is the common protocol suite (in different updated versions) for transferring data over the internet and describes operations to be carried out for wrapping and sending data, independent of content (Cowley, 2012, p.35). It is responsible for mainly two things: for establishing a (virtual) connection between any two hosts on the internet, independent of their location in the physical layer, and for transferring data between them successfully (Beasley, 2009, p. 157). When a communication happens on the internet, the TCP (Transmission Control Protocol) establishes a virtual circuit between any two communicating hosts. The circuit is called virtual because it establishes a logical, not physical, connection between the two. There is no pre-established communication circuit between any two computers on the internet – this connection has to be logically set up when they want to communicate. The IP (Internet Protocol) wraps the data to be sent and labels it with the address of the host computer and destination host. Then it routes the data between the host IP address and the destination address (Beasley, 2009, p. 162), letting it flow through the physical infrastructure. The IP protocol is responsible for routing over the internet, for finding a path which the data can travel to reach its destination. It sends the datagrams off from the sender and lets them find their destination through hopping from router to router, from interchange point to interchange point, from network to network. At every station on this journey, at every router that is, the protocols check whether the data has arrived at its destination. If this is not the case, they search for the next hop which lies in the direction of the destination and pass the data on (Baker, 1995). In order for this system to work, a router must know its relative location within the network and the direction of other addresses (Blum, 2012, p. 29). However, no router knows the exact location of all hosts on the network, but only where they are situated in relation to its own location. In the distributed network no one node has oversight over the whole structure or fulfills a control function. The graphics provided by *The Opte Project* help us imagine how the internet’s distributed structure

looks like – what they do is visualize all IP addresses participating in the internet and the communication paths between them (Figure 14).

The internet protocols are supposed to guarantee that upon the physical network of cables, servers and routers, information flows are possible that adhere to diversity, redundancy, and distribution (Galloway, 2004, p. 42).The structure of the protocological layer resembles what the internet was supposed to be when it started, namely a distributed network with redundant communication paths but without regulatory centers, which can resist centralized power and threat. For organized dragnet surveillance, this distributed system poses a problem – the push towards total and centralized surveillance actually emerged in light of a new threat which works through a distributed network (i.eg. 'terrorism'). A network where communication flows are distributed is much more difficult to attack by a centralized power but it is also considerably more difficult to surveil and control, due to the absence of hierarchies and the redundancy of communication paths which would need to be intercepted in an incredible number of places (see chapter 3).Therefore, as I showed above, through operating on the physical layer, NSA surveillance aims at creating a centralized network wh ere its own facilities build central hubs. But this network diagram goes against internet's original purpose, created as a distributed hierarchy-free network in which information flows a) from any one participant to any other participant without having to consult an authority and b) bidirectional between two communicating hosts.

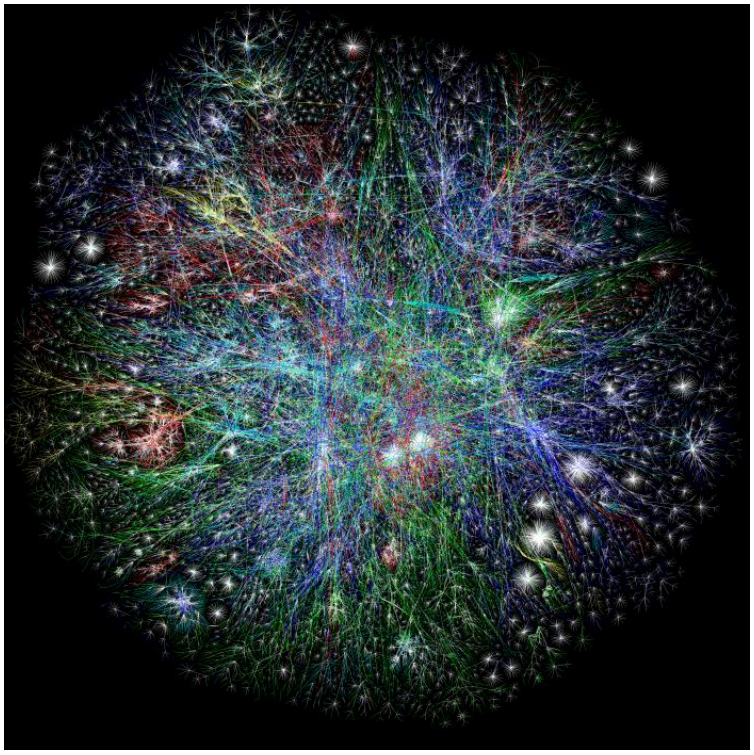


Figure 14: The distributed diagram of the internet's protocological IP system

The protocols specify how semantic content has to be encoded – they are responsible for encapsulating data. At the end of this process of encapsulation, a string of binary bits is created upon which the physical layer can operate. The protocols tell the physical layer how and where to send data. When it has reached its destination, protocols are reversely applied to unwrap the data packages and display the semantic content (the e-mail, picture, etc.). However, as a set of formal

rules, the protocological layer is indifferent to the specific configuration of the physical layer. It also does not care about which operations are carried out upon the data packages. As a highly formal format it does not 'see' anything outside its standards. For the protocols, the only important thing is that there is a public IP address through which hosts on the network can be linked and found and that data hops from router to router until it's reached its destination. As long as there is a physical structure supporting this, being able to read and transmit the data, its exact make-up and geographical map is irrelevant for the protocols. Whether a package from Germany to India goes through Nairobi or New York does not mean anything to them, and how exactly broadband connections and undersea cables run is something which they do not mind and do not know as long as there is any possible path towards the destination. As long as data packages remain undisrupted or are only disrupted in a way which keeps up their rules, anything can happen with the actual signal along its way. A splitter like the one installed in Room 641A operates in a mode invisible to the protocols. It is making a physical copy of the signals and therefore reduces the signal's strength but it does not change the protocological encapsulation or the order of bits within the stream. In fact it relies on leaving the protocols untouched! Like this, data transmission can continue without the signal showing it had been intercepted, and the powerful analytical machines which look at the packages can make use of protocological rules to unravel content and meta-data.

In this way, protocols are not only not able to circumvent a centralized network of surveillance, but they can even help make it invisible. The distributed network which protocols create comes about by the logical rules they define for communication – so that any participant on the network can talk to any other. But if in the process of materially realizing this network, certain physical transmission routes gained precedence and strength, possibly due to economic and political factors, and if this fact is used by powerful agencies to intercept and secretly create an invisible centralized network on top, eventually executing control on information flows, this does not touch the distributed nature logically defined by the protocol suite. So even though protocols aim at a distributed network, the NSA can use this network for surveillance purposes, because, since the protocols are public and standardized, anybody who gets a hold of the data packages flowing through the physical layer can unwrap them and find out their content. Additionally, one can gather meta-data from higher protocological layers containing information *about* the data, like source and destination address, and find out who is communicating with whom or who is looking at which webpage(CCCen, 2013). This is what meta-data collection is: it is the analysis of data streams according to the protocols in order to find out who is communicating with whom or who is looking at which website and when and where. And technologically, if one has access to the data package, they can as well get to the content of the data transmitted by simply unwrapping the full package. Once

you have a package or its exact copy, this is as possible as gathering the meta-data, but happens to be more complicated and demand more processing capacity.

Counter-Surveillance Technologies

So on the one hand, the open and very formal design of the protocols does not directly protect from surveillance, but on the other hand it also allows for the use of technologies that do so. What counter-surveillance in effect does, as I now argue, is to strengthen the distributed network of bidirectional peer-to-peer communication in such a way that it does not allow a secret listener in between or a centralized surveillance network on top. In doing this it weakens the physical structure's diagram to the extent that its geography becomes insignificant and useless for surveillance purposes. As the NSA relies on the decentralized network of the physical layer, this strategy is a counter-techno-politics to NSA surveillance. While surveillance technologies massively exploit the physical structure of the internet, counter-surveillance technologies aim at tricking its coercions and at circumventing the possibilities for dragnet surveillance it creates. Even though they cannot avoid having to use the physical layer at some point, they use the possibilities the protocological layer offers them to formidably complicate surveillance. In this way, they aim at strengthening the distributed diagram in dominating communication flows on the internet and prevent surveillance which works through a centralized diagram. Because the IP/TCP suite cannot per se protect the network from dragnet surveillance and its centralized structure on the physical level, a solution to cope with surveillance would be to avoid the internet's existing physical layer all together and to create a totally new physical structure. Currently there is a project which tries to create the so-called *Outernet*, a new internet infrastructure which uses satellites from space to avoid privacy and censorship issues by simply creating a new infrastructure for signals transmission (Outernet, 2014). Despite this rather utopian project (until now), another way is to logically circumvent the hidden coercions of the physical layer, just like the protocols were supposed to do (when there is no surveillance) in creating distributed communication flows. As Edward Snowden said in an interview with James Bamford (2014):

> We have the means and we have the technology to end mass surveillance without any legislative action at all, without any policy changes. […] By basically adopting changes like making encryption a universal standard—where all communications are encrypted by default—we can end mass surveillance not just in the United States but around the world.

Encryption.

Snowden actually called for the active use of techno-politics here: he said instead of tackling the issue through a public discourse, and eventually changes in policy, we should enact political ambition by the intelligent use of technologies. Without policies, but through this enactment we can

then achieve the global socio-technical structure we deem appropriate for the internet. Technologically, Edward Snowden proposed we can say: 'Well, we can't use the distributed structure of the current protocols to avoid interception on the centralized physical layer, but we can use applications that add to the protocols without violating the internet's rules and like this make the data unusable for surveillance, even if you get hold of the physical signal.' This is exactly what encryption technologies do, one of the most powerful tools against surveillance so far. Encryption technologies do not omit the decentralized physical layer but they make its structure functionless for surveillance while still using it to transmit data. They basically trick its power by strengthening protocols' nature and reinforcing a distributed peer-to-peer character into internet communications. The basic principle of encryption is to transform plain text into cipher text by running a program over it. The cipher text consists of a seemingly meaningless mumbo-jumbo of characters – only with the right decryption key can the message then be transformed back and its meaning read. Only the parties who are supposed to receive the information should hold the decryption keys and be able to read the message on their site. Even if a third party would get hold of an encrypted signal travelling through the internet's backbone, they still could not read the message. Encryption thus uses how protocols allow any two nodes on the internet to communicate through its physical link structure, and at the same time it makes sure it is only those two which initially agreed on communication which actually exchange information.

Hiding meta-data.

One of the problems with most common encryption technologies is even though one can hide the content of a message its meta-data is still on open display, because IP needs this information for routing data packages to their destination. This meta-data can still contain very valuable information for surveillance purposes. For hiding meta-data, encryption of the message's content is not enough – instead one needs to manipulate the protocols which route data packages through the internet. Since concerns for privacy and anonymity on the internet have grown, projects which try and do exactly this have spread. One project currently tries to develop an e-mail service which does not only encrypt content but also hides origin and destination (Zetter, 2014). They do so by not publicly announcing the exact address, but only its proximate environment (the domain). Once a message has left its domain, any analysis of meta-data cannot specify its original resource anymore but only the broader network. It also cannot see the exact destination but only the destination's proximate environment. Once the data has reached this environment, its exact destination is disclosed. This tactic requires new protocols for e-mail transmission since current ones need both the source and destination address to be public. It not only requires acting in the network, as common encryption does when scrambling content without changing the protocols, but it also requires acting on the protocological layer through changing the protocols. The challenge is to create

new protocols and standards which work just as fine upon the internet infrastructure. While encryption leaves transmission protocols untouched and operates merely on the content, techniques for scrambling meta-data operate within the protocological layer and asks for new transmission protocols. Therefore the *Dark Mail* project is not an easy task, since to make the application "universally deployable with current systems requires an aggressive overhaul of existing protocols and software infrastructure" (Zetter, 2014).

Another tool for hiding meta-data through manipulation of protocols was created by the *Tor* project which has set out to (re)create a "distributed, anonymous network" (Tor Project, 2014). It does so by connecting its own technologies and servers to the internet and by letting them use its own set of protocols. The project offers a new technology for routing data over the internet which does not adhere to the standard routing protocols. Instead, it creates a random path between source and destination throughout a network of globally distributed Tor relays (=servers). Data sent through this network is wrapped in several layers of encryption, subsequently unwrapped while bouncing through the network. Any intermediary relay can only read information about the next Tor router to send the data to, but has no knowledge about source and destination. So within each transmission between two intermediary nodes, only the addresses of the two are known but the rest is encrypted. Therefore if one were to intercept this data, one could not tell who send the data and to where, as little as read the actual content. The only data accessible would be the routing information between the two intermediaries – data unusable for surveillance. So even though also with Tor, the data travels over the internet's backbone and thus the major interception points, the information accessible through wiretapping these lines is reduced to the minimum of information required for data transmission (namely knowing the next hop). The data made public is just enough for fulfilling the internet's function but totally uninteresting for a potential surveiller. This shows that even though the physical infrastructure provides a platform for dragnet interception – and common protocols do not care or cannot avoid this – the protocological layer still in principle offers the possibility for ensuring a distributed peer-to-peer network nevertheless. In fact, to this day onion strategies like Tor are extremely hard to crack. And in any case, this requires an incredible amount of calculating capacity. Therefore these radicalized forms of internet protocols, forcing distribution by all means, appear as the 'natural' enemy to centralization and consequently institutions like the NSA.

Antagonistically, just like the NSA's way of operating is symbolically embedded in the headquarters which represent it, the ambition of counter-surveillance movements to strengthen distribution through radicalizing the protocological layer can be identified in their use of symbols (Figure 15). The symbolic representation of the internet activist group Anonymous for example speaks the language of the distributed diagram. The Guy Fawkes mask has become its favorite

symbol, allowing its members to stay unidentified behind it. The mask has become a popular tool for hiding one's identity, but it represents more than that. It carries symbolic meaning. The mask refers to the character V in Alan Moore and David Lloyd's graphic novel *V for Vendetta* and the homonymous film adaption by James McTeigue. It symbolizes armed resistance against centralized state power and an all-knowing, all-controlling police state. It symbolizes the (explosive) infiltration of stable hierarchical institutions of control, a viral threat attacking the center from within. But its real power is obtained when it is worn by all members of the group, for example at a demonstration or protest. It hides their identity in the same way as encryption hides data. Their faces become a mass of equal entities, all bestowed with the same power, the same abilities, the same freedom – their masks transcend their place in socio-economic hierarchies (Hayase, 2011). They *become* the distributed network, consisting of equal nodes connected to each other by a complex web of associations. They *become* the viral threat, the antagonist of the central network. In contrast to the material consistency of the headquarters in Fort Meade, their preferred form of representation is protocological. They prefer to be symbolized as being embedded in three dimensional rows of 1's and 0's, resembling the glimmering computer screens of *The Matrix* (Figure 15). Their home is not the physical structure of the material world, but the virtual fluidity of the matrix: they are only *information*. Their preferred mode of operation lies in the zeros and ones, in the protocological rules that make sense of the matrix' numerical representations.

Figure 15: Graphic impression of the internet activist group Anonymous

Counter counter-surveillance.

Because of this antagonism between the NSA's vision of the network and the structure projects like Tor imagine, it does not surprise how the NSA tries to compromise Tor users and Tor server providers. Actually, it has decided to label Tor users in general – and there are an incredible number of reasons for using such an application – as potential suspects as well as those either using

other services providing internet anonymity or visiting website of or about those (Appelbaum, Gibson, Goetz, Kabisch, Kampf, & Ryge, 2014). And not only does it target users but also those which make services available – recently it had for example been revealed the NSA was surveilling a German student running a server through which Tor bounces its communications (Smale, 2014). When thinking about the current events not so much as security issues but as a struggle over the network's architectural form (centralization vs. distribution), these strategies indeed make sense. But watching traffic on the Tor network or similar technologies still is incredibly difficult even though NSA appears to have tried to compromise the infrastructure (Schneier, 2014). Because counter-surveillance strategies work through encryption which strengthens the distributed nature of the protocological layer and undo the geographically strategic position NSA holds, technologically it is a smart move for the NSA to counter counter-surveillance technologies on the protocological layer itself. It appears to work hard on decryption technologies (Horchert & Reißmann, 2013) and on compromising network security. Several NSA and GCHQ memos available to the New York Times have revealed the immense effort which the secret agency is likely to put into both finding powerful decryption technologies and on compromising security and encryption standards (Perlroth, Larson, & Shane, 2013). It seemed to have forced companies, Microsoft probably amongst them, to hand over their master encryption keys. This basically makes encryption useless since anyone in possession of the keys can decipher the messages. Additionally it has been accused of illegally breaking into companies' servers in order to find out about keys not handed over to them. An infamous example can show how rigorous the NSA acts to get to these keys. A company called *LavaBit*, offering anonymous internet services to its customers, was recently forced to shut down after the NSA had dragged its founder Lavar Ledison through a quite dubious court process (Levison, 2014).

Above I explained how comprehensive anonymity on the web would require some changes to the protocols, so both content and meta-data are hidden. With regard to this, what might be even more significant is how the NSA actually directly tried to shape encryption *standards* to its advantage. Its aim is, as quoted by the New York Times (Perlroth, Larson, & Shane, 2013), to "influence policies, standards and specifications for commercial public key technologies". It seems its agents have taken part in the shaping of major standards such as those issued by the International Organization for Standardization, in order to make the general design of encryption technologies vulnerable and it consequently easy for them to crack. This appears as a special breach against the fundamental principles of the internet infrastructure. They ensure the complexity and flexibility of the network and allow it to be distributed by nature, because they make it possible for anybody to tie up to the network without having to consult authorities. Due to the democratic medium the internet was intended to be by its developers, these standards are supposed to be open and shaped democratically (Berners-Lee, 1999). At the same time they ought to help build trust in the network

and allow lay users to interact freely within it. When thinking about network design, NSA's efforts to compromise the internet on its protocological level through infiltrating standards is a visual exemplar of how standards, and the network structures they allow or disallow, align the relationships between humans and technologies within a shared infrastructure (as Star suggests). It is in this way that Galloway argued power is exercised within the distributive network, too. The design of standards determines what can and cannot be done on the network and brings forth a certain coerced behavior. But if strong encryption manages to survive, and to this day well-implemented uncompromised encryption tools are still the most private way to communicate on the internet, strategic use of the protocological layer remains successful in making NSA's presence on major exchange points unexploitable. They are technologically left with no other opportunity than to intercept directly at single communicating nodes. Understanding this, they appear to have developed comprehensive programs to intercept and infect single private devices (nodes). It has been reported they actually force companies to implement security backdoors in their devices or have caught off devices from package delivery services and implemented spying tools in their hardware (Appelbaum, Horchert, Reißmann, Rosenbach, Schindler & Stöcker, 2013).

Network Struggles

By now we have seen and analyzed surveillance strategies as concrete examples of techno-politics and of a techno-political struggle. Surveillance and counter-surveillance strategies are techno-politics because they aspire to systematically regulate the channels of human interactions, ICTs that is in this case, and through this strive towards embedding a specific form of social structure, communication structure, in the network. They do so by engaging in a technological enterprise, through employing technologies to reach their purpose. Techno-politics work through the politization of the technological and the technification of the political, using the reciprocal relationships between politics and technology. Politics are neither simply concerned with the network, nor does the network merely force politics to change: the network itself *is* inherently political, because its structure determines the way interactions and communications are channeled. Dewey, writing in 1927, already recognized the central importance technological networks and infrastructures play on the political stage; he recognized how they enable flows which can (re)organize society. Thus the network as a politically important category is not a new thing, it is only particular networks which change and emerge. The techno-politics we have seen not only respond to changes in technological structures and aim at regulating them through policy, but they actually enact, or at least try to enact, their desired network through the application of technologies directly on the network. The case NSA provides a prime example for how current techno-politics work, for how political struggles are expressed and carried out in technological infrastructures and how these

infrastructures in turn bring about transformations that concern the relations of all citizens of a shared network.

If we follow Dewey's philosophy, then we can come to conclude that networks and the organization of flows of goods within them are always political a) because being networked, being part of a community and embedded in an environment, is a necessary condition for existence, b) because the shape of the network determines the types of relations and interactions possible, and c) because politics are concerned with the conscious shaping of the network and its shared practices and interactions. The shape of a network mirrors its political culture at work. For example, Marxist media theorists Berthold Brecht and Hans Magnus Enzensberger interpreted the radio as a capitalist media because its functional division between sender and receiver was seen as reflecting the division between producer and consumer, between the ruler and the ruled, between the manipulator and the manipulated. As a remedy, so they proposed, a new form of media which allows each receiver to also be a potential transmitter would bring emancipation from this bipolar structure of (how they saw it) capitalist oppression (Galloway, 2004, p. 55 ff.). What they articulated here were the socio-political dimensions of technological network structures, of specific network diagrams: for them, the unidirectional information flow of the radio (from station to receiver) embedded capitalist socio-political structures and values, whereas a potential bidirectional medium (which the internet created) embedded a socialist structure which would emancipate and equalize people. This is a pragmatic belief, because it shows how the articulation of values connects to material structures. We have by now seen how today, surveillance and counter-surveillance also work through network diagrams which embed different power relations and control mechanisms.

My analysis of the technological operation of surveillance and counter-surveillance showed the two in opposition, struggling about shaping the networks' internal infrastructural hierarchies and defining and exploiting a dominant layer. I have demonstrated how surveillance and counter-surveillance employ technologies to reach given – antagonistic – ends. They aim at creating specific network types – centralized and distributed – in order to bring about a space with defined social relations. These specific spaces can be understood as technological assemblages, as the surveillant and the counter-surveillant assemblage. The two antagonistic poles we could identify were the centralized network in which the NSA aspires to build the major hub and control communication flows, and the distributed network in which participants can interact bidirectional and autonomously, and without being surveilled. Both aim at creating a particular network that comes with a space in which social relations are structured in the way they wish. The techno-political struggle seems to be about the creation of a certain material product that comes with certain practices and relationships which give it its form, function and meaning – a space. They are created through the intelligent and

strategic use of technological devices and techniques, which presupposes comprehensive understanding of the internet's structures and structural layering. As the parties try to change the network's structure in a specific way, their purpose is to shape channels of interaction. The public concerned by these structural influences is a global public because – since in the internet all flows are part of a global network and, as we have seen in the beginning of this chapter most communications also flow along major communication lines around the globe – all internet users become part of the space created. The techno-political struggle we see is not necessarily about the opposition between the two abstract values "security" and "freedom", but about creating different network structures. It is a struggle between the centralized and the distributed network:

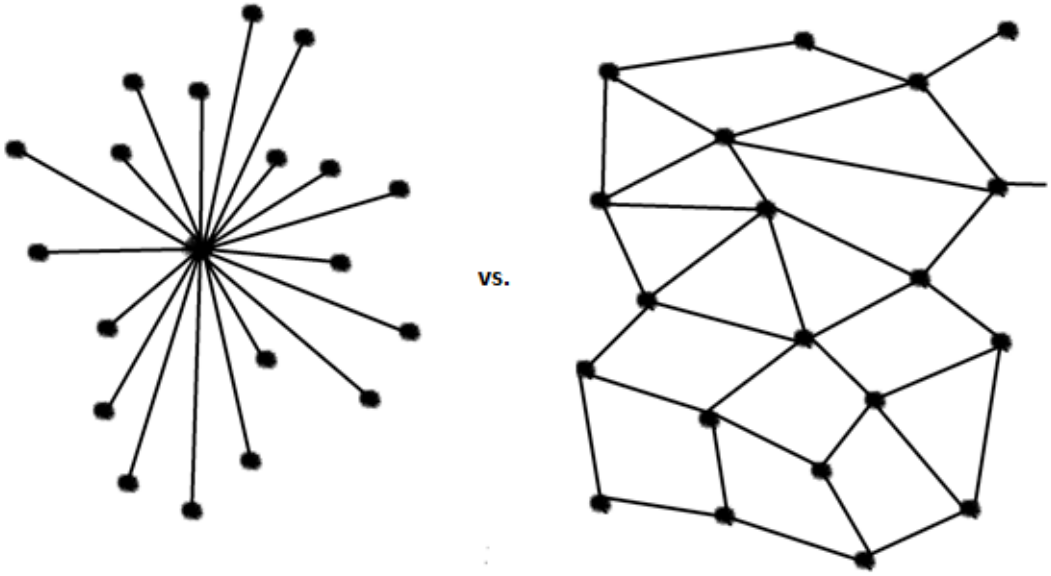


Figure 16: The network struggle between surveillance and counter-surveillance: The central network vs. the distributed network

In preceding parts I already pointed out how both the centralized and the distributed network can offer a particular and contextual form of security. An institution like the NSA can use wiretapped information which it obtains through the centralized network to provide national security, possibly against cyber threats (Brey, 207). Because it overviews the network and can ultimately control information flows, it can also provide protection from (viral) cyber attacks which might target crucial infrastructures and computerized systems. But counter-surveillance and encryption technologies also aim at offering security. Counter-surveillance movements see it as their aim to provide protection from the threat of a police state and from power abuse by authorities and as securing people's autonomy Encryption can provide information security because it protects information from eavesdropping and abuse (Brey, 2007). I have discussed how the NSA can use a centralized surveillance network in order to wield power over other network participants, and I have described how counter-surveillance tries to deprive it of the means to do so by establishing total

anonymity and exclusively peer-to-peer communication. Both the centralized and the distributed diagram incorporate power structures and mechanisms of control, but they differ in how they distribute power and control over the network, in how they distribute "effective means of operation" amongst the network participants (Hildreth, 2009, p. 786). In the centralized network, the central hub is in the privileged position to hold oversight over the network and to be able to control and initiate data flows. The (most) effective means of operation are then held by those who surveil and control information flows, by those who can exercise power over all subordinate communications. Even though in the distributed network all nodes are equal and autonomous and even though there is no central hub which can exercise control over information flows, the distributed protocological layer also incorporates control mechanisms. They are inscribed into the protocols all network participants must stick to for initiating communications. Since the norms of the network standardize the participants' behavior, those who set the rules, those who warrant or prohibit access, hold power over those who wish to connect, and can control the way they interact. So, in the distributed network, control is exercised through generally binding standards, but these can be established by democratic or despotic means.

Here one can think of the difference between speaking about democratic governance *of* the internet and speaking of it as an *inherently* democratic medium. The distributed network is more anarchistic – without a ruler or authority but with equally autonomous nodes – than democratic. But the protocological rules which in the network guide interactions for *all* can be established by a democratic process similar to the shaping of laws[13]. In a distributed space of flows, there are, by the very network structure, no elites and no central power hubs. But elites can influence *how* the generally binding rules in this space look like. This is why the NSA for example tries to infiltrate standardization committees or weaken encryption technologies as we shall see below. Its operation supports Castells' argument about the structure of the domination power elites exercise in the space of flows. He said "the real social domination [in the space of flows] stems from the fact that cultural codes are embedded in the social structure in such a way that the possession of these codes opens access to the power structure", but the elites who master these cultural codes do not themselves become part of the network (Castells, 1996, p. 416). So whereas the centralized network incorporates power inequalities between network participants in its structure, in the distributed protocological network they can be carried in to the network from outside. Within the distributed

[13] Today, the protocological rules are often set, in conjunction with industry partners, by professional engineering societies like the Institute of Electrical and Electronics Engineers (IEEE) (https://www.ieee.org/index.html) Another importan instution is the Internet Corporation for Assigned Names and Numbers (ICANN), an international non-profit which works closely together with policy makers (https://www.icann.org/). Up to this day, the question of how to democratically govern a global internet poses one of the biggest challenges.

network all are governed by the same rules, but these rules can be designed in a way that they favor some (i.eg. secret services) and disadvantage others (i.eg. those who wish to communicate privately).

The NSA's surveillance activities have long been known – the agency already appeared as the 'natural enemy' to the Cypherpunk movement back in 1992 that brought together early advocates of network anonymity, distribution and freedom of information (May, 1992). But Snowden's revelations and their great media resonance brought NSA's activities back to the consciousness of people and disclosed a dimension which caught us by surprise. They offered us more information to systematically investigate how surveillance politics operate in practice – to perform the inquiry into the technological forces making for consolidation. I explicated how internet surveillance purposefully exploits the internet's infrastructural layering, in which the different layers have different network properties. To understand which layer has control over the whole structure, so how power relations are enacted in the network, requires analyzing which layer can ultimately dominate the others. Also with NSA surveillance, the distributed internet people use and experience still continues to exist and up to now it seems most people can use it as usual (like they do without the NSA). But upon this distributed network, there resides a centralized surveillance network on top. In this network, the central hub ultimately has control, because it can in principle take over communication flows whenever it feels inclined to do so.

In the centralized network, the NSA is in principle in the position to *control information flows* throughout (nearly) the whole internet. This additional shadow network is made possible by the physical layer of the internet infrastructure, a layer which mostly remains hidden to the average user. It is the NSA's strategic position within the internet's geography which gives it the power to intercept information flows, like it does in Room 641A, and to be able to achieve the race condition in Quantumtheory. But in doing so, the NSA also exploits the distributed nature of protocol for its purposes. In fact, it not only tries to exploit the physical layer, but to influence the making of protocols in order to weaken the distributed network. Protocols, as the essence of the medium internet, are by design open and flexible. They function according to the principle "be conservative in what you do, be liberal in what you accept" (Galloway, 2004, p. 43). This principle, strength in the original network, now becomes a weakness of the distributed network, because it offers little protection against centralized surveillance.

On the other hand, because of internet's physical structures, protocols are so far the most applicable way to ensure the distributed and frustrate the centralized network. It is through protocols communications can flow distributed while the underlying infrastructure is decentralized or even centralized. Therefore counter-surveillance movements try to operate through using protocols strategically. In their strife towards encryption they actually try to radicalize and empower protocols,

ensuring peer-to-peer communication stays distributed *only*. In their vision, data still flows through the same physical channels but the dominant infrastructural layer becomes the protocol: through strategic implementation of protocols, physical raw data becomes unusable for surveillance purposes. Anonymizing networks like Tor also use their own physical structure as they run relays throughout the world. These relays are necessary to make Tor's protocols work and to create a network in which one can cover her tracks. However, in order to enable connection to the whole internet, the Tor network needs to connect to the normal infrastructure in its end relays. Here they allow protocols to communicate with regular servers fully functionally. What they confuse is the origin of data flows so intercepting along major communication lines and exploiting protocological information through deep packet inspection becomes superfluous. So the Tor network too uses the physical layer to create its own network of relays that allows the operation of a fully encrypted protocological layer and to confuse data paths. But its ultimate strength to counter surveillance lies in the protocological layer that scrambles data.

Interestingly, the NSA creates an elitist position, located outside the internet's space of flows, by connecting to the physical layer's hubs, but it can also *become part* of the space of flow, for example to secretly infiltrate computers or to detect and eventually combat malware. Its surveillance politics are located in between the disciplinary and the control society: it can surveil, persecute and invite self-censorship, but it can also act through the space of flows and influence access through influencing standards, beating the race condition, and redirecting and disconnecting nodes. The centralized network it aims at establishing through surveillance technologies and unidirectional communication flows then provides it with a panoptical power which appears nearly reactionary. But this panoptical power can be used to exercise control in control society's space of flows. The NSA does resort to strategies characteristic for distributed networks and control societies, too, including the infiltration of standards and distributed nodes such as personal computers. But in any case, through establishing a centralized network by attacking the network where it is most vulnerable, at its open protocols, and using the advantage of the decentralized physical structure beneath, their strategy of control seems to regress back to the forms of the disciplinary society. The NSA seems to aspire controlling the distributed network by letting it exist on the one infrastructural layer that average users experience. The NSA maintains its authoritarian position by combining its geographical advantage within the internet's physical infrastructure with strategic operations upon the protocological layer.

From this position, it operates upon the distributed protocological layer by striving to control standard committees, by infecting single computers, but also by creating cultural codes. For example, the agency has their own markers by which they decide on whether someone is a target, and usually

these markers are activated once someone visits a specific site (i.eg. Inspire magazine), contacts a certain person (i.eg. a known suspect), or uses a certain service (the Tor browser), or if someone is active in a specific religion (Greenwald & Hussain, 2014; Rich & DeLong, 2013). Thus it creates forbidden areas on the net anyone who wishes to stay a spotless member of society better shies away from – it creates cultural codes that regulate access to information and imply certain rules of how to interact within and act upon the network. It becomes the power elites Castells speaks about – situated outside the space of flows but dominating the codes embedded in its structure. Again, this control over the rules of the network is established by the centralized power of surveillance. The NSA can only hold this privileged position of being able to control, because it creates its own centralized network on top which gives it overview and executive power.

Chapter 5: New Techno-Politics

At this point we have gained a deeper understanding of how the internet's techno-politics work. Back in 1927, John Dewey already believed technological structures are a major concern of politics. In the second chapter I presented his political thought which came out of the philosophy of pragmatism. In extension to his framework, I have in the third chapter proposed a methodology for investigating and analyzing technological infrastructures like the internet in detail. This contributed to Dewey's framework because it helps us to understand how politics can be carried out *through* networks, making them inherently political. Whereas Dewey saw political structures mainly as *responding* to or *preventing* technological changes, we now see how political groups *use* these structures to shape society and political culture. On the internet, this is possible because it consists of a multiplicity of quite different networks leveled on each other.

It is only when these different networks are *operated*, both as surveillance and counter-surveillance technologies, so when they are the subject of a conscious activity, that a defined form of organization – to be described by network diagrams – emerges. If this technological activity is used for a political purpose, namely for the regulation and control of the interactions of people, and gives rise to a global public connected by the network, it then becomes techno-politics. In the former chapter we have then seen how the internet is built up and how surveillance and counter-surveillance technologies operate within the different layers. This provided us with an understanding of how surveillance techno-politics are carried out on the internet and in practice, and how the struggle between the two opposing groups – NSA surveillance and counter-surveillance movements – is essentially a struggle between structurally different networks. In this final chapter of my work I would like to discuss which conclusions we can draw from my research results. What does the inquiry into the technological dimensions of the internet infrastructure and into the operation of surveillance and counter-surveillance technologies tell us about the techno-politics of surveillance? How should we evaluate this form of politics and what can its reveal about the applicability of Dewey's concepts today? How ought we to judge current techno-politics, at least those of internet surveillance, against the demands of democracy?

So in this last chapter of my paper I now discuss what the results of my research, and the network struggle we identified, imply for the conduct of contemporary politics and their democratic justification. In the first part of this last chapter I discuss how the practice of surveillance and counter-surveillance and the network struggle between the two impact on and transform Dewey's understanding of politics, marking a transition to techno-politics. I then discuss if and how the techno-politics we have seen, and the different network types they struggle for, can be considered democratic politics. Finally I sketch out how my pragmatic approach to techno-politics can

subsequently build a fundament for future research and for understanding the experience of the new techno-politics. My research in this paper was confined to a very specific topic or case, namely contemporary surveillance and counter-surveillance politics on the internet. An interesting point for further research would be to empirically verify the transferability of this kind of techno-politics to the regulation of other technological infrastructures. This would imply other infrastructures also have a layering which incorporates contradictions. A comprehensive body of research on the topic would, possibly together with a comparative study of older forms of politics, elucidate whether we are witnessing a change in politics as a whole, and if yes, which kind of change. This change might then stand in relation to the globalization of techno-political structures.

Techno-Politics as Network(ed) Struggles

A new territory for techno-politics.

The research results of my analysis of NSA surveillance and counter-surveillance technologies proved to support the importance Dewey's ideas still have today. His understanding of politics emerged from a philosophy where human beings are seen to be deeply embedded in an environment. Because they are constantly engaged in activity, and this activity happens within and on the environment, they are in a constant experimental process of mutual co-shaping with it. Since they have the ability to reflect on this experimental process, they can consciously shape it: this is where technology happens. For pragmatists, technology described a process – this is why I have often spoken of a 'technological enterprise' – in which techniques are consciously and purposefully employed on "raw materials and intermediate stock parts" so that these can fulfill a specific function (Hickman, 2001, p. 12). For example, employing surveillance technologies strategically on and in the internet can shape the way it organizes interactions so it enables a space that offers centralized control or preserves the autonomy of its participants. Thus, through technological activity, people can organize social structures in a specific way. Within these structures, communities can emerge wherever people purposefully interact with each other. By creating large technological networks like the internet, people can interact in different ways and on a different scope, exchanging or spreading information, communicating and engaging in joint activities. The network offers them a platform where they can meet and come together in communities. In *The Rise of the Network Society*, Castells (1996) explored how new global networks profoundly shape and change modern society, because they enable flows that bring forth interactions and consequently new spaces. He described how the way the network channels and enables flows impacts on socio-political relations. When looking at the internet's physical layer, we could see how geographic relations are changed by the bandwidth certain cable connections provide, and how the protocological layer on top aims at changing relations so they become independent of location in the network. We have seen how the internet

builds a new global network in which people are implied in a shared network of interactions, and how its structures create spaces in which social relations are materially manifested.

For Dewey, politics are concerned with the organizing of these networks in a way that they regulate, channel and coordinate human interactions; the internet's network politics here are a perfect example. Regulation can be enacted by creating policies and laws which regulate the relationship between actions and their consequences. As the internet builds a network in which people are implied in a shared space of interactions, it gives rise to the aspiration to govern the infrastructure in order to organize the interactions which are carried out in it. The surveillance techno-politics we have seen aimed at shaping, and consequently regulating, the spaces created by the internet, but not through policies but through applying technologies that change or influence the network's structures. Through this techno-political enterprise, they can create a specific social structure in which control and power are distributed according to a specific form, so in which the actions of certain parties influence the activities of others in a specific way. In the centralized surveillance network the NSA strives towards, it has oversight over all the network's (communication) flows and can ultimately control them. In the distributed network, control is embedded in the rules that prescribe what can and cannot be done on the network. These rules count equally for all – the network's participants are equally autonomous entities who can interact with any other without having to consult an authority.

Techno-politics & infrastructures.

The case of internet surveillance shows how important the governance of the internet infrastructure is in current politics. Surveillance is a form of politics, because it organizes the channels of human interaction in a specific way and achieves systematic regulation of the consequences of actions through indirectly controlling behavior. Indirect forms of control can be embedded in the network's structure: in a centralized network, through surveillance and persecution, forbidden areas can be created; in the distributed network protocological rules can define what one can and cannot do. Surveillance is a form of techno-politics because, in organizing these channels, technological and political developments co-influence each other. Because, like pragmatism described, there is this constant experimental change going on, because human-environment-society relationships are constantly changing through the impact activities have, politics need to constantly adapt their endeavor and become part of this experimental process. As Dewey said, "modifiable and altering human habits[14] […] generate political phenomena", political facts as he called them (Dewey, 1927, p. 6). Had it not been for the internet, comprehensive surveillance would not have been possible, had it not been for its physical layer, it would have been much more challenging. Here technological

[14] That is automized and internalized techniques which can be carried out without active reflection on one's activity.

structures induced certain politics. On the other hand, we have seen how politics influence the make-up of technological structures in order to reach political goals. As such, specific technologies and infrastructural configurations are a result of political aspirations which use them to govern and control societies.

In taking a close look at the composition of the internet, we could see how the specific contextual make-up of an infrastructure can define the way social relationships are structured and the way interactions can be carried out. Here, the approach philosophy of technology takes, namely taking a close look at how technological structures function and which social norms they can embed, enriches Dewey's (political) philosophy. Philosophers of technology and STS scholars have long argued how technologies emerge out of an experimental process in which they are co-shaped by the social circumstances and ideals of their designers and users. I took up this perspective and explained how infrastructures describe the technological ordering of things, of flows and goods. As such they build the technical complexes which ride underneath social phenomena. The specific way different infrastructural components are assembled can be described by network diagrams which illuminate the social relations the assemblage embeds – thus they describe different spaces. In their research, Star and Bowker (2006) described how infrastructures always consist of yet another layer underneath, because depending on which phenomenon one looks at, the underlying structure will be a different one. And because the network diagram which describes an infrastructure crucially depends on the way social practices configure its parts, infrastructure come with inherent contingency. Just as politics can operate through policies and through technologies, infrastructures can be shaped politically and technologically. When looking at the different layers of the internet infrastructure we saw how technological conditions (data transmission media), economic relations (undersea cable companies) and formally defined logical rules (protocols) make for certain network structures. Techno-politics can exploit these different aspects in order to reach their goals.

In the preceding chapter I explained how (NSA) internet surveillance and counter-surveillance movements operate on the internet and how this operation gives rise to specific spaces which embed power structures and organize how people's interaction in the medium are framed. They can do so because the internet as an infrastructure is highly contingent, providing a foundation which enables different spaces of communication. It is only in the way it is operated that specific social relations establish and a particular space emerges. Network diagrams helped me to describe the structural elements of control embedded in the specific configuration of the different layers and the structural form of interaction this configuration allows. This perspective on the techno-political strategies I explored in my work could show a new aspect of politics which Dewey had not anticipated (explicitly). Yes, he saw politics as concerned with the governance of technological

structures and the interactions which propagate through them, but it appears he believed this would be done through policy, legal frameworks and public discourse. He did not dedicate any thought to the exact design of infrastructures and consequently to how politics could not only govern them through (legal) policy and public discourse, but through actually just acting in and on the network. In a sense he did not anticipate the control society in which control *of* infrastructures is directly embedded *in* protocols and access codes. Because he had not considered how infrastructures are designed and used in particular, he did not see the important role the inherent contingency which they come with can play in politics. Snowden himself made clear how the wish to avoid centralized surveillance does not need to be pursued through policies, but can be achieved through encryption technologies. It is this contingency, for the internet expressed very concretely by the different diagrams of its structural layers, which makes this way of politics so interesting and fruitful. It is the struggle over resolving this contingency, over making the specific network, which I called the network struggle. Without having to make policy decisions in a public discourse, politics can now shape social structures by hooking technologies up to the network.

Opposing internet layers.

In the case of internet politics, my research made clear how surveillance techno-politics purposefully exploit the internet's contingent social structure. The key to this lies in its division into structurally different layers. We have seen how the protocological layer structures the internet to be a distributed diagram, where all participants in principle have the same rights and the same weight in the network, where no central authority exists and where communications flow bidirectional between any two participants, based on peer-to-peer. The distributed diagram comes about because communications can bounce from node to node until they have reached their destination and in this way make specific locations irrelevant. The protocological layer can create the space early www-pioneers envisioned: a virtual world of information exchange, uncoupled from the geographic and material circumstances of one's environment. Through acting on the layer by aspiring to change– that is *radicalize* – the protocols, and through acting in the layer by encrypting data, counter-surveillance movements appear to strengthen the distributed network protocols are supposed to bring about. On the other hand, surveillance technologies aim at establishing a centralized network where the NSA builds the major hub. From this hub it can in principle oversee the whole network and control and induce communication flows. For building this network, the NSA exploits the decentralized physical layer and its strategic position within its global geography. Its surveillance strategy is based on the fact that the internet's space of flows, on its most fundamental layer, is still bound to a geography in which locations matter. This geography comes with specific relations determined by how physical data flows happen – many of its important IXPs are located in the US or on the soil of its allies. Using this, the NSA acts on the network and creates new channels of

information flows, influencing technological practices. For instance in their program Quantumtheory they also act in the network, using its protocological data flows to infiltrate computers.

The case has shown how, in contradiction to Dewey's tone, a traditional institution can be very apt and up-to-date to respond to new technological structures with suitable techno-political methods. They can do so because the internet as a technological network is contingent and (still) in a process of constant development. Interestingly, the NSA's way of acting on the network seems to advance an old form of control (disciplinary surveillance) and not the form of control which distributed networks and control societies bring with them (distributed access control embedded in protocols). They only employ strategies inherent to control societies to weaken the protocols so that they do not interrupt with surveillance, a characteristic feature of the disciplinary society. But they do not influence the shaping of protocols in a way that they bare only to certain areas or allow only specific activities. That they are on the cutting edge of practically operating techno-politics does not mean what they do is democratic, but that it is well adjusted to the technological conditions of the time and displays profound understanding of technological structures. However, counter-surveillance technologies have means to respond and counter the NSA's strategy. They are aware of the internet's contingency and potential openness which can be exploited through operating on a different layer. Dewey thought people would have to organize into publics which appoint (governmental) officials which shape policies in their interests. He did not foresee how regular people could use their technological expertise to act upon the network in a way which influences its social organization, and how they would do so out of political motivation. He also did not foresee how people could just circumvent government policies by using and creating new technologies (i.eg. encryption programs). What we see with counter-surveillance movements and the technologies they come up with is how citizens can use technology politically and challenge the structures political institutions aim at establishing, changing the channels of human interaction.

Techno-politics & network struggles.

I have suggested understanding this form of politics which my research results made visible, a politics which picks up issues brought by technological changes and corresponds to them through technological activity, as *techno-politics*. By explicating practices of current surveillance techno-politics, in the preceding chapter I have given extensive examples of how these techno-politics operate. They are not only called techno-politics because they are concerned with technologies in the colloquial sense of the word, but their political activity is deeply technological in the more sophisticated conceptualization of technology the pragmatic approach suggested. Techno-politics involve reflection and active inquiry because they depend on extensive knowledge of the network's composition and functionality, and they use this inquiry to apply "intelligent techniques", that is conscious purposeful (technological) action, to "raw material and intermediate stock parts", the

infrastructural components, in order to reach the aspired political aim – to reach a special structure of social control (Hickman, 2001, p. 12). Hence, also within the pragmatic conception, this form of politics is a deeply technological enterprise. Techno-politics actually appear to radicalize a pragmatic view on politics, because they describe how political structures and ambitions are *pursued* – they take activity, not discourse, as the starting point. Instead of regulating people's interactions through policies and guidelines, techno-politics create social structures through technologies and by creating a specific network type. My paper could show this because it married Dewey's account, which in principle was open to a conceptualization of networks as intrinsic to politics, by taking seriously the approach philosophy of technology suggests. By using the work of Star and Bowker, Galloway and Castells I could find a way to conceptualize and investigate how politics can operate through technologies and technological networks and in this way organize (that is influence and shape) channels of human interaction.

This approach could show how surveillance techno-politics can be understood as network struggles because the opponents strive towards different network types. In the case of NSA surveillance, this network is a centralized network with the NSA on top. Counter-surveillance movements, opposed to the socio-political structure the NSA envisions, respond to this way of politics through technological activity, too. Thus, in techno-politics, the experimental process in which Dewey saw communities and societies constantly involved, gets carried into the operation of techno-politics. Political camps constantly adapt to new technological conditions, possibly brought about by their opponents, and act on them by trying to find a way to technologically change the network's structure. Consequently, current surveillance techno-politics turn out to be a network(ed) struggle: a struggle between networked forces which are part of the broader network internet, and a struggle between the different network types which are aspired to dominate the infrastructure globally. The different network diagrams describe different modes of interaction, resulting in different consequences following actions. These network types come, so I discussed in the last chapter, with different forms of control and they distribute power differently.

Global Publics & Democracy

With the framework Dewey has provided for understanding (representative) democracy, we can realize how both the centralized surveillance network and the distributed counter-surveillance network are not inherently democratic structures. Whereas the centralized NSA surveillance network operates secretly and governs a global network as a national institution, counter-surveillance and its distributed network do also not work through democratic representation. As such both cannot live up to the demands of democratically representing the global public they impact on. Recognizing this might lead us to rethink how to govern the internet and its global public, technologically and

politically. I can here only superficially touch upon eventual solutions. Future research then ought to be dedicated not only on how to balance security and freedom, which are as we have seen very context dependent anyways, but also on how to structure and govern the network in a way which can take the democratic rights of its political public into account.

By making apparent the technological forces making for consolidation, the structure and scope of these networked forces and their internal power structures, Dewey's pragmatic approach can inform the inquiry into current political practices and can contribute important insights to the discourse. We can see how surveillance techno-politics on the internet concern a global public, while being executed out of sight and by institutions justified only on a national level. This tension has implications for its political legitimization. As I explained in the second chapter, Dewey's account of democracy centered on the emergence of political publics which are bound together by the consolidating forces of technological structures and which ought to organize and let officials represent their interests. Dewey argued that when people are mutually affected by a shared technological structure and the corresponding global techno-politics, the structure gives rise to a common public. In order to exercise its democratic rights on a political level, so Dewey, this public ought to organize and appoint officials which act on its behalf. He believed in a democratic political structure, open political discourse and accurate representation of the public's interests ought to take center stage.

New techno-politics.

Awareness of and high level of information about the technological forces shaping our interactions is crucial for us to understand causal relationships and power structures at work and to identify the public we are part of. This, so Dewey, is necessary to overcome the eclipse of the public which results out of the complexity of new technological infrastructures and the operation of techno-politics outside people's awareness. Only then can we develop concepts and ideas of how to deal with them accurately. We saw this exemplified by the network struggles which give rise to specific conceptualizations of security. If we are unaware of the networks values correspond to, judging their implications and desirability is very difficult, as is judging existing political institutions. In line with this, Dewey's idea of democracy was very much based on informed representation and it appears he believed solutions to emerging issues would then be formed through discourse and joint inquiry and enacted through policies. These policies would regulate the technological forces, for him still extrinsic to political forms, in a democratic manner. In the case of internet surveillance politics, we see a shift in how politics are done. In techno-politics, technological changes are intrinsic to political forms, and they do not work (solely) through policies, but through (technological) action. So whereas Dewey's politics worked through discourse and representation, techno-politics work through actively shaping the network technologically. Publics on the other hand can do the same – with internet activism we

actually see how opposition groups also enact their political views through influencing the network as do counter-surveillance technologies.

Global public.

As the disclosure of NSA surveillance and the results of my research unearthed, the NSA uses its geographic advantage to create a global surveillance network. It ultimately aspires to overview the geography of a global space of flows. As the internet infrastructure connects people all around the globe, making them part of a shared space of flows, and as it is their data which gets surveilled by a US American agency as well as their devices which are infiltrated, people around the globe are mutually concerned. We have seen how surveillance and counter-surveillance activities impact on all citizens of the web, because they change the network structurally, impacting on communication structures in general. The geography of the internet's space of flows is global – its major hubs are major global cities (Figure 4) like London, Frankfurt, Paris, Amsterdam, New York etc. These hubs are the focal points of global information flows, similar to capitals in nation states. As the analysis of NSA programs like PRISM, Upstream and Quantumtheory showed, they are the basis for establishing global oversight and eventually control over the network and for establishing hierarchical communication structures. Hence, the surveillance network the NSA and its programs build up is a global network, and this global network comes with a global public.

For Dewey, for people to become part of a common public the decisive factor is that "the consequences […of (inter)actions] expand beyond those directly engaged in producing them" (Dewey, 1927, p. 27), so that they are part of a complex space of flows and its social relations. The public's members then have a shared interest in the regulation of the network's structures. Global internet activist groups are good examples of how issues around the regulation of a shared internet with shared practices bring together people globally. People around the world are concerned with and affected by its regulation. The more transactions are carried out through this infrastructure, the stronger these mutual bonds become. Users of the internet then become part of a vast, diverse and widely distributed public. Through building a shadow network which connects to the internet's global hubs and changes the network's communication structures, developing copied data flows and infiltrating communications, the NSA impacts on the network's structure globally. In this way, it concerns a global public. Even US president Obama acknowledged the global public the NSA affects by its surveillance programs, and hinted at how it conceives a responsibility to govern interactions globally. In a speech about NSA surveillance on January 14th 2014, which he gave in reaction to Snowden's going public, he pointed out how the NSA is concerned with the lives of people *around* the world, saying the programs' "efforts have prevented multiple attacks and saved innocent lives, not just here in the United States, *but around the globe*." (Wall Street Journal, 2014, 5'48). He pointed to the US' self-concept of having a special role globally and responsibility for people around

the world, a view according to him shared by other countries' leadership. It seems this special role partly comes out of the US unique capabilities for comprehensive global surveillance, which, as we found out in the last chapter, has to do with their location on the internet's very own geography. In his speech, Obama said:

> Meanwhile, a number of countries, including some who have loudly criticized the NSA, privately acknowledge that America has *special responsibilities as the world's only superpower*, that our *intelligence capabilities are critical to meeting these responsibilities* and that they themselves have relied on the information we obtain to protect their own people. (Wall Street Journal, 2014, 17'52, my emphasis)

Invisibility.

But even though the NSA responds to this global public and fundamentally impacts on the network, its surveillance technologies are distinguished by invisibility, operating unnoticed and outside people's experiences. Both because this simplifies gathering data *and* because they want to stay secret, they operate on deeper infrastructural layers. As infrastructures are always below experienced phenomena and meant to become transparent, it is not surprising the NSA's activities then become invisible. Already with the example of electricity, Dewey recognized how technological structures which govern interactions are unknown, while only their effects are experienced. The problem with internet politics is not so much the invisibility of infrastructures but the fact that, instead of the conditions of governance being negotiated in a public discourse and in the awareness of people, techno-politics themselves operate on the infrastructure and become invisible, too. They take advantage of the invisibility of infrastructures in order to exercise politics outside democratic legitimization and to influence the space of flows unnoticeably to the public eye. Operating on underlying infrastructural layers, the centralized surveillance network is invisible and operates outside the internet we interact with. So the NSA surveillance technologies consciously operate in secret (or so we assume).

Because they operate invisibly on lower layers of the infrastructure and outside the internet's space of flows we interact with, it is difficult for people to become aware of the socio-technical structure of which they become part; it makes organizing as a common public difficult. If people cannot realize how the political regulation of social channels is enacted and experience the (technological) structures in which they find themselves, they cannot use these insights to form a public and have a joint discourse based on rational inquiry into the technological forces. In this sense, Edward Snowden's whistleblowing and the work of those who supported his strive for an open public discussion on surveillance can be considered acts to further a democratic climate. They took part in bringing about conditions for overcoming the eclipse of the public and the invisibility of the

underlying technological forces making for consolidation. They provided the necessary information for understanding the network's specifics which structure our interactions and imply people in a shared web of consequences. They opened up a public discourse on one of the most pressing issues of contemporary techno-politics and they provided a means for checking up on the actions officials carry out on behalf of the public, nourishing the free exchange of information and the unlimited access to it. Like Dewey, they believe restriction on information impedes the search for knowledge and stops us from finding the best solution to techno-political problems.

The problem the high secrecy of surveillance activities poses to democracy might arise out of a general problem with secret services, whose role Dewey did not consider. Obama's strongest point to end the discussion might be that "intelligence agencies cannot function without secrecy, which makes their work less subject to public debate" (Wall Street Journal, 2014, 8'58). But further discussion is warranted on how we ought to deal with secret agencies especially when their possibilities and responsibilities change. In this thesis we have witnessed a shift from politics which are executed through discourse to politics which are done by technological activity – techno-politics. This shift is surely furthered by the possibilities ICT infrastructures and the new geography of the space of flows bring. Secret agencies might just happen to be the best equipped for this and start to take on more responsibilities. The NSA's activities appear to expand traditional political espionage on foreign adversaries: the NSA actually strives towards a privileged position to control a global network. It is here not only concerned with spying on foreign forces, but it actually operates on the network in such a way that it takes on responsibility for a global public. Thus, how to deal with such 'new' secret agencies is an important topic of further research. Partly because of this secrecy and partly because of the complexity and extensiveness of the internet infrastructure, the common public is not apt to timely adjust to these new technological forces or to even ponder about how they should be governed. Because these techno-politics operate outside their level of experience, they are majorly unconcerned by it and if at all experience the consequences indirectly and obscurely.

Global publics & nation states.

But even if NSA's activities would be democratically justified within the existing political landscape, within the nation state system, this justification would not concern the public it should concern. The NSA is a national institution, even though it acts on an international network. A democratic justification would then only apply to US citizens. In accordance with this, the NSA also only acts on behalf of a nation state. The United States' government has repeatedly made it clear that NSA's activities are concerned with the interests of US persons. After all, they always name one significant reason for dragnet surveillance – the attacks on September 11th 2001, a single event explicitly carried out specifically against the United States of America. Even though they share signal intelligence with other countries (Spiegel Staff, 2013), their priority is always to ensure the advantage

of their country. They are only interested in representing the interests of foreign citizens when these coincide with their own.

And even if the NSA would be subjected to democratic scrutiny, democratic mechanisms would be confined to the American national community. To include the National Security Agency and its activities within the democratic system of checks and balances would only empower American citizens. But the NSA's activities, which increased under the Bush administration as a response to the attacks, expand around the whole globe. This means they concern a diverse network in which people all around the world are implied in and directly refer to the global governance of one of the most important global infrastructures. The NSA concerns citizens not nationally but globally and significantly changes the world's most extensive global network profoundly. The NSA however has no democratic justification from those who it concerns and also does not act upon this public's behalf. Dewey believed political decisions are only those which are made in the interest of the public (the concern) and not out of personal advantage (i.eg. to achieve benefits from preeminence in the socio-technical structure). So if the NSA does not act on behalf of the public it concerns, but for example on behalf of its own supremacy or the national security of a fraction of the public, its decisions might even, for Dewey, not be political decisions at all.

Whereas in the virtual world we experience disassociation from places and enter into a space of global flows, on the political stage we are still part of a system based on the sovereignty of nation states. The geography of the internet's space of flows, manifested in its physical layer, connects to nation states and can bring about specific power relations between them. And even though on the internet we are part of a common political space with people around the globe, otherwise we are still very much embedded in local cultural and political context. This is a serious obstacle for us to realize the political society we are part of, to communicate with others and identify common issues and aims, and to organize politically. Given the diversity of internet users and their difference in culture, language, private, political and economic aims and belief systems, such a global organization of the public, abounding from its eclipse, seems hard to imagine. However, Dewey believed publics form as a response to specific perceived problems, associated with (technological) infrastructures. Its members do not need to agree on all issues; rather they should be drawn together around specific issues. Creating the internet as a space with a specific structure could be such an issue. It is actually this shared moral framework around a particular issue which can bring together global internet activist groups like Anonymous.

Dewey did not anticipate such a global public, because he was sure distant "social groups [would be] so separated by rivers, seas and mountains, by strange languages and gods, that what one of them does – save in war – has no appreciable consequences for another" (Dewey, 1927, p. 42).

Hence, they would never be in need to form a public around techno-political issues. In the case of internet techno-politics however, people become connected by a network so that their actions have appreciable consequences also on very different social groups. The effects on the global network structure surveillance and counter-surveillance have made this clear. In a way however, the NSA (and the US) seems to be keen to counter such a finding of the public rhetorically. For one, they separate the global from the national public, putting things within very national frameworks: in justifying the programs, the government appeals to Americans (nearly) exclusively and emphasizes how it surveils US citizens differently. This can actually give rise to the impression that Americans are somewhat differently concerned and hence build a particular public. (As the disclosures continue we learn more and more how there was no clear cut difference between surveilling US citizens and others.) Next to that, Dewey saw a difference in the case of war where (national) publics would stand in opposition and consciously induce negative effects on each other. The rhetoric around the NSA is signified by war slang: national security is overly emphasized, a term which emphasizes a country-versus-a foreign force situation; additionally they repeatedly justified new drastic surveillance programs as being necessary in a time of high emergency, in times of the 'war on terror'.

Globalization & institutions.

But even if this global public would illuminate, it would not have any political structures through which it could act or to which it could appoint representative officials. When it comes to organized politics we are still very much bound to a state level. The internet however offers a new, sort of parallel, world in which we live next to our local context. The NSA acts within this global world, but it does so on behalf of a nation state bound to the context of politics outside the net. There is a tension here between the NSA's global public, for which Obama partly took on responsibility (see quote above), and the NSA's emphasis on providing *national* security. Due to this tension, Obama had to perform a balancing act in his speech. On the one hand he said he wanted to let people around the world know the US wasn't spying on "ordinary people", regardless of their nationality, and said he wanted the trust from people around the world. On the other hand, he specifically addressed US citizens ("the American people") and emphasized the need of the surveillance programs for providing national security, positioning them as normal activities of nation-states and emphasizing how all countries are concerned with spying. (Wall Street Journal, 2014).

In any event, global public governance of internet infrastructures would trouble the concept of the nation state we have had so far and its responsibilities; it directly ties into current debates around globalization. Even though he had no concept of such a global network like the internet, Dewey already had a fluent conception of the state. What was difficult for him to imagine back then was that there could at the same time exist a global space like the internet while on the other hand people would still live their lives outside this space based on a nation state system. For him, the

whole of associations within a given community would be contained in a place, would be part of geographic container which then maps out the nation state. However the space of flows transcends the boundaries of such a national container. While the internet creates a new space with new international structures, its significant locations are still on national territories and advantaged player like the US or Germany can exploit this. In Dewey's explanations on democracy, international or inter-state relations are not taken into account. He did not expand on how comprehensive global networks that extend trade relations can exist simultaneously within a national organization of political communities. His mode of democratic thinking appears to be very much restricted to the governance of state-like territories. Even though he acknowledged the boundaries of states to be fluent, it seems unlikely he anticipated such a profound global network like the internet. On the one hand he might have cheered in the face of the informational resources it provides, on the other hand he might have cringed when asked how to govern it democratically.

Concluding it can be said that the surveillance institution NSA works outside democratic political frameworks for two reasons: for one it does not make its politics part of the public discourse, but instead obscures its profound and comprehensive activities on the network, surrounding them by secrecy. In this way people do not have the ability to become aware of the underlying forces making for consolidation, or jointly inquire them to find a common solution to issues which takes into account the public's needs. Secondly, the NSA operates like a global institution. By operating on the new geography of the space of flows, it puts itself in a privileged position within a global network. As such it concerns a global public while operating in the interests of a single nation state (if at all). In light of these insights, it seems Dewey was right when he described how new infrastructures transform the technological forces making for consolidation and call for new political structures. It also seems accurate when he described how institutions which emerged out of former structures still channel the flows of interactions, but do not anymore present the accurate institution for representing the public they ought to govern. In this case he even went so far as to propose the new public should "break existing political forms" (institutions) in possibly even revolutionary manner (Dewey, 1927, p. 31). Maybe new counter-surveillance movements and especially groups like Anonymous see themselves in this revolutionary position and as enacting the interest of a global public. But to what extend can they be considered as an accurate democratic response to the new challenges global surveillance brings about?

The distributed network & democracy.

I argued the technological practices of counter-surveillance movements aim at strengthening the distributed network. The distributed protocological network, by its very properties, is more an anarchistic than a democratic network. It is marked by the absence of authorities. Each node is autonomous and has equal rights to all other nodes. There are no official representatives acting on

behalf of a group or community. Control in the distributed network does not work through surveillance, but by implementing rules in the protocols which regulate behavior by denying and barring access. These rules can be designed from outside, through the dictate of an authority or through democratic decision making[15]. Hacker and counter-surveillance groups operate on the protocological layer and envision the distributed network. They support a specific organizational form because it represents the network they promote. It is therefore no wonder they gravitate more towards an anarchistic form of organization than a democratic system in Dewey's sense. But Dewey proposed a representative democracy in which the public would assemble and then appoint or elect officials that represent its interests and shape socio-technological dimensions accordingly through institutional power. However, in the case of global internet politics we have seen how democracy is not enacted, due to the vast scope of the network, the contradiction between the global and the national, and the absence of suitable political structures.

Maybe, just as Dewey came to conclude that democracy emerged as a response to misdirected politics and happened to appear as the best political structure to organize and benefit people at the time, anarchistic movements are now a response to a failed democratic politics in the light of a globally distributed structure. The fact that politics can now be enacted through techno-politics contributes to this. When it comes to the internet, people and political groups are no longer dependent on being represented accurately by governmental officials but can themselves do techno-politics. We have seen how counter-surveillance technologies become political because they can support to channel communications structures according to a specific form. They can create new networks with new properties, they can fight the surveillance network with encryption tools, they can spread the word worldwide on the internet and they can attack existing institutions through the intelligent use of the internet infrastructure and its technologies. However, they too operate outside democratic frameworks, because they do away with public discourse, at least in their technological operation. It is true that counter-surveillance movements, most of all Edward Snowden, are often very interested in furthering the public discourse about government control of the internet and that they, much more than secret surveillance agencies, aim at making apparent the underlying technological forces. They often even set out to teach people on how to use technologies so as to avoid becoming part of the centralized network. However, in their techno-political activities on the network, they also enact politics without people's awareness and without consulting the public. By simply acting on the network, and especially on infrastructural layers which disappear under the

[15] To find out about common standardization and protocol development organizations and committees like the Internet Corporation for Assigned Names and Numbers (ICANN), Internet Engineering Task Force (IETF), Institute of Electrical and Electronics Engineers (IEEE), see Galloway, 2004, p. 119 ff. and Berners-Lee, 1999, p. 91 ff. These comittees often in principle have open processes of decision making but in practice consit of a relatively small number of internet experts. Political and economic stakeholders, who have a severe interest in shaping the protocols (like i.eg. the NSA) often also play a major part

surface of the user interface, both surveillance and counter-surveillance technologies avoid public discourse. Hacker groups which enact their own moral framework through technologies then also become elites, because they have access to technological knowledge most people do not have and can employ it to their advantage. Hacking attacks aimed at taking down a particular server or infecting a particular website only represent the interests of those who carry these actions out. This is the distributed network where entities act autonomously. Additionally, the processes of developing and implementing encryption technologies and similar often happen outside regular people's attention. They only – if at all – become aware of them when a green lock blinks in their browser.

Counter-surveillance publics.

Still, the distributed layer of the internet provides a great medium for people to communicate and exchange information, and hence to organize as a (global) public outside regular institution forms. It allows them to recognize the existence of distant people who share their views and worries and to learn about the workings and effects of technological structures. At the same time, because it offers so much autonomy, it accommodates people with very different interests and world views. On the internet, there coexist many different communities with their own languages, cultures, religions, ethnicities, agendas, beliefs, purposes and goals, it seems impossible to integrate them all into a unified public discourse. All these different groups may have different visions of how the internet is supposed to work and for what purpose. But while all these groups coexist and share a common infrastructure, certain specific issues pop up as a result from this interaction. In Dewey's eyes, publics form because of the shared experience of the effects of technological infrastructures. Even though community is genuinely moral for him, publics still arise out of a response to certain techno-political issues. They need not share *all* of their moral beliefs but instead develop a shared moral framework directed towards *certain* issues. For example, cultural differences between the US, India, Germany and Syria are huge. Still, people of all cultures might hold a belief in the power of free information and in the destructive force of censorship. Their motivations might be different, but when they communicate and realize they share a goal, they can recognize their shared affiliation to a moral community that revolves around issues of internet freedom.

In fact we see this effect in popular internet activist groups. Anonymous is organized as a distributed network in which anybody can join – in fact they state they are *not* organized at all (Anonymous Inof, 2010). But when I say "them" I only refer to the opinion of those who made a video about joining Anonymous and uploaded it on YouTube. Because the network has not authorities and no representatives and every participant in the network is autonomous, no single individual or group can ever represent Anonymous. Members are loosely associated and always only speak on behalf of themselves. If spokespeople emerge, this is only indebted to their increased

activity and visibility, to their commitment to a cause and their willingness to speak up. They can claim to represent a general sentiment within the group but they cannot claim to *represent* the views of all members or to have been entrusted with acting on their behalf. Membership of such a group is only loosely defined and by simply *being* Anonymous, one becomes Anonymous. In their video, they claim that you *cannot* join Anonymous, because there is no authority that legalizes membership, there is no database to register; there is no procedure to go through. As a distributed network, connection to the Anonymous group is simply enacted by connecting *to* the network; it works through protocols. Becoming a part of Anonymous is actualized *by action*. At the same time it builds a moral community. Through its development process a certain but very open moral code has developed. In fact in many of the hacking activities attributed to Anonymous, it seems the group understands itself as a sort of moral police that actively promotes freedom of speech, freedom of information, democracy and the fight against government authorities, what is understands as illegitimate governmental actions, Scientology's ideology and corruption, Nazism, etc. In this way the community grows a certain moral climate. But consent to its most prevalent moral views is not a necessity – because one becomes part through connecting to the network without anyone checking up, it is irrelevant what one believes. As a group, they act upon *issues*. It is possible for someone to join the group only for the promotion of a certain cause some of its members share.

A democratic network?

Some of the aspirations of counter-surveillance movements are in the service of democracy, because they a) aspire a climate of free information sharing and exchange, b) invite us to inquire into the technological forces making for consolidation, and c) build public groups around certain issues, whose members share (certain) moral values. However, the distributed network they aspire does not incorporate mechanisms of representative democracy. On the contrary, groups like Anonymous actively try to work without representation, refusing to take responsibility for the actions of their members. In the anarchistic network they envision, entities are completely autonomous. The surveillance politics of the NSA does also not appear as a democratic form of politics: a) they operate outside the public's awareness and their actions are hence not subjected to public discourse and b) they, if at all, represent the interests of a nation state while concerning a global public. They operate through an invisible and centralized network of unidirectional information flows, while for Dewey democracy should be signified by bidirectional information flows between the public and its representatives. The public appoints the representatives which act in its interest, while their activities are constantly subjected to the public's scrutiny. In Dewey's vision, the experimental process of democracy works through discourse, while in techno-politics it works through technological activity which often leaves eventual democratic rights of the public aside and operates outside their awareness.

Before I have said there is a difference between speaking of an *inherently* democratic network and democratic *governance of* another network. As Castells said, in the space of flows elites are situated outside, dominating the (cultural) codes in a way which works to their advantage. In the centralized network, the NSA is such an elite because it technologically keeps itself outside the flows, working through copied data streams. However, elites could also influence the making of standards from outside a distributed network. For example, if encryption and hence freedom from surveillance depends on advanced technological knowledge, then hackers also build a sort of elite groups which has exclusive access to the space of flows outside surveillance. What I have explored in my thesis were the inherent structural traits of technological networks and not the organizational form of their external governance, or the way these networks are shaped through policy. Both the distributed network and the centralized network could potentially be governed from outside, by a democratic decision making process of shaping the protocological rules or by appointing officials who control the network form a central hub *in* the interest of the public – or possibly a combination of both. Surveillance as such does not per se have to be undemocratic. Surveillance might be acceptable if it were subjected to democratic mechanisms. If information about surveillance programs was available in detail and these would subject to an open democratic discourse and represented by legitimate officials, it could be democratically justified[16]. In this way, the executive channels of techno-politics would enter our awareness and be an open topic to discuss. I would envisage a democratic network to be more of as decentralized than a distributed or centralized one. The hubs would be the officials and represent the nodes as the public's members. Within this network, information would flow in both directions and the nodes could control the hubs through elective power. The different officials would then get together and shape institutions in a democratic process and according to their mandate. Decisions over the network's structure and eventual surveillance institutions would be made in an open democratic discourse.

To demand democratic governance would imply to extend the network where the space of flows of the internet get connected to other (political) networks which govern and shape it. Thinking about how this network looks like and how it ought to look would then also require to take more parties, and network structures into account. In my thesis I provided a simplified version of the structural diagrams of the internet. However, there are also economic forces which play a role in

[16] I.eg. also in a democratic society, law enforcement agencies have to surveil people to a certain extent in order for the laws to have a function at all. Maybe, another reason why counter-surveillance movements tend to affiliate with anarchy is because a government which is supposed to govern people will always, to a certain extent, need surveillance. And of course, surveillance mechanisms can never fully be out in the open, because they would become useless as people, intending to commit a crime or break (democratically made) laws, could circumvent them. In this line of thought, Dewey's political philosophy even points to a contradiction surveillance an sich poses to democracy. This contradiction is seen to be resolved in a Deleuzian control society where control mechanism are implemented directly into the structures which allow and disallow. Surveillance here becomes superflous because breach of rules implies idleness.

building hubs, for example internet giants like Google. Also, there are more secret services which aim at controlling internet flows, too, and hence challenge the privileged position the NSA is trying to establish. Taking all these factors into account would lead to a more complex picture of ongoing network struggles and would complicate finding a way to govern it further. Additionally, dealing with the global public the internet creates would, according to the demands of Dewian democracy, require having global infrastructures governed by a separate political system than publics inside nation states. Those concerned by the infrastructure would then have democratic rights to influence their governance. Dewey did not offer a framework of how to do this since his political philosophy was confined to nation state-like entities. How such political structures could be put into place would be another important subject to expand on the research done in this paper. The parallel global world of the internet, which coexists to the world's political organization in nation states, would possibly need its own governmental structure. How this could be provided, and how nation states, especially those on which the physical layer's hubs are located, would be forced to tolerate this structure is a difficult subject matter until today.

Future Research on Political Experience

Throughout this chapter, I have already indicated some of the puzzles global surveillance politics, and techno-politics in general pose, and presented starting points for future research. In the introduction I said my aim was to develop a tool for analyzing the transformation of political experience through surveillance technologies by filling the 'technological gab' in surveillance research. By focusing on technological infrastructures and the operation of politics through technologies, I have successfully built a tool which allows us to discuss the issues around global surveillance from a new view point. The inquiry into the technological forces could help us understand which *structures* are at the bottom of the use of words like security in different contexts. It helped us understand how the tension between different techno-political groups is enacted in a struggle between different networks and power structures, and it made clear how the opposition between national politics and global publics comes about and inflicts on democracy.

Subsequently this tool, based on pragmatism's approach to experience can help us conduct future research on the experience of politics and especially techno-politics – an endeavor which has not been done (extensively) yet. Here I can only give some indications on potential starting points. In fact, with the pragmatist approach it is possible to frame experience as *central* to democratic governance. As we have seen in the second chapter, in the pragmatic framework experience has a special status and describes something different than conventional everyday experiences we have during our regular whereabouts. For pragmatists, experience describes a cognitive activity in which we come to terms with novelty and resolve uncertainty, in which specific relations become

conceptualized. In order to do this, we have to be able to engage with the technological forces making for consolidation, either in technologically interacting with them or through making them a topic of inquiry and public discourse. In Dewey's theory of democracy, people need to *experience* the channels of human interaction in order to find solutions to common problems and exercise their democratic rights by appointing and checking officials which govern technological structures in their interest. However, by now we have seen how techno-politics operate invisibly through deeper infrastructural layers outside our experience of the internet, and how this operation is consciously kept secret and obscured in the public discourse. Dewey believed new technological forces would lead to an eclipse of the public, *because of the invisibility of technological infrastructures*. He did not anticipate how political groups could *actively use* this invisibility in order to avoid the democratic rights of people. Due to the eclipse of the technological forces through which techno-politics operate, we do not experience them, and hence cannot perceive of and deal adequately with the underlying issues they pose. Hence, an agency like the NSA which carries out techno-politics unnoticed and outside people's experience, through using deeper infrastructural layers, is *per se* problematic for democracy.

Disclosures such as Snowden's then can induce an experience of techno-politics. They present a disruptive moment, and force us to halt in our habituated use of the internet. By making us reflect actively on the structures which channel our interactions on the web, they invite us to a technological activity in which Dewey saw experience established. Through becoming aware of surveillance, we now become aware of the invisible centralized network. Even though we are still formally free to interact in a distributed network, we know there is a higher authority which controls our interactions. This changes our experience of the network and our activity within it: we might become more cautious or more unsecure. But the diffuse knowledge of being part of a centralized surveillance network without knowing its exact purpose and influence subjects us to a somewhat Kafkaesque law. When secret service agencies are involved, there is no clear line of what is allowed and what is not. The secret FISA courts in the US exemplify such obscurity (Cain Miller & Perlroth, 2013). The absence of an openly discussed, democratically shaped law does not offer us a structure to guide our operations[17]. Because its technological operation is outside our experience, on deeper infrastructural layers and through copied data flows Instead, we need to trust the central authority which controls the network fully. But for Dewey, in a democratic system the public checks on its officials.

[17]This, by the way, could be an approach to explaining why the NSA disclosures did not have any significant impact on the way people use the internet. For one they could just have high confidence in the benevolence of the institution, but on the other hand they might just have no way of knowing how they *should* change their behavior. Even though we now know that we are being surveilled, we do not know to what ends exactly the data is used or to which behavior we should be coerced. This ignorance really makes it hard for us to know *how* to change our internet behavior; as a consequence we might then not change it at all.

Hence, the experience of specific forms of techno-politics will be close to our experience of the network they create. A centralized network could also come with a positive experience. In the centralized network we know that all interactions are monitored and checked upon by a central authority. This protects us from the experience of the viral threat the distributed network poses. And even though we might not be able to oversee the network, and hence the consequences of our actions fully, there is a control function in place which takes responsibility for the network. The anticipation of an authority holding oversight over the network and fulfilling a control function can take away from us the sense of being overstrained by an unclear network. It offers us reassurance that we are not interacting in an anarchistic web of associations, that there is an instance that controls all flows in the network and can protect us from viral threats or acts of terrorism. In a democracy we should then be able to have the justified trust that this authority controls the network on our behalf and according to legal rules. But the centralized surveillance network the NSA establishes operates through hidden eavesdropping outside our realm of active engagement. It operates on deeper infrastructural layers, on the decentralized physical network whose structure the protocols obscure, and it does so in secret: its hidden surveillance is crucially signified by *non-experience*.

List of Abbreviations

ACLU	American Civil Liberties Union
ASCII	American Standard Code for Information Interchange
AT&T	American Telephone and Telegraph Company
EU	European Union
DNS	Domain Name System
GCHQ	Government Communications Headquarters (UK)
HQ	Headquarters
HTML	Hypertext Markup Language
ICT	Information and Communication Technologies
IP	Internet Protocol
ISP	Internet Service Provider
IX/IXP	Internet Exchange Point
NSA	National Security Agency (US)
STA	Semantic Traffic Analyzer
STS	Science and Technology Studies
TCP	Transmission Protocol
UK	United Kingdom
US	United States (of America)
WWW	World Wide Web

List of Figures

Figure 5

References

Ackerman, S. (2013, July 2). Clapper: I gave 'erroneous' answer because I forgot about Patriot Act. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/jul/02/james-clapper-senate-erroneous

Anonymous Inof. (2010, December 15). *How to join Anonymous – A beginner's guide* [Video file]. Retrieved from https://www.youtube.com/watch?v=XQk14FLDPZg

Appelbaum, J., Horchert, J., Reißmann, O., Rosenbach, M., Schindler, J., & Stöcker, C. (2013, December 12). Neue Dokumente: Der geheime Werkzeugkasten der NSA. *Spiegel Online*. Retrieved from http://www.spiegel.de/netzwelt/netzpolitik/neue-dokumente-der-geheime-werkzeugkasten-der-nsa-a-941153.html

Appelbaum, J., Rosenbach, M., Schindler, J., Stark, H. & Stöcker, C. (2013, December 12). NSA-Programm "Quantumtheory": Wie der US-Geheimdienst weltweit Rechner knackt. *Spiegel Online*. Retrieved from http://www.spiegel.de/netzwelt/netzpolitik/quantumtheory-wie-die-nsa-weltweit-rechner-hackt-a-941149.html

Appelbaum, J., Gibson, A., Goetz, J., Kabisch, V., Kampf, L., & Ryge, L. (2014, July 3). NSA targets the privacy-conscious. Retrieved September 6, 2014, from http://daserste.ndr.de/panorama/aktuell/nsa230_page-1.html

Baker, F. (1995, June). Requirements for IP version 4 routers. *The Internet Engineering Task Force (IETF), Network Working Group, Request for Comments: 1812*. Retrieved from http://www.ietf.org/rfc/rfc1812.txt

Bajc, V. (2007). Introduction: Debating surveillance in the age of security. *American Behavioral Scientist, 50*(12), 1567-1591.

Ball, J. (2013, August 21 a). Edward Snowden NSA files: Secret surveillance and our revelations so far. *The Guardian.* Retrieved from http://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations

Ball, J. (2013, September 30 b). NSA stores metadata of millions of web users for up to a year, secret files show. *The Guardian.* Retrieved from http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents

Ball, J., & Hopkins, N. (2013, December 20). GCHQ and NSA targeted charities, Germans, Israeli PM and EU chief. *The Guardian.* Retrieved from http://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner

Ball, K., DiDomenico, M., & Nunan, D. (2014).*The face of the faceless: Big data and the surveillant other*. Working paper. Draft provided by the author (Kirstie Ball).

Ball, K. (2009). Exposure: Exploring the subject of surveillance. *Information, Communication & Society, 12*(5), 639-657.

Bamford, J. (2014, August 22). The most wanted man in the world. *Wired*. Retrieved from http://www.wired.com/2014/08/edward-snowden/

Bamford, J. (2012, March 15). The NSA is building the country's biggest spy center. *Wired*. Retrieved from http://www.wired.com/2012/03/ff_nsadatacenter/all/

Berners-Lee, T. (1999). *Weaving the web: the original design and ultimate destiny of the World Wide Web by its inventor.* New York, NY: HarperCollins.

Blum, A. (2012). *Tubes a journey to the center of the internet*. New York, NY: HarperCollins.

Brey, P. (2007). Ethical aspects of information security and privacy (preprint version). In M. Petković and W. Jonker (Eds.), *Security, Privacy, and Trust in Modern Data Management* (21-36). Berlin: Springer.

CAIDA [Center for Applied Internet Data Analysis] (n.d.). *AS rank: information for a single AS: AS relationship table (AS 7018)*. Retrieved from http://as-rank.caida.org/?mode0=as-info&mode1=as-table&as=7018

Cain Miller, C. & Perlroth, N. (2013, June 28). Secret court declassifies Yahoo's role in disclosure fight. *The New York Times.* Retrieved from http://bits.blogs.nytimes.com/2013/06/28/secret-court-declassifies-yahoos-role-in-disclosure-fight/?_php=true&_type=blogs&_r=0

CCCen [Chaos Computer Club] (2013, December 30). *Through a PRISM, Darkly - Everything we know about NSA spying [30c3]* [Video file]. Retrieved from http://www.youtube.com/watch?v=BMwPe2KqYn4

Cumbers, A., Routledge, P., & Nativel, C. (2008). The entangled geographies of global justice networks. *Progress in Human Geography, 32*(2), 183-201.

Carroll, R. (2013, June 14). Welcome to Utah, the NSA's desert home for eavesdropping on America. *The Guardian.* Retrieved from http://www.theguardian.com/world/2013/jun/14/nsa-utah-data-facility

Castells, M. (1996). The space of flows. *The Rise of the Network Society* (Vol. 1, pp. 376-428). Malden, MA: Blackwell Publisher Inc.

Cisco (2014). *Cisco visual networking index: Forecast and methodology, 2013 – 2018*. Cisco Public. Retrieved from http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.pdf

Damico, A. J. (1978). *Individuality and community: The social and political thought of John Dewey*. Gainesville, FL: University Presses of Florida.

Deleuze, G. (1992). Postscript on the societies of control. *October, 59*, 3-7.

Dewey, J. (1927). *The public and its problems: An essay in political inquiry*. Athens, OH: Swallow Press/Ohio University Press Books.

European Commission (2014, May 13). *Factsheet on the "Right to be Forgotten" ruling (C-131/12)*. Retrieved from http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

Finn, P. (2013, June 27). NSA chief says surveillance programs helped thwart dozens of plots. *The Washington Post*. Retrieved from http://www.washingtonpost.com/world/national-security/nsa-chief-says-surveillance-programs-helped-thwart-dozens-of-plots/2013/06/27/e97ab0a2-df70-11e2-963a-72d740e88c12_story.html

Floridi, L. (2001). Information ethics: an environmental approach to the digital divide. *Philosophy in the Contemporary World, 9*(1), 1-7.

Galloway, A. (2004). *Protocol: how control exists after decentralization*. Cambridge, MA: The MIT Press.

Gellman, B., & Soltani, A. (2013, October 30). NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. *The Washington Post*. Retrieved from http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

Greenwald, G. (2013, July 31). XKeyscore: NSA tool collects 'nearly everything a user does on the internet'. *The Guardian.* Retrieved from http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

Greenwald, G., & MacAskill, E. (2013, June 7). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Greenwald, G., & Hussain, M. (2014, July 9). Meet the Muslim-American leaders the FBI and NSA have been spying on. *The Intercept.* Retrieved from https://firstlook.org/theintercept/2014/07/09/under-surveillance/

Gude, H., Poitras, L., & Rosenbach, M. (2013, August 5). Mass data: transfers from Germany aid US surveillance. *Spiegel Online*. Retrieved from http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html

Horgan, J. (2013, June 7). U.S. never really ended creepy "Total Information Awareness" program. *Scientific American.* Retrieved from http://blogs.scientificamerican.com/cross-check/2013/06/07/u-s-never-really-ended-creepy-total-information-awareness-program/

Frontline PBS (2014, May 20). *The United States of Secret* [video file]. Retrieved from http://www.pbs.org/wgbh/pages/frontline/united-states-of-secrets/#united-states-of-secrets-%28part-two%29

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *The British journal of sociology, 51*(4), 605-622.

Hayase, N. (2011, May 15). *Anonymous in wonderland: The identity of anonymity*. [Blog post]. Retrieved from http://aworldbeyondborders.com/2011/05/15/anonymous-in-wonderland-the-identity-of-anonymity/

Hepting vs. AT&T (2006, June 8). *Declaration of Mark Klein in support of plaintiff's motion for preliminary injunction.* United State District Court. Retrieved from https://www.eff.org/node/55051

Hickman, L. (2001). *Philosophical tools for technological culture: Putting pragmatism to work*. Bloomington, IN: Indiana University Press.

Hildreth, R. W. (2009). Reconstructing Dewey on power. *Political Theory,37*(6), 780-807.

Hill, K. (2013, July 24). Blueprints of NSA's ridiculously expensive data center in Utah suggest it holds less info than thought. *Forbes.* Retrieved from http://www.forbes.com/sites/kashmirhill/2013/07/24/blueprints-of-nsa-data-center-in-utah-suggest-its-storage-capacity-is-less-impressive-than-thought/

Hintjens, H. M. (2013). Screening in or out? Surveillance of unwanted humanity across the EU. *Surveillance & Society, 11*(1/2), 87-105.

Horchert, J., & Reißmann, O. (2013, September 6). Neue Snowden-Enthüllungen: Wettlauf um die sicherste Verschlüsselung. *Spiegel Online*. Retrieved from http://www.spiegel.de/netzwelt/netzpolitik/snowden-geheimdienste-nsa-und-gchq-knacken-internet-verschluesselung-a-920814.html

Horchert, J. (2014, March 12). Snowden-Enthüllungen: NSA plant Schadsoftware für die Massen. *Spiegel Online*. Retrieved from http://www.spiegel.de/netzwelt/netzpolitik/snowden-enthuellungen-nsa-setzt-auf-automatisierte-ueberwachung-a-958324.html

infra-. (n.d.). In *Wiktionary*. Retrieved from http://en.wiktionary.org/wiki/infra-#English

inter-. (n.d.). In *Wiktionary.* Retrieved from http://en.wiktionary.org/wiki/inter-

Keller, B. (2013, October 27). Is Glenn Greenwald the future of news?. *The New York Times*. Retrieved from http://www.nytimes.com/2013/10/28/opinion/a-conversation-in-lieu-of-a-column.html?pagewanted=1&_r=1&src=recg

Klein, M. (2007, May 15). *Spying on the home front* (H. Smith, Interviewer). Retrieved from http://www.pbs.org/wgbh/pages/frontline/homefront/interviews/klein.html

Levison, L. (2014, May 20). Secrets, lies and Snowden's email: Why I was forced to shut down Lavabit. *The Guardian.* Retrieved from http://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email

Lloyd-Jones, Trevor (2005, September 14). Narus signs regional licence with Giza Systems. *BusinessIntelligence Middle East*. Retrieved from http://www.bi-me.com/main.php?id=2047&t=1

Lyon, D (2001). *Surveillance society: Monitoring everyday life*. Open University Press.

Massumi, B. (1987). Translator's foreword: Pleasures of philosophy. Gilles Deleuze & Felix Guattari, *A Thousand Plateaus* (Vol. 2 of *Capitalism and Schizophrenia*, pp. ix-xv). Minneapolis, MN: University of Minnesota Press.

MacAskill, E. (2013, August 23). NSA paid millions to cover Prism compliance costs for tech companies. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid

Mendelsohn, B. (Producer & Director). 2011. *Bundled, buried & behind closed doors* [video]. United States: Alex + Ben.

Miller, C. (2013, June 7). Tech companies concede to surveillance program. *The New York Times*. Retrieved from http://www.nytimes.com/2013/06/08/technology/tech-companies-bristling-concede-to-government-surveillance-efforts.html?pagewanted=1&hp

Mitchell, A. (2013, June 10). Who is Edward Snowden?. *NBC Nightly News.* Retrieved from http://www.nbcnews.com/video/nightly-news/52162003#52162003

Monahan, T., & Regan, P. (2013). Beyond counterterrorism: Data sharing, privacy, and organizational histories of DHS fusion centers. *International Journal of E-Politics, 4*(3), 1-14.

Nakashima, E., & Gellman, B. (2014, June 30). Court gave NSA broad leeway in surveillance, documents show. *The Washington Post*. Retrieved from http://www.washingtonpost.com/world/national-security/court-gave-nsa-broad-leeway-in-surveillance-documents-show/2014/06/30/32b872ec-fae4-11e3-8176-f2c941cf35f1_story.html

Narus (2004, September 29). *Press release – Narus appoints former deputy director of the national security agency to its board of directors*. Retrieved from https://web.archive.org/web/20050206184639/narus.com/press/2004/0929.html

Nissenbaum, H. (2005). Where computer security meets national security. *Ethics and Information Technology 7*(61), 61-73.

NSA-Geheimdokumente: "Vorwärtsverteidigung" mit QFIRE.(2013, December 12). *Spiegel Online*. Retrieved from http://www.spiegel.de/fotostrecke/qfire-die-vorwaertsverteidigng-der-nsa-fotostrecke-105358.html

Outernet (2014). *Outernet- Information for the world from OuterSpace*. Project website. Retrieved from https://www.outernet.is

Pecora, V. P. (2002). The culture of surveillance. *Qualitative Sociology, 25*(3), 345-358.

Perlroth, N., Larson, J., & Shane, S. (2013, September 5). N.S.A. able to foil basic safeguards of privacy on web. *The New York Times.* Retrieved August 14, 2014, from http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all&_r=1&

Poe, R. (2006, May 5). The ultimate net monitoring tool. *WIRED*. Retrieved from http://archive.wired.com/science/discoveries/news/2006/05/70914

Poulos, J. (2013, July 10). Obama administration anti-leak scheme shows precrime and total information awareness go hand in hand. *Forbes.* Retrieved from http://www.forbes.com/sites/jamespoulos/2013/07/10/obama-administration-anti-leak-scheme-shows-precrime-and-total-information-awareness-go-hand-in-hand/

Priest, D., & Arkin, W. (2014). A hidden world, growing beyond control. *The Washington Post.* Retrieved from http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/1/

Reuters (2007, December 10). *Narus expands traffic intelligence solution to webmail targeting.* Retrieved from http://www.reuters.com/article/2007/12/10/idUS140435+10-Dec-2007+BW20071210?sp=true

Rich, S., & DeLong, M. (2013, October 4). NSA slideshow on 'The Tor problem'. *The Washington Post*. Retrieved from http://apps.washingtonpost.com/g/page/world/nsa-slideshow-on-the-tor-problem/499/#document/p4/a124607

Rushe, D., & Ball, J. (2013, June 7). PRISM scandal: Tech giants flatly deny allowing NSA direct access to servers. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/jun/07/prism-tech-giants-shock-nsa-data-mining

Schneier, B. (2013, October 4). Attacking Tor: How the NSA targets users' online anonymity. *The Guardian.* Retrieved from http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity

Smale, A. (2014, July 3). German student under N.S.A. scrutiny, reports say. *The New York Times.* Retrieved from http://www.nytimes.com/2014/07/04/world/europe/german-student-under-nsa-scrutiny-reports-say.html

Snowden, E. (2014, January 26). *Snowden exklusiv - Das Interview* (H. Seipel, Interviewer). Das Erste, 2014, January 26, 23^{05} pm.

Solove, D. J. (2007). "I've got nothing to hide" and other misunderstandings of privacy. *San Diego Law Review, 44*, 745-772.

Spiegel Staff. (2013, September 9). 'Project 6': CIA spies operating in the heart of Germany. *Spiegel Online*. Retrieved from http://www.spiegel.de/international/germany/cia-worked-with-bnd-and-bfv-in-neuss-on-secret-project-a-921254.html

Spying together: Germany's deep cooperation with the NSA (2014, June 18). *Spiegel Online*. Retrieved from http://www.spiegel.de/international/germany/the-german-bnd-and-american-nsa-cooperate-more-closely-than-thought-a-975445.html

Star, S. L. (2002). Infrastructure and ethnographic practice. *Scandinavian Journal of Information Systems, 14(*2), 107-122.

Star, S. L., & Bowker, G. C. (2006). How to infrastructure. *Handbook of new media: Social shaping and social consequences of ICTs*, 230-245.

Steiner, H., & Veel, K. (2011). Living behind glass facades: Surveillance culture and new architecture. *Surveillance & Society, 9*(1/2), 215-232.

structure. (n.d.a). In *Wikipedia*. Retrieved from http://en.wikipedia.org/wiki/Structure

structure. (n.d.b). In *Wiktionary.* Retrieved from http://en.wiktionary.org/wiki/structure#English

TheAnonMessages. (2013, September 14). *Anonymous- The Story of the Hacktivists (Full Documentary)* [Video file]. Retrieved from http://www.youtube.com/watch?v=i7tQ1VtLMyk

The Associated Press (2010, July 8). Boeing buying cybersecurity firm Narus. *Bloomberg Businessweek*. Retrieved August from http://www.businessweek.com/ap/financialnews/D9GQTHC00.htm

The Washington Post (2013, June 6). NSA slides explain the PRISM data-collection program. *The Washington Post*. Retrieved from http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

Thompson, J. B. (2005). The new visibility. *Theory, Culture & Society, 22*(6), 31-51.

Tor Project (2014). *Tor: Overview*. Project website. Retrieved from https://www.torproject.org/about/overview.html.en

Van der Berg, R. (2008, September 2). How the 'Net works: An introduction to peering and transit. *Ars Technica*. Retrieved from http://arstechnica.com/features/2008/09/peering-and-transit/4

Vidal, J., & Goldenberg, S. (2014, January 30).Snowden revelations of NSA spying on Copenhagen climate talks spark anger.*The Guardian*. Retrieved from http://www.theguardian.com/environment/2014/jan/30/snowden-nsa-spying-copenhagen-climate-talks

Wall Street Journal. (2014, January 17). *President Obama's full NSA speech* [Video file]. Retrieved from https://www.youtube.com/watch?v=p4MKm2uFqVQ

Waterman, S. (2013, October 2). NSA chief's admission of misleading numbers adds to Obama administration blunders. *The Washington Times*. Retrieved from http://www.washingtontimes.com/news/2013/oct/2/nsa-chief-figures-foiled-terror-plots-misleading/?page=all

Wiretap Whistle-Blower's Account. (2006, April 7). *Wired*. Retrieved from http://archive.wired.com/science/discoveries/news/2006/04/70621

Warner, R. (2005). Surveillance and the self: Privacy, identity, and technology. *DePaul Law Review, 54*, 847.

Zetter, K. (2014, July 18). A convicted hacker and an internet icon join forces to thwart NSA spying. *Wired*. Retrieved from http://www.wired.com/2014/07/dark-mail-hides-metadata-from-nsa