Master Thesis

DEFINING REALITY AFTER SNOWDEN: A mixed methods study to global surveillance discourses across societal sectors

Leon Jansen

Erasmus University Rotterdam

27-06-2014

DEFINING REALITY AFTER SNOWDEN:

A mixed methods study to global surveillance discourses across societal sectors

by

Leon Jansen

Student number: 321106

Supervisor: Lela Mosemghvdlishvili, MSc.

Second Reader: Marc Verboord, PhD

Master Media Studies

Media & Business

Erasmus School of History, Culture & Communication

Erasmus University Rotterdam

Master Thesis

June 2014

Abstract

Design: This study features a comprehensive design, both conceptually as well as methodological, in order to uncover surveillance discourses in different sectors throughout society after the groundbreaking disclosures on global mass surveillance. These disclosures were fundamentally aided by the whistleblowing activities of Edward Snowden. Through a triangular conceptual design, this study investigated the discourses used by the corporate sector, government, and citizen groups.

Methodology: This study featured a very comprehensive methodological design using digital research methods (DRM), quantitative and qualitative content analysis, and in-depth discourse analysis. Accordingly, while moving forward through the research process, the data captured with the different methodologies allowed for an increasingly rich understanding of how surveillance is understood in different societal sectors. The network analysis (DRM) capitalized on the linking structure of the internet and collected big data in bulks, whereas the content analysis identified themes and differences among societal sectors, and finally, the discourse analysis was instrumental in finding out what discourses were prominently used by what sectors. Because the methods build on each other, results gained increased validity through triangulation.

Findings: The corporate sector, government sector, and citizen group sector draw on fundamentally different discourses, that sometimes draw on each other through interdiscursivity, and sometimes are engaged in discursive struggle. Most notably, the triangular sectors fail to acknowledge the fundamental role of the corporate sector in facilitating current mass surveillance. This failure has fundamental ideological consequences.

Relevance: The relatively recent mass surveillance disclosures made possible by Edward Snowden, leave a substantial gap for identifying surveillance discourses after his leaking. In addition, the innovative triangular design adds to a knowledge gap by contrasting the discourses used by different societal sector in a framework. In addition, the societal relevance is evidenced by the large societal interest in the topic as well as public recognition for the relevance of the issue. Surveillance discourse fundamentally influences the way we perceive reality.

Suggestions: As discourses are contingent they change over time. As a result, a longitudinal study to surveillance discourses could be conducted in order to observe how discourses change over time. In addition, a study could be conducted to surveillance discourses prior to the leaking of Edward Snowden, and potentially compare the results with the discourses after leaking. Finally, surveillance discourses could be compared across different geographical regions.

Keywords: Surveillance Studies; Discourse Theory; Edward Snowden; Mass Surveillance; Mixed Methods.

Acknowledgments

First of all, I would like to especially thank my supervisor Ms. Lela Mosemghvdlishvili for her inspiring guidance, her vital contributions to the creative process, her flexibility and kindness, and her enthusiasm. In contrast to advocating a strict professor-student hierarchy, she instead encouraged a more egalitarian collaboration, which made me truly feel like I had ownership over the project. This helped me find necessary motivation to complete the research and writing process in a personally satisfactory fashion, and in addition it allows me to now feel the intrinsic gratification of having produced a piece of scientific work that may be a contribution to the field of surveillance studies – a field I have become passionate about over the last six months.

Also I find it appropriate to especially thank my father Francis, my mother Sonja, and my twin and best friend Remy for their encouragement; as well as their ability to endure my occasional complete social isolation while working hard in order to meet deadlines. In addition, I would like to thank my other family members, friends, fellow students, and fellow thesis writers for encouraging me during stressful moments. You know who you are!

Finally, I would like to thank you, the reader, for your time and your interest in reading my thesis.

- Leon Jansen
  June 26, 2014

Table of Contents

Chapter 1: Introduction

"I am willing to sacrifice all […] because I can't in good conscience allow the US government to destroy privacy, internet freedom and basic liberties for people around the world with this massive surveillance machine they're secretly building"
(Snowden, 2013)

- Edward J. Snowden

This first chapter of the study introduces the background and foundations of the study. After the background of the surveillance disclosures is introduced; this chapter will give insight into the innovative framework and comprehensive research design this study draws on. Furthermore, the academic and societal relevance of the study will be discussed, and finally, a preview of the following chapters will be provided.

1.1 Introduction

The statement shown on top of this page comes from Edward Snowden, the man who in early June, 2013 disclosed himself as one of the largest leakers of state secrets in U.S. history (Greenwald, MacAskill & Poitras, 2013). Snowden, a 29-year old former defense contactor, as employee of companies Booz Allen and Dell deployed at the National Security Agency (NSA) and the Central Intelligence Agency (CIA), claims to have gotten remorse problems after having been disposed to grave abuses by intelligence workers working for the signals intelligence branch of the NSA (Gellman, Blake & Miller, 2013). Having access to large amounts of classified documents while working in a senior position at the NSA, Snowden decided to copy many NSA documents and release numerous of these to investigative journalists Glenn Greenwald and Laura Poitras who worked for The Guardian newspaper (Greenwald, MacAskill & Poitras, 2013).

The first disclosures exposed bulk collection of U.S. phone call metadata from operator Verizon by the NSA under a top secret court order (Greenwald, 2013a); operations of a NSA program named *PRISM* which through backdoors in server encryptions grants the

NSA with direct access to the servers of U.S. internet giants including Microsoft, Google and Facebook (Greenwald & MacAskill, 2013a); and NSA's tool for cataloguing global surveillance data named *Boundless Informant* (Greenwald & MacAskill, 2013b). As a result, Snowden was charged with Espionage by the U.S. Department of Justice (Finn & Horwitz, 2013), and while he had planned to leave his initial place of refuge Hong Kong for Latin America he was trapped at Moscow Sheremetyevo airport (Arutunyan & Stanglin, 2013) from boarding an onward flight to Havana, Cuba (Reuters, 2013b) because the U.S. Department of State revoked his passport a day earlier (Reuters, 2013a). After having spent several weeks in the transit zone of the Moscow airport, Snowden was granted temporary asylum in Russia (Chumley, 2014), where he resides to this date.

In the meantime, numerous surveillance programs have been exposed, used to gather intelligence from which many is shared within the *Five Eyes* – an allegiance for joint cooperation in signals intelligence among five Anglophonic countries which next to the United States includes Australia, Canada, New Zealand, and the United Kingdom (Cox, 2012). Notable exposures include the *XKeyscore* program, from which it is claimed it allows the NSA to virtually access all a user does online (Greenwald, 2013b); the *Tempora* program operated by the British counterpart GCHQ accessing global communications through the wiretapping of fibre-optic cables (MacAskill, Borger, Hopkins, Davies, and Ball, 2013); the GCHQ and NSA joint operated program named *MUSCULAR* which did help them to secretly break in to the main communication links connecting Google and Yahoo! data centers (Gellman & Soltani, 2013a); the NSA operated *FASCIA* database which includes trillions of location records of devices (Gellman & Soltani, 2013b); the *DISHFIRE* joint operated program by the NSA and GCHQ collecting and storing millions of sent text messages on a daily basis (Ball, 2014); the *Squeaky Dolphin* program monitoring social media networks in real time (Esposito, Cole, Schone & Greenwald, 2014); *Optic Nerve* program surreptitiously collecting private webcam images from users running a Yahoo! webcam application (Perlroth & Goel, 2014); and finally, the NSA's spying on 122 world leaders (DW, 2014) including monitoring the calls of 35 world leaders, notably German chancellor Angela Merkel (Poitras, Rosenbach & Stark, 2014).

1.2 Triangular Framework

While surveillance malpractices have been exposed previously, including the NSA spying on U.S. citizens without the need for a warrant which came to light in 2005 (Dinev et al., 2008),

arguably the disclosures made possible by the Edward Snowden leaking are unprecedented. As a result, much has been reported about the issue in a variety of sources including, but not limited to, news reports, government statements, company statements, and advocacy group reports.

This study aims to identify *discourse*, which has been defined as "a particular way of talking about and understanding the world" (Phillips & Jørgensen, 2002, p. 1), regarding surveillance after Snowden. Discourse starts from the premise that our ways talking about the world do not neutrally reflect reality, but instead language use has an active involvement in creating and changing the ways we perceive the world, social relations, and identities. In other words, while the study of discourse does not make claims about the reality regarding a certain phenomenon itself, it studies how 'reality' and knowledge about a certain phenomenon are constructed discursively through language (Phillips & Jørgensen, 2002). This study contributes to the understanding of surveillance discourse by studying how the reality of surveillance in our society is constructed through language in several sectors of society. This is done by means of textual analysis.

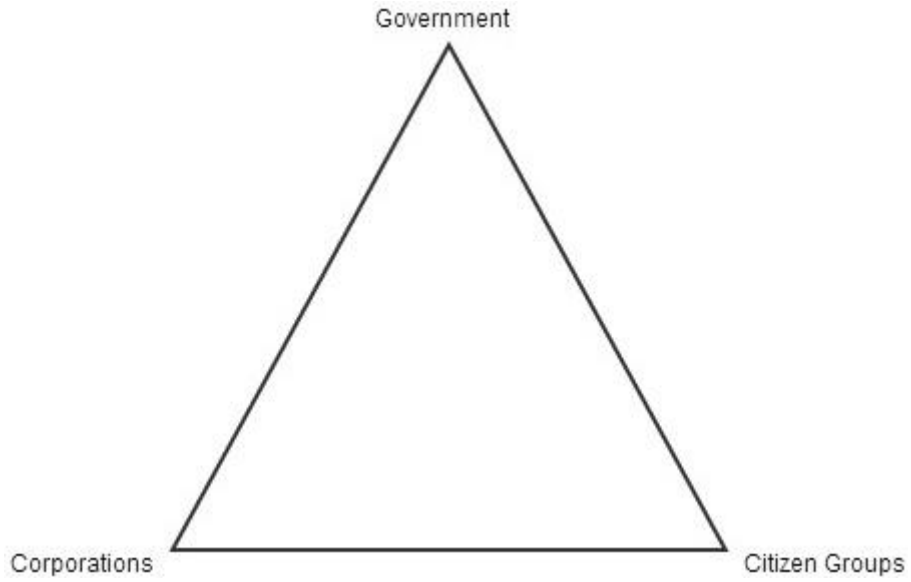

Figure 1.1: Triangular Framework

The sectors included in this study are *the corporate sector*, *government*, and *citizen groups*. Envisioned in a triangular relationship (see Figure 1.1), the three sectors identified are the most important representatives of the groups involved in the current surveillance debate. First, companies building their business models around the monetization of assembled user profiles, which they sell to third party advertisers (Fuchs et al.,2012), likely suffer reputation damage

by media reports claiming surveillance malpractices by government agencies tapping into these user data (e.g. Gellman & Soltani, 2013a). In addition, governments worldwide may suffer from increasing skepticism by their citizenry seeing that intelligence agencies from many countries have been found to collaborate and exchange data on their own citizens with the Five Eyes allegiance in secret, and thus without ensuring public approval (Borger, 2013). And thirdly, citizen groups acting as "privacy advocates" (Bennett, 2012, p. 413) represent citizens worldwide, thereby striving to safeguard privacy and human rights (Bennett, 2012).

In addition, media outlets may cover the viewpoints of certain sectors more than others, or may critically scrutinize different sectors to varying extents, thereby privileging viewpoints in their coverage. As a result, media has a mediating role among the three sectors included in the triangular framework. Arguably, mass media have the largest potential audience, and hence is included as a *source* in this study. In other words, mass media sources – which are texts in this case – are scrutinized with regard to their coverage of the sectors included in the triangular framework. In addition, texts specifically representing the *corporate sector* as well as *citizen groups* are included. Hence, this study draws on three groups of texts: mass media texts, corporate sector texts, and citizen group texts. The latter two (corporate sector-and citizen group texts) each represent a sector in the triangular framework, while the mass media mediates among all three.

Indeed, while in this study the analysis focuses on the three sectors of the triangular design depicted in Figure 1.1 (more specifically the corporate sector, government, and citizen groups), the actual empirical data is collected from online texts from corporations, citizen groups, and the mass media. Reason for this is the fact that online texts from the mass media cover the viewpoints of the three triangular sectors to varying extents, but especially the government viewpoint is well represented through citations of government representatives in mass media. As a result, texts from mass media are adopted as representing the three sectors in the triangular design as the mass media mediate among the three, including – very explicitly – the government's viewpoint. Including additional texts from corporations and citizen groups provide the opportunity to compare and contrast among the viewpoints covered in the mass media and the viewpoints covered in the texts from their respective sectors. Because the corporate sector, government, and citizen groups are subject to analysis, this study is guided by the following main research question: *How is the practice of mass surveillance presented in the corporate sector, government, and citizen groups communication during the NSA scandal?*

Furthermore, the research for this study is performed in a comprehensive design, consisting of three parts using multiple methods, and as a result it is possible to perform triangulation, whereby the research results gain more validity. The research design consists of three parts: the first part utilizes digital research methods (DRM); the second part consists of a content analysis; and the final part uses an in-depth discourse analysis. The research design including specifics on the process and procedures is more specifically outlined in Chapter 3 of this study: Methodology.

1.3 Relevance

First, the academic relevance of this study will be discussed, and following the societal relevance will be outlined.

Due to the relatively recent disclosures by Edward Snowden regarding mass surveillance unprecedented in scope, surveillance discourses have potentially changed from the ones studied by scholars previously. This leaves space to add to existing studies.

In addition, due to the comprehensiveness of this study; as evidenced by its innovative triangular framework, and its inclusion of data from multiple sources with a multiple methods research design, this study has the potential to become a significant empirical study in the field of surveillance studies. As a result, future studies conducted in the same field may substantially draw on the results of this study for the premises or starting points of their research.

In addition, the comprehensive methodological design of this study specifically provides the opportunity for performing triangulation. This means that within this same study, the results of the different methods can be used to have research conclusion with more validity.

The societal relevance is evidenced most notably by the large interest in the topic, deduced both from extensive news coverage around the topic as well as from public recognition regarding the importance of the issue. For instance, journalists from The Guardian and The Washington Post – the newspapers who through investigative journalism broke the story to a large audience – won Pulitzer Prizes for their reporting, the highest award in newspaper journalism (Associated Press, 2014).

In addition, the surveillance issue touches upon many societal disciplines; for example the role of technology in societies around the world, what in this case constitutes good

governance, under what conditions governments may be authorized to act outside of legal supervision, and the roles, responsibilities, and limits of investigative journalism.

This study adds to this debate by uncovering how the current surveillance situation is discussed discursively. In other words, once one has insight into how current surveillance activity is constructed discursively among different societal sectors (in the triangular framework), that is, how understanding and reality around it is created through discourse, one can take part in the debate better positioned, and more effectively work towards a better situation, if deemed necessary.

In the following, this study covers the theoretical lens of the study in Chapter 2 (Theoretical Background), in which the theoretical perspectives regarding surveillance studies and discourse most relevant to this study are discussed. Furthermore, the methodological design of this study is outlined in-depth in Chapter 3 (Methodology). The findings of the research process as well as a synthesis of the results among the different research parts and with literature are covered in Chapter 4 (Findings & Discussion). Based on this, conclusions are drawn in Chapter 5 (Conclusions), which will also include theoretical implications and practical implications, as well as limitations to the project and directions for future research. This is followed by references and appendices.

Chapter 2: Theoretical Background

This chapter discusses the theoretical starting points of this study, which includes a comprehensive selection of relevant theories from the respective fields of surveillance studies and discourse analysis. In addition, the chapter comprises a theoretical lens that focuses one's attention on the scholarly theories most relevant to the analysis of empirical data. First, theory from the field of surveillance studies will be presented in this chapter, which is followed by an introduction to discourse analysis on a conceptual level. Finally, the research question and sub-research questions driving the research process of this study will be presented.

2.1 Surveillance Studies

This section includes theory from surveillance studies adopted in this study. After the concept of surveillance has been addressed and how it has been situated in society, the influential theory of Foucault's panopticism is introduced. Furthermore, post-panopticism, the role of the commodification of data, as well as innovative web 2.0 practices will be discussed.

2.1.1 The surveillance concept

Surveillance is a broad and multifaceted concept, and narratives and discourses around the surveillance concept have been articulated in both positive and negative extremes – and all the shades in between. One view is that one should accept a certain level of surveillance in order to allow centralized systems benefiting the citizens in present-day society to work. For instance, in the context of the "benevolent welfare state" (Marx, 2012, p. xxv). By contrast, fundamentally dystopian views regarding surveillance have emerged due to the fears of power abuses by autocratic regimes suppressing their citizens – inspired on for instance Orwell's *Nineteen Eighty-Four*, Kafka's *The Castle*, or Zamyatin's *We* (Kammerer, 2012).

In addition, Marx (2012) distinguishes between several kinds of surveillance. For example, strategic surveillance – involves deliberate strategy and should be distinguished from non-strategic surveillance. Similarly, traditional surveillance which relies on the human senses – e.g. by watching someone, is different from the new surveillance which uses technological means for its operations. Surveillance may be agent-agitated, for instance at

border control. However people may also engage in self-surveillance, such as when checking payments with one's bank account.

The previous list is an indication of the variety of contexts in which surveillance may arise. Nonetheless, several scholars have attempted to provide an encompassing definition of the surveillance concept – most of them include critical notes regarding power imbalances. For instance, Akerlof (1970) provides a broad definition of surveillance, emphasizing an unequal information balance between the surveilling and surveilled party as a prerequisite. A more detailed definition is provided by Lyon (2001), who claims that surveillance is "any collection and processing of personal data, whether identifiable or not, for purposes of influencing or managing those whose data have been garnered" (as cited in Dinev, Hart & Mullen, 2008, p. 214).

While acknowledging the productive nature of the "benevolent welfare state" (Marx, 2012, p. xxv), this study emphasizes the problematic effects of grave information imbalances among triangular sectors. While certain government agencies capitalize on mass data collection facilitated by the corporate sector, the public (represented by citizen groups in the triangle) finds their data exploited by the other two sectors.

2.1.2 Surveillance in historical perspective

The earliest accounts of surveillance were probably those linked to information collection by governments, of which the English *Domesday Book* of the year 1086 serves as the earliest example, including some 13,000 records on citizens. Similarly, the earliest significant evidence of the current modern information state in rise can be found during the late eighteenth century. The emergence of the nation state and – somewhat later – the increasing industrialization of societies in Western Europe and Northern America facilitated the necessity of a more centralized information collection. Over time, the methods of collecting information became increasingly structured, organized, centralized, and gradually evolved into the modern bureaucratic surveillance system, as we recognize it today (Weller, 1986).

However, while the system of information collection and surveillance was expanding, concerns were raised regarding the risks of control abuse and alienation. Beniger (1986) argued that while the information processing increased in terms of scale and rationalization, citizens were increasingly regarded as 'numbers' and 'things' rather than actual human beings. Citizens were dehumanized, which contributed to a sense of alienation due to the expanding bureaucracies typical of modernist societies. At the same time, bureaucracies

granted administrations with a tool of control, which was why Beniger (1986) considered bureaucracies to be new control technologies.

As opposed to Beniger's (1986) rather dystopian view on state surveillance in society – effectively controlling and alienating citizens, Giddens (1990) argued that state surveillance may also serve citizens. More specifically, Giddens (1990) claims that on top of information control, surveillance serves as "social supervision" (p. 59). Indeed, information on citizens is collected and managed by authorized institutions in order to promote their protection and wellbeing. This articulation of the surveillance concept is very comparable to the notion of a social contract stressed by for instance the famous philosophers Thomas Hobbes, John Locke, and Jean-Jacques Rousseau, in which citizens are provided with protection, security, and welfare in return for abandonment of (some of) their sovereignty (Weller, 2012). In other words, Giddens (1990) argues that rather than information being misused for sinister and Orwellian forms of control and monitoring, surveillance serves the valuable and benevolent purpose of promoting social welfare.

In recent times, surveillance capabilities of governments have tremendously expanded, especially in the wake of the 9/11 terrorist attacks in the United States in 2001 (Dinev et al., 2008). This expansion has for a prominent part been achieved by judicial means. In addition to what arguably may be the most noticeable changes in daily life, such as increased worldwide airport security measures after 9/11, in the legal field laws have been passed in the United States and the European Union that authorize significantly more surveillance (Fuchs, Boersma, Albrechtslund and Sandoval, 2012). For example, in the United States the USA Patriot Act of 2001 widened the scope of data that the US government was authorized to obtain from internet providers, and furthermore extended wiretapping from phone calls to e-mails and internet traffic. Moreover, the Combating Terrorism Act of 2001 made it legal for U.S. intelligence to obtain information through internet filtering without the permission of a judge. In addition, the Data Retention Directive that was passed by the European Union in 2006 made it mandatory for member states to pass laws that required internet service providers to store connection and identification data regarding phone calls and internet usage for a minimum of six months (Fuchs et al., 2006).

2.1.3 Foucault's panopticism

Virtually every theory in the field of Surveillance Studies either contains elements of Foucault's (1977) panopticism or situates itself in the field in some relation to panopticism.

With panopticism, Foucault (1977) developed one the first comprehensive frameworks explaining the fundamental workings of surveillance in a modernist society.

Foucault (1977) based the fundamental idea of his panopticism largely on the writings of the English philosopher Jeremy Bentham (Elmer, 2012). Bentham (1995) argued that the panopticon prison design was the ideal building for maintaining order and discipline among the prisoners without the need for physical coercion. The panopticon prison is a circular building, with a watchtower where the guards reside in the center, and the cells where the inmates reside surround this watchtower. From the perspective of the inmates in the cells around this watchtower – of which the windows are shaded and reflect light, there is the omnipresent uncertainty whether the guards are watching them. From the perspective of the guard in the watchtower however, the prisoners every move can be monitored. Here again the element from Akerlof's (1970) definition of information imbalance can be discovered. Moreover, the omnipresent 'threat' of surveillance will not only lead the prisoners to regulate their behavior according to the expected norms, also the guards will feel the constant pressure of the supervisor watching them, avoiding escalations of force against prisoners for instance. As a result, there will likely be increased efficiency, without the need for coercion which leaves the situation with winners on all sides in Bentham's explanation (Elmer, 2012).

Hence, Bentham's intentions where rather benevolent when advocating the panopticon as an ideal design for prison. Foucault's view on the panopticon however, was more sinister – and in fact served as a metaphor for the way individuals are socialized in society to behave according to the norms set by some higher authority such as the state, the school, or the workplace. Indeed, Foucault (1977) argues that institutions in society vitally contribute to the disciplining of individuals through *discipline* which in Foucault's view is a domain of *power* that leads to individuals (bodies) to become docile.

Through such discipline (exercised through disciplinary acts) individuals not only learn to behave according to the norms and regulations they are expected to subscribe to, but gradually come to think in a way according to these norms. At this stage bodies have become docile and have thus been turned into *docile bodies*, while the surveillance and discipline have naturalized themselves, and as a result are taken for granted. Indeed, Foucault (1977) argues that "a body is docile that may be subjected, used, transformed, and improved" (p. 136).

Essentially, while bodies have become docile through disciplining power, institutions and organizations in society can be run more efficiently. Therefore, discipline is functional. The disciplining mechanism according to Foucault (1977) is "a functional mechanism that must improve the exercise of power by making it lighter, more rapid, more effective, a design

of subtle coercion" (p. 209). More specifically, docile bodies are carefully crafted by the practice of *biopower*, which is exercised not exclusively by the state, but instead can be utilized by any organization or institution wishing to discipline its 'subordinates' (Ceyhan, 2012). *Biopower* specifically exercised in the context of the state is called *biopolitics* or *governmentality* (Bajc, 2007). Biopower is exercised through the practices of information collection, information processing, and predictive analysis through statistics (Ceyhan, 2012). Specifically in the context of the state, information about characteristics of citizens, such as demographics, is collected by government institutions in order to explain, classify, and sometimes predict the behavior of entire populations. The process of governmentality involves the individuation, because large bodies of people in a society characterized by an internal structure involving hierarchies, relations, loyalties, and morals are very difficult to effectively govern for the state. Therefore, group members are individuated into their own selves, for instance by the attachment of an ID-number to every individual. This turns individuals into subjects and essentially allows for the governing of people through evaluation, surveying, and prediction (Bajc, 2007). Furthermore, Bajc (2007) argues that governmentality has expanded over time seeing that once geographical areas were divided into parcels which we know as nation states, today authorities are able to classify and predict based on fingerprint detection, retina scan, and even DNA.

2.1.4 Post-panopticism

Notwithstanding the explanatory potential of Foucault's panopticism, there are two substantial shortcomings to the theory that lead prominent scholars in the field of Surveillance Studies to question the relevance of panopticism to modern day and age. Panopticism does not adequately explain the involvement of (a) consumerism and (b) technological innovations in the current surveillance process (Bogard, 2012; Lyon, 1994; Mann, Nolan & Wellman, 2003). These shortcomings provided an incentive for contemporary scholars to develop a new strand of theory in contemporary Surveillance Studies: post-panopticism.

Andrejevic (2012b) argues that "we are living in a time when more information is gathered, collected, sorted and stored about the everyday activities of more people in the world than at any other time in human history" (p. 91), while referring to the impact of technological innovation on the process of surveillance. In turn, Haggerty and Ericson (2000) drew on Deleuze and Guattari's (1987) notion of 'assemblage' for explaining surveillance in contemporary society, hence they develop a concept of 'surveillance assemblage'. In addition,

similar to the notion of 'network society' as envisioned by Castells (1996), the surveillance assemblage creates and manipulates data, rather than physical bodies in closed spaces. Similarly, Deleuze (1988) argues that individuals are integrated into circulations of larger economies, that includes the circulation of objects and information. To clarify, Deleuze (1992) introduces the concept of 'dividual', claiming that just like society, the individual becomes increasingly fragmented. In contrary to what Foucault (1977) claims regarding bodies becoming docile under the influence of surveillance, Deleuze (1992) argues that a surveillance increase is exercised through the two bodies that the individual was split in while it became a dividual: a physical body and a data body.

This 'dataveillance' (Clarke, 1994) through a data body is further developed by Baudrillard (1994) by his notion of *simulation*. Simulation is the "reproduction of the real according to its model" (Baudrillard, 1994, p. 1). In other words, the data body is reproduced according to the physical body. However, the data body composed of digital codes does not represent the physical body, but instead it is a manufactured hypothetical body that has true existence by itself. In Baudrillard's (1994) words: it is hyperreal. As a result, Baudrillard (1994) argues that with the manufacturing of hyperreality the panoptic control as articulated by Foucault (1977) has shifted into a higher register. In today's simulated surveillance, the shaded windows and prison walls of the panopticon are replaced by data mines and information clouds, their accessibility no longer regulated by doors and locks, but instead by passwords and decryption tools (Baudrillard, 1994). Similarly, Deleuze (1992) argues that today's network society coupled with newly developed statistical techniques such as data mining, allow for remote control and surveillance technologies, superseding the need for concentrating actual bodies behind walls of certain institutions.

2.1.5 Internet surveillance and information capitalism

The "silent surveillance" (Ceyhan, 2012, p. 43) possibilities fueled by the development of computerized technologies have significantly improved with the inception of the internet. Indeed, as Fuchs et al. (2012) argue, the internet – which "operates in real time over networks at high transmission speed" (p. 15) – allows for surveillance at a distance. Moreover, apart from the fundamentally increased information collection capabilities due to widespread use of the internet, the storage in serves and huge databases, the analysis capabilities have expanded tremendously due to data mining techniques and the development of complex algorithms (Ceyhan, 2012). Furthermore, because internet is virtually not hindered by state borders, the

space of mobility of internet surveillance potentially embraces the whole globe (Fuchs et al., 2012).

In addition, as Weller (2012) states, the growth of capitalism and consumerism during the late nineteenth century led to increased information collection not only on the side of the state, but increasingly on the side of commercial businesses. Today, the private sector potentially possesses more information about its customer than any state institution would be capable of collecting (Kammerer, 2012). Moreover as Fuchs et al. (2012) argue, "surveillance shapes and is shaped by economic production, circulation, and consumption" (p. 8). And whereas during post-WWII years Fordist mass production and mass consumption spurred the interest in consumption patterns, which in turn led to the development of consumer research, the growth in internet usage specifically has increased the potential of targeted advertising (Fuchs et al., 2012).

The effectiveness of targeted advertising is largely dependent on one aspect: consumer data. As a result of technology development, is has become possible to build extensive customer profiles from collected data. Customer can be targeted individually with tailored advertisements, this way increasing advertising returns. The use of cookies, collaborative filtering, spyware, clickstream analysis, log file analysis, and web crawlers are but a few examples of techniques used to build consumer profiles on individual internet users (Fuchs et al., 2012). Such "information capitalism" (Wall, 2006, p. 340) may come in the annoying form of spam e-mails or intrusive search engine advertisements. However, the larger issue here is what Cohen (2008) names the "valorization of surveillance" (p. 8), which refers to the underlying profit structure of a large portion of today's internet – one that makes profitable the potential surveillance by means of consumer data gathering on a mass scale.

2.1.6 Surveillance and social media

During the past decade, the internet has gone through a fundamental transformation phase that, according to optimistic views from some scholars, has left the internet more democratized (Tapscott & Williams, 2006); collaborative and non-proprietary (Benkler, 2006); or interactive and participatory (Deuze, 2007). This transformation is commonly referred to as the inception of *Web 2.0* or *Social Media*. Fuchs et al. (2012) provide a concise, yet comprehensive definition on the phenomenon, stating that "web 2.0/social media platforms are web-based platforms that predominantly support online social networking, online community-building, and maintenance, collaborative information production and

sharing, and user-generated content production, diffusion, and consumption" (p. 3). According to Fuchs et al. (2012) prominent examples of social media platforms are: Facebook, Orkut, Twitter, LinkedIn, YouTube, MySpace, Hi5, and Friendster.

At the same time however, social media facilitate the collection, storage, and analysis of user data (Fuchs et al., 2012). More specifically, Andrejevic (2007) speaks of a "digital enclosure" (p. 2), referring to "an interactive realm wherein every action and transaction generates information about itself" (p. 2). Moreover, social media not only generate more data – social media data also potentially reveal more personal information. As McGrath (2012) notes, social media profiles are often infused with a vast volume of constantly updated narrative about the users life's. Trottier and Lyon (2012) argue that in the activity of collaborative identity construction on social media content is often posted with a particular audience in mind such as close friends. As a result, social media users are not aware that much of the data they initially share with their friends on social media is also available to a much larger audience. Furthermore, surveillance capabilities are fundamentally enhanced seeing that social ties become detectable and analyzable, platform interfaces and privacy settings are ever-changing enhancing profile visibility throughout the platform, and mobile technologies foster spatially versatile surveillance – e.g. geo-tagging (Trottier & Lyon, 2012).

Yet, the experiences of many social media users suggests the contrary: for them social media surveillance is empowering. This "participatory surveillance" (Albrechtslund, 2008) allows users to share preferences, tastes, and opinions online while socializing and engaging in collaborative identity construction (Trottier & Lyon, 2012). However, Andrejevic (2012a) argues that this interactive and collaborative identity construction is in fact exploitation, due to companies profiting from users' free immaterial labor. More specifically, users with their social media activities generate data that is being used to more effectively target advertisements at them. For these products they are required to pay a price premium, which effectively means social media users are paying a premium for the fruits of their own labor (Andrejevic, 2012a).

In general, Andrejevic (2012a) shares the critical stance of - among others - Ceyhan (2012), Cohen (2008), Fuchs et al. (2012), and Wall (2006) regarding the increased surveillance capabilities of the corporate sector due to the commercialization of the internet, and the growth of targeted advertising, data mining, and predictive analysis valorized by advertised-based profit models. Additionally however, Andrejevic (2012a) warns not to overlook the political economy of the internet, for he argues that the current commercial infrastructure is by no means inevitable or natural. Instead, it is the result of our trust in and

reliance upon the corporate sector to facilitate us with an infrastructure for our communicative, informational, and also our social needs (Andrejevic, 2012a).

While this study appreciates the foundation for surveillance studies laid by Foucault's panopticism, at the same time it has to acknowledge its fundamental shortcomings regarding explaining the role of technological innovation (in particular web 2.0 practices) and commodification of data. According to this study, these shortcomings are well supplemented with the post-panoptic concepts of 'dividual' and 'surveillance assemblage' emphasizing surveillance through data nowadays, facilitated by technological innovations. These innovations in computerized technologies (Ceyhan, 2012; Fuchs et al., 2012) have partly facilitated the "digital enclosure" (Andrejevic, 2007, p. 2). In addition, this study also adopts Andrejevic's (2012a) contention that the public's trust put in commerce to facilitate the communicative and informational infrastructure of the internet was not an inevitable one. This resulting reliance on a commercialized internet has inevitable effects however, most notably the digital enclosure and the resulting "valorization of surveillance" (Cohen, 2008, p. 8) – turning the activities of collecting and exploiting customer data into profitable activities for commercial businesses.

2.2 Discourse Analysis

The discourses used by the three actors included in the 'triangle' framework of this study are going to be analyzed with the method known as discourse analysis.

2.2.1 Social constructionism

Discourse analysis is a theoretical and methodological whole that includes: a certain set of philosophical premises regarding the role of language and discourse in the construction of knowledge and claims to truth; theoretical models; guidelines for methodology; and techniques for carrying out analysis (Jørgensen & Phillips, 2002). The discourse analytic approaches adopted in this study are all rooted in social constructionism (Burr, 1995). Social constructionism is an umbrella term for a set of approaches subscribing to certain theoretical premises. These include the premise that knowledge is not a reflection of some reality that could potentially exist independent from human conscience, instead knowledge is the product of discourse. Furthermore, since our knowledge is constructed through discourse, knowledge draws on discourses from different ages in history resulting is worldviews and identities being *contingent* – meaning that they may change over time. Knowledge about what is true and

false is created and maintained through social interaction with others. And finally, different ways of understanding the world results in different acts, therefore the construction of knowledge and truth through social interaction has social consequences.

2.2.2 Structuralist and post-structuralist thinking

On a more specific level, the discourse analytic approaches included here resonate to a certain extent to a 'sub-category' of social constructionism – which is post-structuralism. Post-structuralism evolved from Saussurian structuralism over time. Ferdinand de Saussure, who is one of the most prominent representatives of structuralist thinking about language, made the distinction between *langue* – which is the structure of language, and *parole* – which is situated language use. In the original Saussurian articulation of structuralism langue constitutes a 'fishing net' – metaphor for a stable network of words that gain their meaning in their relation to other words in that same network. The consequence of parole is that is a word is used in a certain situation – meaning in relation to a certain set of words, its meaning is fixed. Post-structuralism, even though it starts in structuralism, differs two important respects from Saussurian structuralism. First, post-structuralism rejects the idea that language is structured within a stable fishing net-like structure of words. Instead, the words that stand in relation to a certain word, and that this certain word hence gains it meaning from can change, and as a result, the meaning of this certain word changes. And secondly, structures themselves are not necessarily consistent, and therefore may change. With the latter premise, post-structuralism solves a prominent problem of structuralism, which is: how to deal with change.

2.2.3 Discourse Theory and Critical Discourse Analysis

The two discourse analytic approaches adopted in this study are *Discourse Theory* (DT) – most prominently represented by Laclau and Mouffe (1985), and *Critical Discourse Analysis* (CDA) – which is most prominently represented by Fairclough (1989). Even though DT and CDA have roots in the same philosophical premises of social constructionist thinking and post-structuralism, they bear some notable differences. First of all, Faiclough's (1989) CDA distinguishes among discursive and non-discursive practices. Whereas text, talk, and related semiological systems are included in Fairclough's (1989) understanding of discourse – and hence can be studied with discourse analytical tools, economic and technology are non-discursive for instance, and hence need to be studied with different tools.

By contrast, Laclau and Mouffe's (1985) DT makes no distinction between discursive and non-discursive practices, and hence everything is discursive. Furthermore, being the most post-structuralist of the two approaches, DT understands language as fundamentally unstable, and as a result meaning can never be completely fixed. As a result, different discourses in society are involved in an ongoing discursive struggle to achieve hegemony (Laclau & Mouffe, 1985). CDA however, draws on the notion that language always builds on earlier uses of language, because users of language build on earlier established meanings. Therefore, discursive social practices (text, talk, or semiological systems) draw on other discourses, and thus are influenced by *intertextuality*. As a result, by adoption of the notion of intertextuality, CDA studies how earlier discourses are either reproduced by current discourses or changed by them (Fairclough, 1989).

Even though subtle differences exist in the theoretical premises adopted by DT and CDA, it is not only allowed to create a package including elements from both discourse analytic approaches, it is actively encouraged. This is called a multiperspectival research, where instead of creating a mishmash of elements, the practice of creating a coherent package characterized by deliberate consideration of elements from both approaches benefits the research. Indeed, research results from different perspectives provides knowledge in different forms that complement each other, and thereby contribute to a broader understanding of the phenomenon under examination (Jørgensen & Phillips, 2002).

2.3 Research Questions

As a result, the following main research question is presented:

How is the practice of mass surveillance presented in the corporate sector, government, and citizen groups communication during the NSA scandal? (RQ)

The main research question is divided into sub-research questions, which are addressed with different methods (discussed in detail in the following chapter).

The sub-research questions addressed by digital research methods are:

What are the most prominent sources in the networks of the respective publications in terms of mass surveillance coverage online? (sub-RQ 1)

What are the key moments in time in terms of the largest interest online in the surveillance scandal from June 2013 until April 2014? (sub-RQ 2)

The sub-research question answered by content analysis is:

What are the most notable trends and differences among the respective sectors in terms of mass surveillance? (sub-RQ 3)

In addition, the sub-research questions answered by discourse analysis are:

How is the practice of mass surveillance articulated in discourses used by the corporate sector? (sub-RQ 4)

How is the practice of mass surveillance articulated in discourses used by government? (sub-RQ 5)

How is the practice of mass surveillance articulated in discourses used by citizen groups? (sub-RQ 6)

Chapter 3: Methodology

This chapter thoroughly sets out how the research was conducted; what methods were used in order to adequately answer the set of sub-research questions and, eventually, the main research question. The research was guided by a comprehensive design as evidenced by the three parts making up the mixed methods research design. The choice for a mixed methods design was a deliberate one, for it provides the opportunity to reap the benefits of including multiple perspectives that complement each other well. Moreover, the collection of research data of different nature allows for verification (Sechrest & Sidana, 1995), and as a result the research results will be arguably more valid. Indeed, a mixed methods design provides researchers with the equipment to increase the likelihood that the research results are a more adequate reflection of the underlying phenomenon studied, rather than a mere artifact of the method itself (Johnson, Onwuegbuzie & Turner, 2007). In addition, a prominent way to achieve this is by means of triangulation (Jick, 1979). In this study, data triangulation (inclusion of multiple sources) and methodological triangulation (inclusion of multiple methods) were used (Denzin, 1978) – and regarding the latter, sequential methodological triangulation was used more specifically, because the different methods used build on each other (Morse, 1991).

Naturally, the utilization of different methods of research leads to the entire research process being split up in different parts. In this case, the process was split up in three distinct parts: digital research methods, content analysis, and discourse analysis. These three methods complement each other. The idiographic explanation provided by the depth and thoroughness of discourse analysis, combined with the nomothetic explanation from content analysis and especially network analysis (as part of digital research methods), allow this study to reap the benefits of both, and enable a more comprehensive understanding of the phenomenon under study. In addition, while the discourse analysis studies discourse in-depth, and content analysis is concerned with uncovering patterns and trends among the triangular sectors, the network analysis is the only method capable of uncovering the very online network of sources used by corporate-, mass media-, and citizen group texts through the analysis of big data. As a result, network analysis enables for enriching the study with (big) data that neither discourse analysis nor content analysis are capable of. Then, the trends and patterns uncovered by content analysis complement the in-depth discourse analysis, and the online network of

sources uncovered by network analysis complements the trends and patterns of content analysis by providing insight with big data into what sources corporations, mass media, and citizen groups use for making the claims uncovered by content analysis and discourse analysis.

The first part of the research process involves the analysis of the network structure among a set of sources for which the data were collected with help of digital research methods. Partly based on the results of part one was the selection of texts analyzed for the content analysis – which is part two of the research process. Finally, the patterns discovered with content analysis were complemented by a more in-depth discourse analysis in part three of the research process.

The decision was made to include three types of sources in the data collection and analysis process, namely sources from the corporate sector, the mass media, and citizen groups. An initial assessment of available online data showed that this combination of sources allowed to include the individual viewpoints of the three actors within the triangle introduced in Chapter 1: the corporate sector and citizen groups, as well as the official government standpoint, which all three sources refer to in varying extents. In addition, initial assessment showed the mass media to varying extents include the stances of the three actors within the triangle.

3.1 Digital Research Methods (DRM)

The first part of the research process involved the use of digital research methods (DRM) for (1) uncovering the network of most prominent sources covering the topic under scrutiny, and (2) identifying the dates with the largest online interest in the topic. DRM is a relatively new research paradigm that evolved recently due to revolutionary advancements of computational power (Berry, 2012), able to analyze ever larger amounts of data. Being an increasing popular method in the field of internet research, for an important part DRM tools collect data from the internet according to a specific strategy resonating with the purpose of the tool (Rogers, 2013). Because next to data collection also data analysis is performed by computers with DRM, the data is primarily collected in formats friendly to computer analysis, namely quantitative code (Berry, 2012). In order to prepare the collected network data for human judgment, it was visualized with special software named Gephi (Benkler, Roberts, Faris, Solow-Niederman & Etling, 2013). In addition, the data regarding the moments of most

prominent interest in the topic were collected, analyzed, and visualized with a tool integrated in the Google search engine, named Google Trends.

3.1.1 Data crawling

In order to collect the required data for the network analysis, a DRM tool named web crawling was used. Specifically, web crawlers follow the out-links from a selected set of URL's functioning as starting points. This following of out-links can be performed for a certain amount of iterations, meaning that if a web crawl is performed for two iterations for instance, one has to click two links in order to end up from the starting point at the desired web page. Because this part of the study is interested in uncovering networks, the decision was made to perform co-link analysis, meaning that in the data collection only sources that at least two starting points link to were included (GOVCOM.ORG, n.d.). Furthermore, a separate crawl was run for the corporate sector, the mass media, and citizen groups.

More specifically, the web crawl tool used for part one of this study was the Issue Crawler tool from the digital methods initiative – which is a collaboration of the University of Amsterdam, the Govcom.org Foundation, and the New Media TEMLab (DmiAbout, 2014). The tool could be accessed through the Issue Crawler website after an account was created and a password was requested through the website. Upon the finishing of each crawl the data could accessed and downloaded from the website.

Since the Issue Crawler tool harnesses individual web links – and tracks these to a following web link, the unit of observation is the individual web link. The unit of analysis is the a web location however (Babbie, 2007), since the output provided by Issue Crawler depicts certain web locations, such as the Careers page of Facebook of the blog page of CNN for instance.

3.1.2 Network data sampling

As it was not possible to obtain a complete sampling frame for the network analysis, meaning a list that includes all the news outlets that published on the mass surveillance disclosures, it was not possible to use probability sampling (Sirkin, 2006). As a result, non-probability sampling was used in two types. First, the starting points inserted in the crawler were picked according to the purposive sampling strategy, meaning that the starting points were selected based on their relevant traits (Sirkin, 2006). Additionally, the following of links in the web

pages performed by the Issue Crawler tool very closely resembled the snowball sampling strategy (Sirkin, 2006).

The starting points of the crawl for the corporate sector were sampled according to their alleged involvement in mass surveillance, because arguably these were most relevant to this study. The companies from the corporate sector that allegedly were involved in mass surveillance, and thus included in the crawl, were AOL, Apple, Facebook, Google, Microsoft, PalTalk, Skype (NSA Prism program slides, 2013), Verizon (Greenwald, 2013a), Yahoo, and YouTube (NSA Prism program slides, 2013). In addition, the starting points for the mass media crawl were sampled according to the prominence of their reporting on the issue. The Guardian and The Washington Post newspapers were praised internationally for their groundbreaking breaking news stories regarding new information on mass surveillance, which they in many cases obtained directly from whistleblower Edward Snowden. Consequently, The Guardian and The Washington Post were in many cases the first ones to publish new information (Associated Press, 2014), indicating their prominence as media sources in relation to this issue. As a result, uncovering the network of sources The Guardian and The Washington Post based their stories on, leads to the very source of the information regarding the mass surveillance disclosures. And Finally, the starting points for the citizen groups crawl were obtained from a page listing 166 Privacy Advocates from different ideological backgrounds, concerned with the issues of online privacy and mass surveillance (Privacy Advocates List, n.d).

3.1.3 Network data collection procedures

Since no press releases nor any corporate blog posts could be retrieved regarding alleged involvement in mass surveillance from the websites of AOL, PalTalk, Skype, and YouTube, these companies were dropped from the research. However, since the websites of Apple, Facebook, Google, LinkedIn, Microsoft, Verizon, and Yahoo did include press releases and corporate blog posts about their alleged involvement in mass surveillance, a total of 30 links to texts could be included in Issue Crawler. The dates of the blog posts included range from June 7, 2013 to April 11, 2014. A co-link analysis was run with 3 iterations (the maximum) and a crawl depth of 2 (default option).

The following crawl included mass media sources. As starting points, the links to two specific web pages from the Guardian and The Washington Post respectively, dedicated to their online news reporting on the NSA topic were included. These web pages are named

'The NSA Files' – from The Guardian (The NSA files, 2013), and 'NSA Secrets' – from The Washington Post (NSA Secrets, 2013). The NSA files is archived under 'World News' and at the time of data collection covered news reporting about the issue starting at June 5, 2013 until December 29, 2013. NSA Secrets is a separate page in itself and includes coverage from June 10, 2013 until April 17, 2014. A co-link analysis was run with 3 iterations and a crawl depth of 3. The choice for a deeper crawl depth was made because in contrast to the individual press releases blog posts links selected for the web crawl of the corporate sector, The NSA files and NSA secrets are homepages, essentially portals, to individual news articles. Hence, a deeper crawl depth is recommended by Issue Crawler (GOVCOM.ORG, n.d.).

The final crawl included citizen group sources. After screening the homepages of the citizen group websites listed in the 'Privacy Advocates' page, 22 homepages were removed from the sample, because of double listings or dead links. The remaining 134 links to the homepages of citizen group websites were included as starting points. A co-link analysis was run with 3 iterations and a crawl depth of 3. The reason for the deeper crawl depth was similar to that of the mass media sources: homepages were used instead of links to specific pages.

3.1.4 Network visualization

After each of the three crawls had finished, the collected data were downloaded from the Issue Crawler tool in a format compatible with the data visualization software named Gephi (.gexf format). After importing them, the respective data files were visualized with the Fruchterman Reingold layout of Gephi. The visualization was depicted by Gephi in a format of nodes and edges. More specifically, in network theory the nodes represent the different actors in a network – in this case the individual sources; and the edges represent the linking network among them (Introduction to Social Network Methods, n.d.). The Gephi visualizations are found in Chapter 4.1 of this study.

3.1.5 Google Trends

The Google Trends tool allowed for identifying the moments of most prominent interest in the NSA mass surveillance debate. Since Google Trends collects individual web searches from people, and from these searches analyzes search terms inserted in the search engine (Where Trends data comes from, n.d.), the search term is the unit of observation as well as the unit of analysis (Babbie, 2007). In addition, the Google Trends tool allowed search terms to be typed in, and as a result depicted the interest of Google search users over a specific period of time.

After probing search terms, it was found that the search terms ‘snowden’ and ‘nsa’ in particular provided insightful results, hence they were adapted as search terms. Furthermore, January 2013 was chosen as the starting date of the time frame, because it is the start of the year of the surveillance disclosures by Edward Snowden, and April 2014 as the end date of the analysis because this was the moment in time the analysis was conducted. The visualization (which can be found in Chapter 4.1 of this study) allowed for the identification of the moments of most prominent interest in the issue. These moments were depicted in units of weeks.

3.2 Content Analysis

For the second part of the study, a content analysis was conducted in order to uncover themes and patterns in the selected texts, providing the broader patterns of explanation against the more in-depth and richer explanations provided by the discourse analysis later on. The method of context analysis has been formally defined as “the study of recorded human communications” (Babbie, 2007, p. 350). As a research instrument, a codebook was developed inductively with help of Grounded Theory, and included both quantitative (numbers) and qualitative (non-numbers) variables, meaning that the latter category allowed for obtaining richer descriptions. However, taking into account the ultimate goal of uncovering themes and patterns, some of the collected qualitative data was re-coded into quantitative data at a later stage in order to make possible analysis in numbers. This allowed for statistical data analysis, and the presentation of the data in the form of percentages.

3.2.1 Selection of texts

A total of 50 texts were selected from three sources: corporate sector press releases or corporate blog posts; online news articles from mass media outlets; and press releases or blog posts from citizen groups. More specifically, 20 texts were selected from the corporate sector; 20 texts from mass media outlets; and 10 texts from citizen groups (see Appendix D). Including a total of 50 texts was expected to result in a sufficient amount of data for finding substantial conclusions, while at the same time being feasible to analyze within the scope of the study.

The press releases and blog posts from all three sources (corporate sector, mass media, and citizen groups) were selected by means of purposive sampling. Based on the results of the Google Trends analysis of the digital research methods part of this study, five time intervals

were identified as ‘key points’ in the Snowden surveillance disclosures event. The time intervals were a week in length, and included the following weeks: June 9, 2013 until June 15, 2013; September 8, 2013 until September 14, 2013; October 27, 2013 until November 2, 2013; December 15, 2013 until December 21, 2013; and finally, January 12, 2014 until January 18, 2014. Preferably, all 50 selected texts are exactly from these five intervals. However, in those instances where no texts from exactly these intervals were available, the text that came closest to the desired time interval was selected for inclusion in the sample.

At the time of sampling for corporate sector texts – which was at April 23, 2014, a total of 30 texts were published as either a press release or corporate blog post at the corporate websites of the selected corporations accused in the media of involvement in surveillance by the NSA, namely AOL, Apple, Facebook, Google, Microsoft, PalTalk, Skype, and Verizon, Yahoo, and YouTube. However, since the corporate websites of AOL, PalTalk, Skype, and YouTube did not include press releases nor corporate blog posts covering the event, the total of 30 texts were consequently retained from Apple, Facebook, Google, Microsoft, Verizon, and Yahoo. In the end, a total of 20 texts were included in the sample, which were selected first based on their fitting in (or close approximation to) one of the five time intervals; and secondly their contribution to the creation of a varied mix of texts in terms of length, as to not only include overtly long nor very short texts. Since six companies were included in the sample, a minimum of three texts from each company was included.

Furthermore, the mass media texts were selected from the websites of four large news outlets, which included three newspapers: namely The Guardian, The Washington Post, and The New York Times; and articles were selected from news agency Reuters. More specifically, while The Guardian and The Washington Post were in many instances the first news outlets to publish breaking news stories regarding new mass surveillance revelations (Associated Press, 2014), they were as sources included in the sample based on this argument. As for The New York Times and Reuters, their inclusion in the sample was based on the results of the digital research methods part of this study, because they proved to be important sources for online news articles of The Guardian and The Washington Post themselves. More on this can be found in the ‘Findings’ section on ‘Digital Research Methods’, which is included in the following chapter (Chapter 4.1) of this study. In addition, as prior to selecting the texts the decision was made to include a total of 20 texts from mass media sources, it appeared logical to select five texts from each of the four news outlets. Similar to the selection of texts from the corporate sector, the five texts per news outlet were selected according to the

five ‘key points’ in time at which the mass surveillance issue in relation to the Snowden case proved a prominent news event according to Google Trends.

Finally, the selection of 10 citizen groups to select texts from for analysis, was predominantly based on the result of the digital research methods analysis performed prior to selection. An exception to the digital research methods analysis results were the two rally’s organized for opposing intrusive mass surveillance named StopWatching.Us and The Day We Fight Back. Based on the massive scope of these rally’s and the global appeal, also in terms of citizen groups supporting it, the two rally’s were included. In addition, the eight other citizen groups included based on the results of the digital research methods analysis are: European Digital Rights (EDRi); Consumers International; Privacy International; Big Brother Watch; American Civil Liberties Union (ACLU); Center for Democracy and Technology (CDT); freepress; and Electronic Frontier Foundation (EFF). While the digital research methods provided a certain of amount of citizen groups to included, in the final selection process it was ensured that citizen groups were included in the sample from a variety of ideological backgrounds, headquartered on a variety of locations around the globe.

3.2.2 Data collection

For the data collection process of the content analysis, several codebooks were created including a mix of open and closed variables. The codebooks were constructed with the method of Grounded Theory, meaning that the variables in the codebook were created through an inductive analysis of patterns, themes, and common categories in the texts (Babbie, 2007). During the process of creating the process, it became clear that the creation of a single codebook could not effectively cover the topics and focus between the three categories of sources, being corporate sector, mass media, and citizen groups. Therefore, the decision was made to construct three separate codebooks for the coverage of the three sources. These three codebooks included common variables in order to allow comparison between phenomena found in all three sources, as well as separate variables as to allow the research instrument to collect data typical to each of the sources. After initial probing with the research instrument in observational data, it was found that some variables could be removed, some added, and of some variables the categories were slightly adjusted. This pilot testing of the codebooks was found to increase validity of the research instrument, benefiting the quality of the data obtained. In the end, the codebook for the corporate sector included 15 variables; the codebook for the mass media included 20 variables; and the codebook for the citizen

groups included 13 variables. The actual codebooks can be found in the attachment of this study. Similar to the method of Grounded Theory, the construction of the codebooks was performed while thinking comparatively and following systematic research procedures adapted from the positivist research tradition, while at the same time an certain level of reflexivity was built in while adapting the codebook after initial probing and periodically stepping back adapted from the interpretivist research paradigm (Babbie, 2007).

3.2.3 Data analysis

Prior to the data analysis stage, but after finishing the data collection stage, the qualitative data collected for the open variables in the codebook had to be re-coded into quantitative data in order to prepare them for numerical analysis. More specifically, from the observation of the qualitative data closed-ended categories were created, after which the open-ended variables were re-coded into closed-ended variables. From the 15 variables originally in the codebook for the corporate sector publications, 13 variables could be used in the codebook including exclusively quantitative variables. Additionally, the mass media codebook contained 13 exclusively quantitative variables, and the citizen groups codebook contained 7 exclusively quantitative variables. After this, the variables in the three codebooks were assessed in terms of reliability of the categories, with the help of a second coder. Each of the coders coded ten articles after which the intercoder reliability measure known as Cohen's kappa was calculated. For all of the 33 variables from the three codebooks, Cohen's kappa ranged between .737 and 1. As a result, the reliability of the variables varied from good (.737) to perfect (1) according to the guidelines for interpretation of Cohen's kappa as outlined by Fleiss (1981).

Regarding statistical analysis of the numerical data collected within the sample of n=50, a crosstabs analysis with Chi square statistical test proved the most suitable. Indeed, because the variables in the codebook were measured at a nominal level data, while also taking the sample size (n=50) into account, the crosstabs analysis with Chi square statistical test was the most sophisticated statistical analysis possible to perform.

More specifically, in order to see whether there would be any statistical significant difference among how the different sources have covered the mass surveillance event, the stances regarding mass surveillance of the corporate sector and the citizen groups where compared across the corporate sector and the mass media, and the citizen groups and the mass media respectively. This analysis was a suitable one, because it proved possible to measure the stances of the corporate sector and citizen groups in difference sources. The same counts

seeing whether a statistical different could be found between the extent to which the corporate sector publications, mass media publications, and citizen group publications covered corporate sector data collection and corporate sector data monetization. Also this analysis was performed by means of a crosstabs analysis with Chi square test.

Finally then, interesting differences within the sample, primarily related to the variables measuring the stances of several actors in relation to current mass surveillance practices will be shown in the form of charts.

3.3 Discourse Analysis

Following the content analysis stage, a discourse analysis was performed on a smaller selection of six texts. In line with the goal of discourse analysts of performing rigorous and in-depth research, the selection of texts is rather small, even though it is certainly possible to extract more than from a single text than one might think at first glance. The discourse analytic method used for this project was deliberately assembled by combining elements from Discourse Theory (DT), represented most notably by Laclau and Mouffe (1985); and Critical Discourse Analysis (CDA), represented most notably by Fairclough (1989). This multiperspectival research produces a broader understanding of the surveillance discourses identified in the texts. More details on the combining of different elements from the DT and CDA theoretical strands can found in Chapter 3.3.2: Research instrument.

3.3.1 Selection of texts

The selection of texts (n=6) for discourse analysis was performed according to a purposive sampling procedure. In other words, individual texts were selected because of specific traits they contained, however it was ensured that within the total sample of six texts, two texts were selected from each source (corporate sector, mass media, and citizen groups). In addition, while selecting the texts, attention was paid in particular to how exemplary they were for the texts from that source. For instance, during the qualitative content analysis stage (so, prior to the re-coding of qualitative into quantitative variables) it was found that many texts from the corporate sector had the showing of the amount of government requests received as a primary issue. With respect to selecting texts from the corporate sector for discourse analysis it was a primary goal then to select the text that most clearly exemplify important points raised throughout all the texts from the corporate sector covering this issue, included in the content analysis sample. As a result, from the corporate sector the exemplary

texts chosen were *Facebook Releases Data, Including All National Security Requests* (from Facebook; June 14, 2013) and *Conundrums in cyberspace – exploiting security in the name of, well, security* (from Microsoft; February 25, 2014) were selected; and from the mass media sector the texts with the titles *Earlier Denials Put Intelligence Chief in Awkward Position* (from The New York Times; June 11, 2013) and *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say* (from The Washington Post; October 30, 2013) were selected; and from the citizen group sector the texts with the titles *Governments break silence on surveillance as activists launch human rights principles* (from Privacy International; September 21, 2013) and *Rating Obama's NSA Reform Plan: EFF Scorecard Explained* (from Electronic Frontier Foundation; January 17, 2014) were selected (see Appendices).

3.3.2 Research instrument

As mentioned, the discourse analysis research instrument used for this study was assembled of concepts from the DT and CDA theoretical strands. More specifically, the concepts included from DT were *element*, *moment*, *nodal point*, *hegemony*, *chain of equivalence*, *master signifier*, *myth*, *social imaginary*; and the concepts included from CDA were *intertextuality* and *interdiscursivity*, which together are roughly similar to the DT concept of *articulation*.

Specifically, *element* refers to a sign in the discourse with a meaning that has not been fixed yet, whereas *moment* is a sign with a fixed meaning within the discourse. For instance, if a certain sign was exclusively articulated in relation to a certain set of other signs in a particular discourse, it was considered as a moment in that respective discourse. In addition, a *nodal point* is particularly open to various meaning ascriptions, because it has not much meaning exclusively by itself, and acquires meaning only in relation to other signifiers. To illustrate, 'democracy' is a nodal point because it is highly dependent on several other signs in discourses to fill it with meaning. *Hegemony* then, in the view of Laclau and Mouffe's DT, takes place in many domains of social life in the form of hegemonic struggle. A *master signifier* is a subject position, which comes in the form of an empty signifier. More specifically, an example of a master signifier would be the sign 'man'. Indeed, because the subject position of 'man' is interpellated differently in various discourses, the example illustrates the dependence of the master signifier on other signs in the discourse to establish identity. As a result, subject positions particularly open to ascriptions of identity are adopted

as master signifiers in this study. Identity is established by a *chain of equivalence*, that links (master) signifiers together. In addition, *myth* refers to a type of floating signifier (a sign particularly open to different meaning ascriptions) that seeks to construct society as a totality. Specifically, myths are identified by their potential to contrast an in-group from an out-group as in 'us vs. them'. For example, explicit references to national identities, such as 'The French' or 'The Dutch' are identified as myths due to the discursive dichotomy created by the myth between an in-group and an out-group. Once a myth has succeeded in naturalizing a particular vision of social order – in other words, this vision has established hegemony, one speaks of *social imaginary*. Finally, *intertextuality* refers to how a texts responds to, reworks, or only re-accentuates past texts, and in doing so contributes to the making of history and the wider processes of change; and *interdiscusivity* refers to elements used in a certain discourse and social practice, which at the same time carry meanings from other discourses and social practices (Jørgensen & Phillips, 2002).

3.3.3 Research procedures

The data from the six texts were collected and analyzed during a procedure essentially consisting of four stages. During the four stages, the texts were read and analyzed multiple times. The four stages will be subsequently summarized in this section.

First of all, the texts were read a few times, and from each text the key signifiers were identified and listed. Secondly, the texts were analyzed more in-depth – at times even on a sentence level – in order to identify additional constructs such as myths, moments, social imaginary, intertextuality and interdiscursivity. Then, the relationship was established among the key signifiers in the texts (chain of equivalence). And finally, during a process which qualifies more as a rhetorical analysis than discourse analysis, justifications were identified. More specifically, underlying ideologies, arguments, threats, and prospects were identified.

3.3.4 Data Analysis

First, key signifiers such as nodal points and master identifiers, but also moments and myths were identified in the text. Through establishing the chains of equivalence among these signifiers, it was possible to net out the central discursive structure among the discourses active in hegemonic struggle. A summary of this can be found in Chapter 4.3. These central discursive structures constituted the frameworks of the separate discourses. Furthermore, the key signifiers were compared across discourses, particularly to identify attempts of discourses

to fix a sign in a particular way, in order words a hegemonic intervention. Furthermore, attention is paid to the naturalized understandings of certain signifiers and the very ideology supporting justifications.

Chapter 4: Findings & Discussion

This chapter presents findings of the empirical research of this study, as well as the synthesis of the findings in order to find conclusions and the reflection on scholarly literature. Subsequently, the chapter first deals with the findings of the first part of the research, which were generated through the use of digital research methods; in which network analysis and Google Trends were used. This part is followed by the findings of the content analysis; and finally, the interpretations from the discourse analysis are presented. After, the results are synthesized in the following sections. The final section concludes with a reflexivity report.

4.1 Network Analysis Findings

This section first presents the findings of the network analysis. In addition to the network visualizations, the results of the Google Trends analysis will be presented. A network visualization was produced for every source of publications included in the research. Hence, the first visualization (Figure 4.1) represents the network of the corporate publications; the second (Figure 4.2) the network of mass media publications; and the final visualization (Figure 4.3) depicts the network of citizen groups visualizations.

Network analysis, which is a (visual) analysis methods derived from network theory, envisions structures such as social relations, institutional ties – and in this case websites as a network (Wasserman & Faust, 1994). The visuals below reveal the network of common sources that the three types of publications draw on in terms of linking structure. More specifically, after the starting points of the analysis were tracked for 3 iterations, the websites that were linked to at least two times are included in the visuals. These websites are represented as dots in the visual (called 'nodes' in network theory), and the links among the common sources are visually represented as links among the nodes. In network theory these links are called 'edges'. They represent how the network of common sources are linked among one another (Introduction to Social Network Methods, n.d.).

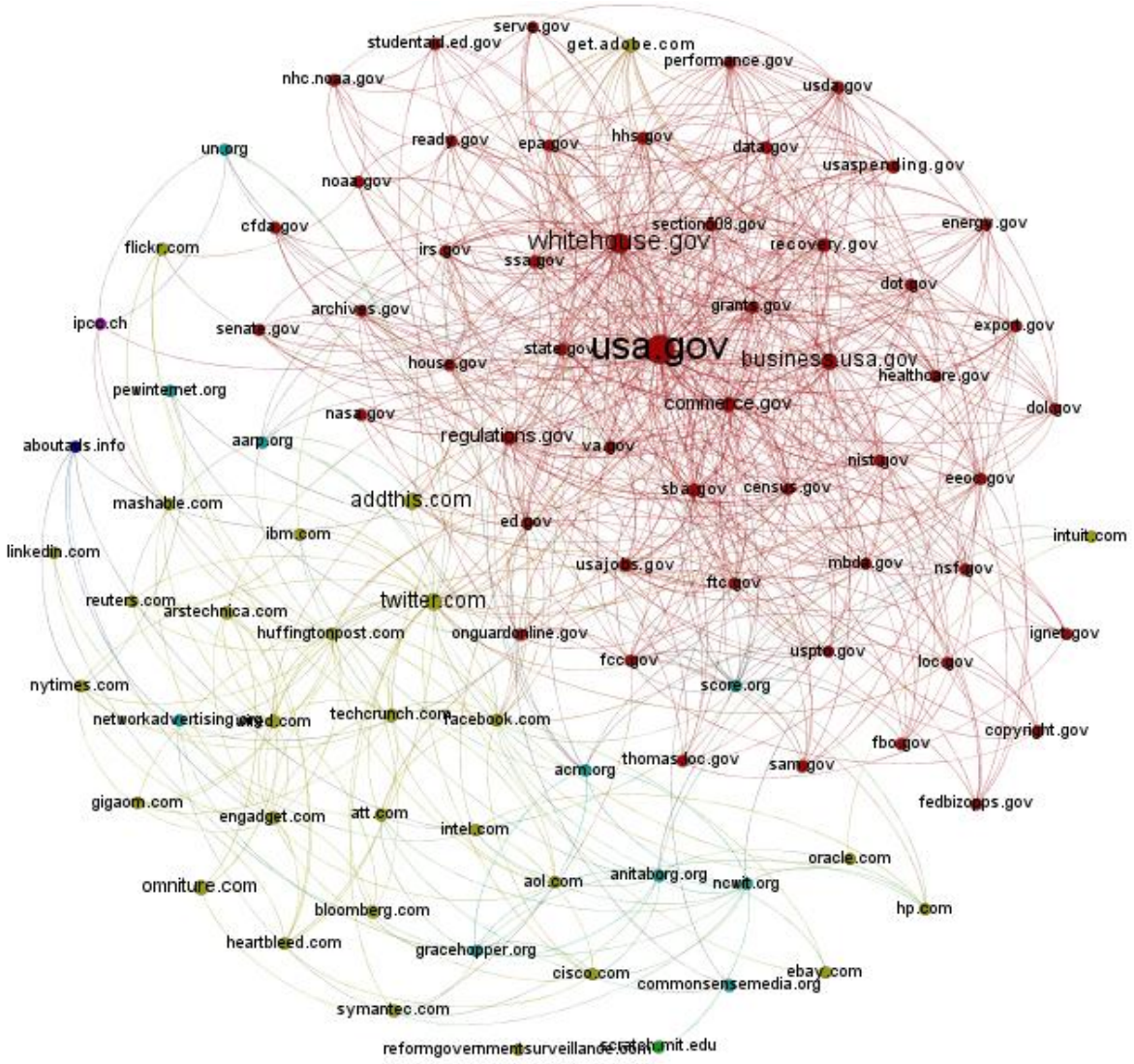

Figure 4.1: Network of corporate publications

The visualization in Figure 4.1 depicts the network of websites that the corporate publications draw on. In total, the network includes 15.141 nodes and 35.951 edges, the most prominent ones visualized in Figure 4.1. The size of each node represents the prominence of the website in the network of common sources. In other words, the larger the node in the visual, the more in-links it receives from other sources in the network.

Very notable in Figure 4.1 is the very dense network among the websites from the U.S. government (.gov top-level domain). In order to prepare the visualization for analysis by the human eye, a red color was given to the U.S. government websites as well as to the links among them. The dense network of U.S. government websites suggests that that in terms of linking structure, the corporate publications included in this research very notably draw on the U.S. government.

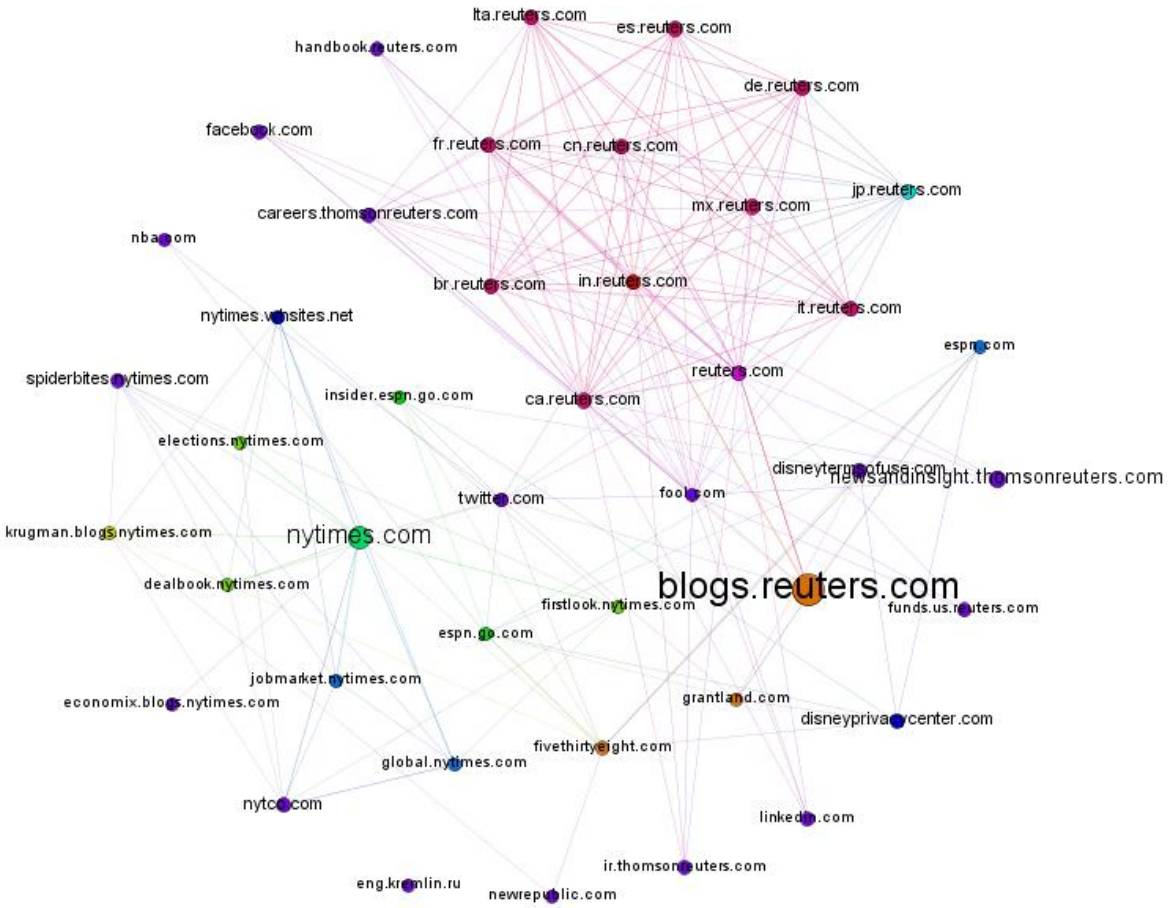

Figure 4.2: Mass media network

Figure 4.2 depicts the network of common sources drawn upon by the mass media publications included in the research. While the entire network includes 5.413 nodes and 73.777 edges, the most prominent ones are visualized in Figure 4.2.

Also here nodes and edges were given colors in order to increase the explanatory power of the visual. Notably, two sub-networks in the visual can be identified. First, the network in light-blue reveals that the homepage of *The New York Times* (nytimes.com) is an important source to the mass media publications included in the research. Secondly, the network in pink-purple reveals that *Reuters* is an important source to the mass media publications, as deduced from the large number (17) of nodes from reuters.com in the visual. In addition, an odd outlier in this visual is the rather large node of blogs.reuters.com. This odd outlier may be explained by the fact that there could be a permanent link to the blogs page of Reuters (blogs.reuters.com) promoted on every page of the Reuters website. As a result, the blogs.reuters.com node appears very prominently in the visual as receiving many in-links

from other sources in the network. As mentioned in Chapter 3, this visual contributed to the selection of mass media texts for content analysis.

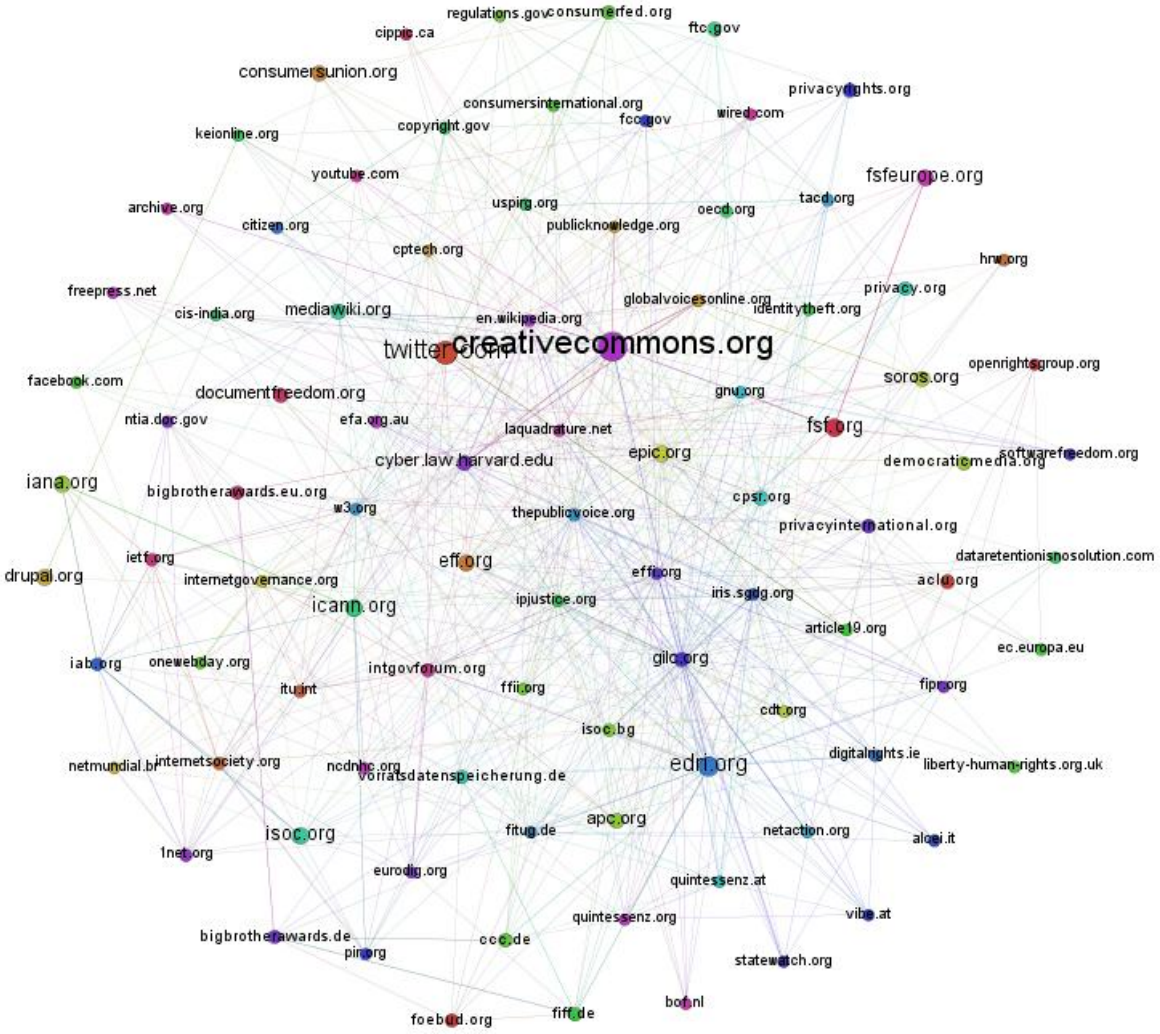

Figure 4.3: Citizen group network

Notably, Figure 4.3 reveals the dense connection among almost all of the nodes in the network of common sources of citizen groups publications. In total this network contains 7.807 nodes and 13.277 edges, from which the most prominent ones are visualized in Figure 4.3.

A few notable nodes such as Twitter.com in red are not citizen groups, however their inclusion in the visual most plausibility is because of same reason why blogs.reuters.com appeared in the mass media network visualization: many citizen groups included in the network could have a link to their Twitter page and as a result Twitter.com is featured very

prominently in the visualization. Also in this case, the visual was used for the selection of citizen group text in the content analysis, more on this in the previous chapter.

4.1.1 Google Trends

This section also includes a presentation of the findings of the analysis with Google Trends showing how the story developed, and what the key moments are regarding online interest in the story.

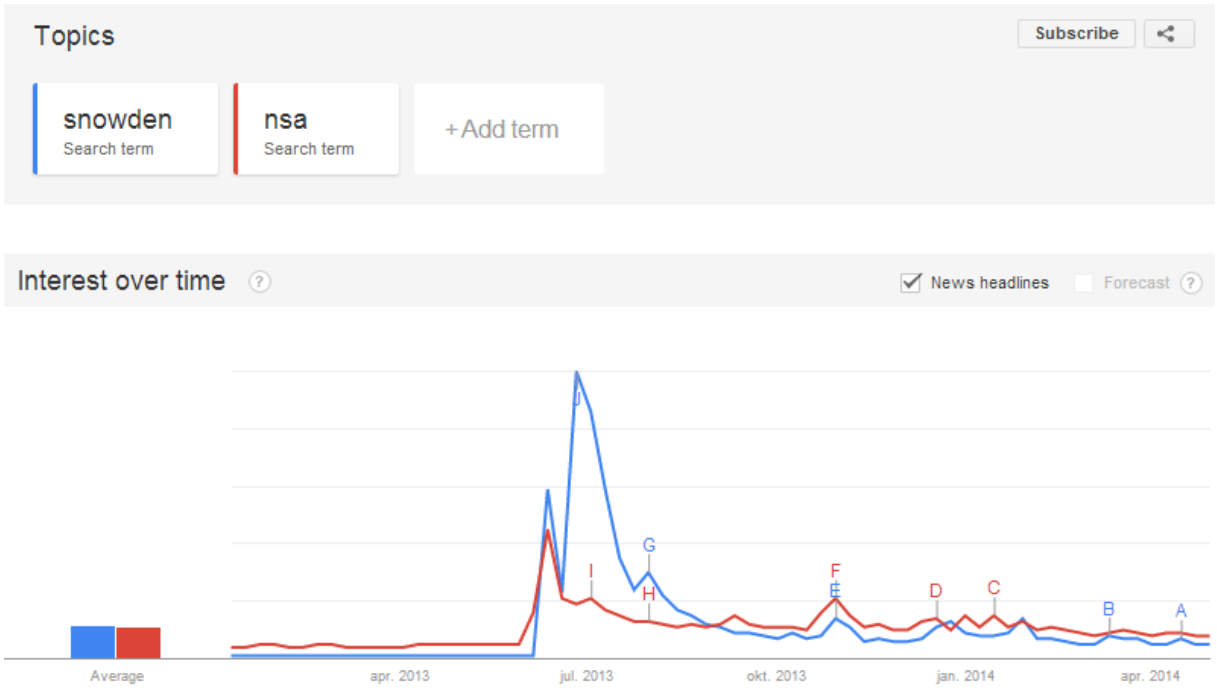

Figure 4.4: Google Trends graph

The analysis with Google Trends was performed from the first month of the year that the mass surveillance story first appeared in the news (January 2013) until the month the analysis was conducted (April 2014). This time frame allowed to capture most of the information, seeing that it includes information on the worldwide online interest in the story before and after Snowden the first disclosures were made by Snowden in early June, 2013.

The search terms ‘nsa’ and ‘snowden’ were found to capture the story most accurately seeing that the Google News stories attached to the key moments of interest (depicted in Figure 4.4. as letters on top of the peaks in the graph) were about the mass surveillance scandal. Very notably, the Figure 4.4 graph reveals that the online interest – measured by means of the amount of Google searches to these key words, skyrocket in early June, 2013.

More specifically, this is the week from June 9, 2013 until June 15, 2013; as Google Trends analyzes key moments of interests in units of weeks.

As seen in Figure 4.4, the interest in either one of the search terms may vary widely. For instance, while in the week of June 23, 2013 until June 29, 2013 there is maximum interest in the search term 'snowden' on Google, this is not at all the case for 'nsa'. To illustrate, observed from the average 'weight' Google Trends assigns to the search terms during certain time units, during this week the interest in 'snowden' was 100; whereas the interest in 'nsa' was 19. In terms of determining what the key moments of online interest in the story were, the decision was made retain those time units of common unusual large interest in both of the search terms. Google Trends reveals that these were June 9, 2013 until June 15, 2013 (nsa 46; snowden 58); September 8, 2013 until September 14, 2013 (nsa 15; snowden 9); October 27, 2013 until November 2, 2013 (nsa 21; snowden 14); December 15, 2013 until December 21, 2013 (nsa 14; snowden 11); and January 12, 2014 until January 18, 2014 (nsa 15; snowden 8). As mentioned in Chapter 3, the Google Trends analysis was used for the selection of publications for content analysis.

4.2 Content Analysis Findings

This section includes the findings of the content analysis part of the study. From the codebook used for the content analysis specific relations among variable arose as particularly interesting to explore. These include the mentioning of data collection and data monetization by the corporate sector, which will indicate to what extent the involvement of the corporate sector in mass surveillance through data collection and data monetization is covered in the respective sources. In addition, the stances of different triangular sectors regarding current mass surveillance practice are covered, as well as the justifications they use to support their stance.

In this chapter, these patterns are first explored most prominently by means of frequency distributions, most notably percentage charts. After this, any potential statistical significant differences among the stances of the corporate sector and the citizen groups sector are explored; as well as any potential statistical significant differences among to what extent the three sources cover data collection as well as data monetization by the corporate sector.

4.2.1 Relative frequency distributions

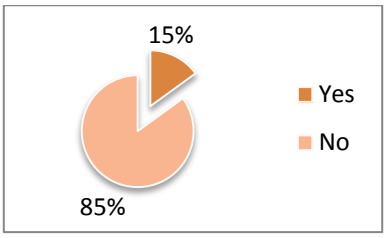

Figure 4.5: Corporate Publications

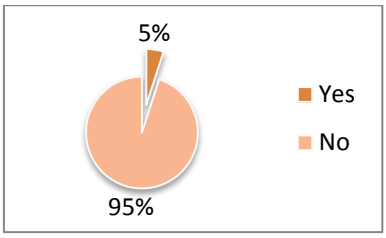

Figure 4.6: Mass media Publications

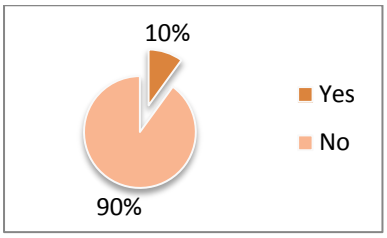

Figure 4.7: Citizen group Publications

The above charts (in orange) reveal that a small minority of publications mention data collection by the corporate sector, most notably the corporate sector itself – through 15% of its publications (Figure 4.5). In addition, 5% of mass media publications (Figure 4.6) mention data collection by the corporate sector, and 10% of citizen groups publications (Figure 4.7) mention data collection by the corporate sector. As a result, it can be observed from the above charts that corporate sector data collection largely ignored in all three sources.

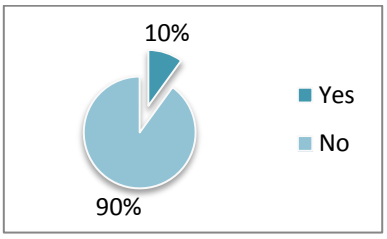

Figure 4.8: Corporate Publications

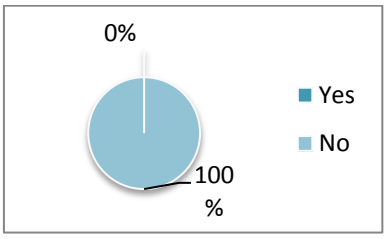

Figure 4.9: Mass media Publications

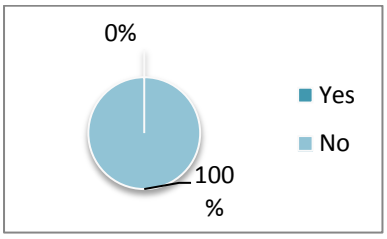

Figure 4.10: Citizen group Publications

In addition, the pattern becomes even more pervasive when considering the mentioning of data monetization by the corporate sector. Apart from 10% of corporate sector publications mentioning it (Figure 4.8), it is not addressed in neither one of the publications (Figures 4.8 – 4.10).

However, when considering the data not exclusively quantitatively, but also qualitatively, data collection and data monetization are mentioned in the following context by one of the corporate sector publications from Apple in the content analysis sample: “Our business does not depend on collecting personal data. We have no interest in amassing personal information about our customers.” (Report on Govermment Information Requests, 2013). In other words, even in the publication in which data collection and data monetization

are mentioned, the accusations made by the press about corporate sector involvement in the surveillance process are rejected. Thus, content analysis suggests that the involvement of the corporate sector in mass surveillance by means of data collection and data monetization is largely absent in all three publications. Arguably, the potential mentioning of mass surveillance in the publications will most notably cover state surveillance.

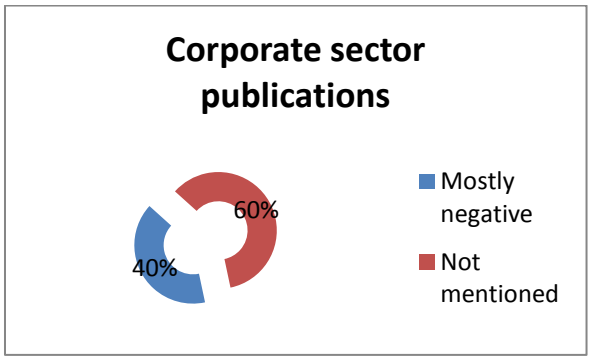

Figure 4.11: Stance in corporate sector publications

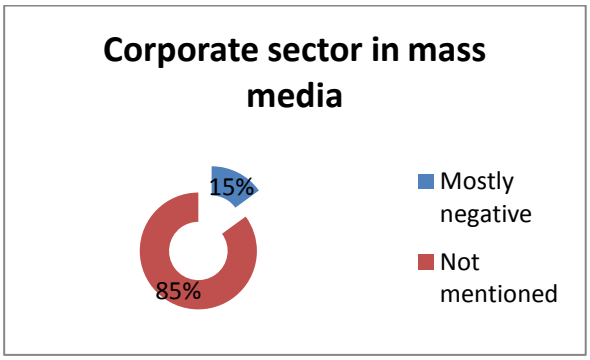

Figure 4.12: Stance of corporate sector representatives in mass media

As shown in Figure 4.11 and Figure 4.12, in a far larger percentage of instances (40% - Figure 4.11) corporate sector publications contained a stance from the corporate sector towards current mass surveillance practices by the state – which if expressed was predominantly negative in all cases, than mass media publications. Also in mass media publications in all instances (15% - Figure 4.12) where a corporate sector representative was cited, the opinion expressed was in all cases negative towards state mass surveillance.

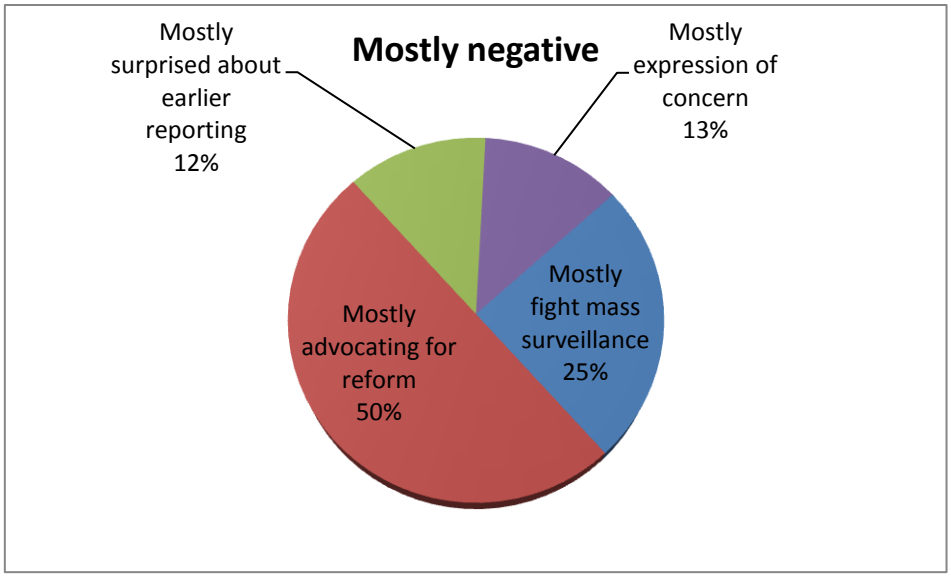

Figure 4.13: Justification for stance corporate sector

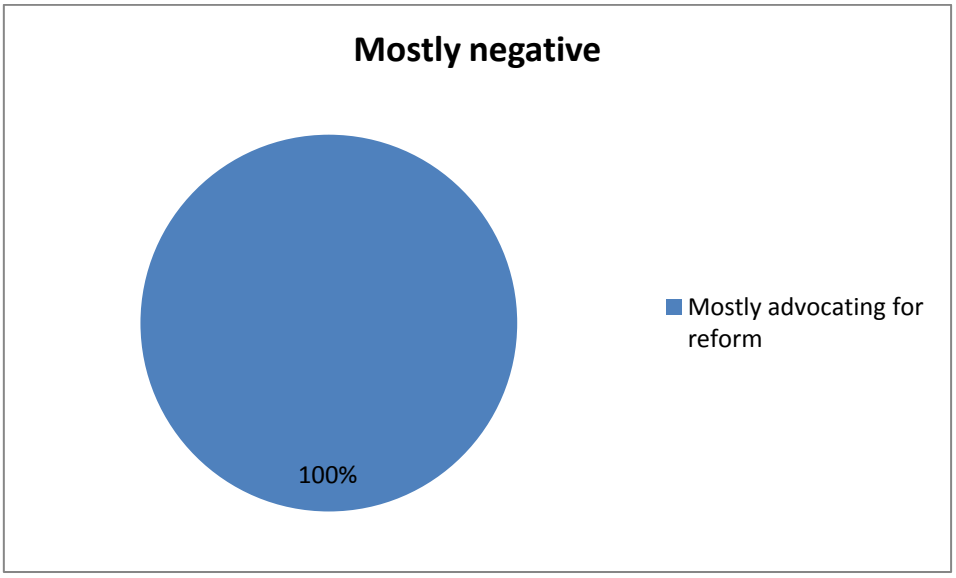

Figure 4.14: Justification for stance corporate sector representatives

As depicted by Figure 4.13 and Figure 4.14, the mentioned supporting justifications for the predominantly negative stance towards mass surveillance practices by the corporate publications was far more diverse (Figure 4.13), than the justification provided by the corporate sector representatives cited in mass media publications (Figure 4.14). Whereas in the latter case all representatives cited mostly advocated for reform of state surveillance practices, this was only the case in 50% of the corporate sector publications. In addition, in 12% of the instances the publications from the corporate sector mentioned being mostly surprised about earlier mentions of state mass surveillance, and 13% mostly expressed concern as primary justification for their negative stance towards state surveillance. Finally, in

25% of the publications the negative stance could be deduced from the indication to fight state surveillance.

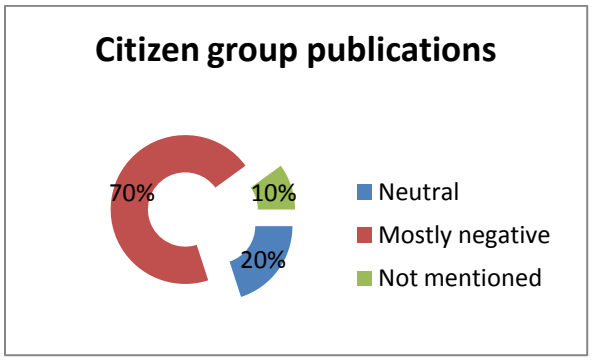

Figure 4.15: Stance in citizen group publications

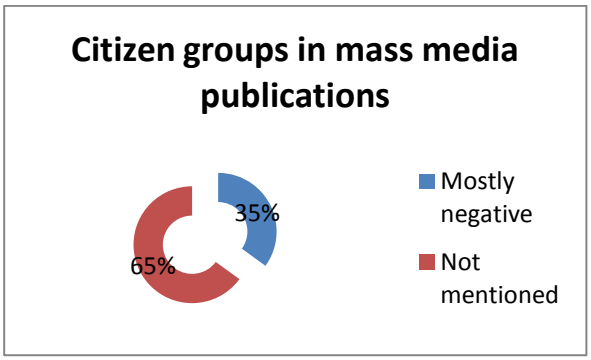

Figure 4.16: Stance of citizen group representatives in mass media

An even stronger trend could be observed for the citizen groups in the sample. While in 65% of the mass media publications, no mention of a stance of citizen groups regarding state mass surveillance was found (Figure 4.16) – the other 35% being mostly negative, 90% of the citizen group publications in the sample included a stance regarding current state mass surveillance practices (Figure 4.15). More specifically, as Figure 4.9 shows, the large majority of citizen group publications in the sample was mostly negative about current state mass surveillance, while 20% expressed a neutral opinion, and the remaining 10% did not mention a stance.

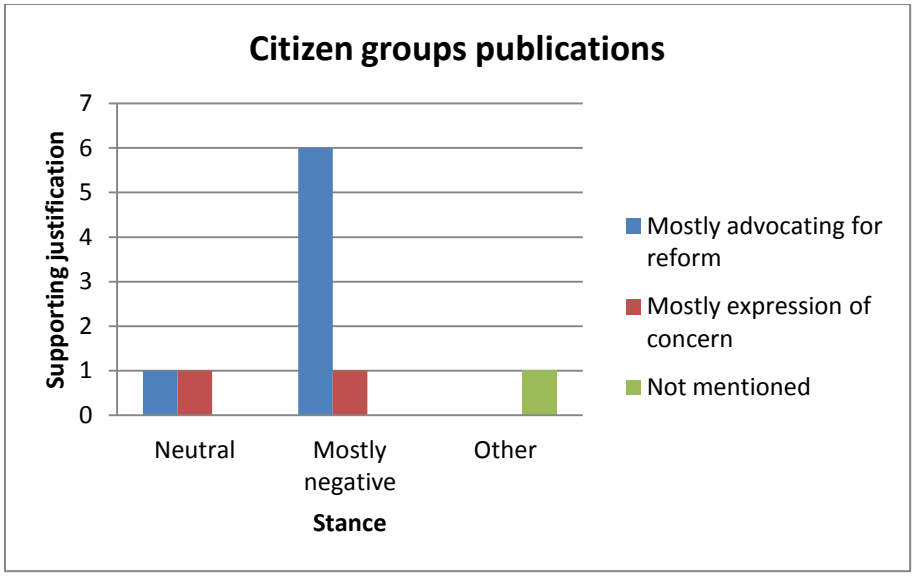

Figure 4.17: Supporting justification citizen groups

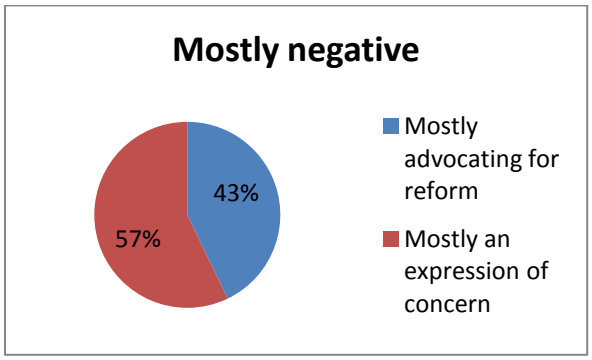

Figure 4.18: Supporting justification citizen groups in mass media

It is primarily noteworthy that in the large majority (86%) of the citizen group publications that is negative about mass surveillance, mostly advocating for reform was found to be the most prominent justification for their negative stance, while in just 14% of the publications mostly an expression of concern was found as primary justification (Figure 4.17). This pattern is reversed when considering the citizen groups representatives brought forward as spokespersons in the mass media publications in the sample (Figure 4.18). Indeed, in 'only' 43% of the instances the representatives were found to mostly advocate for reform, while 57% mostly expressed concern.

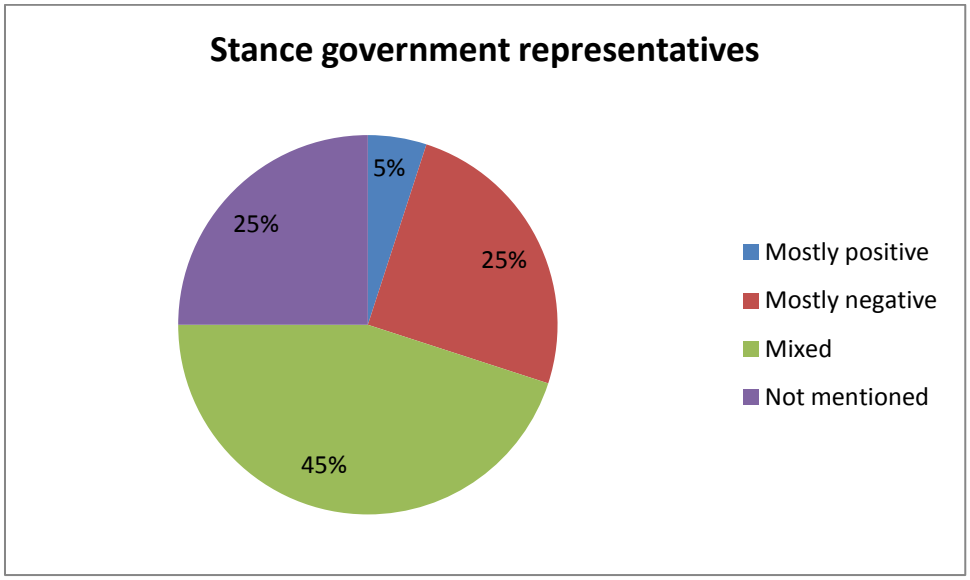

Figure 4.19: Stance government representatives in mass media

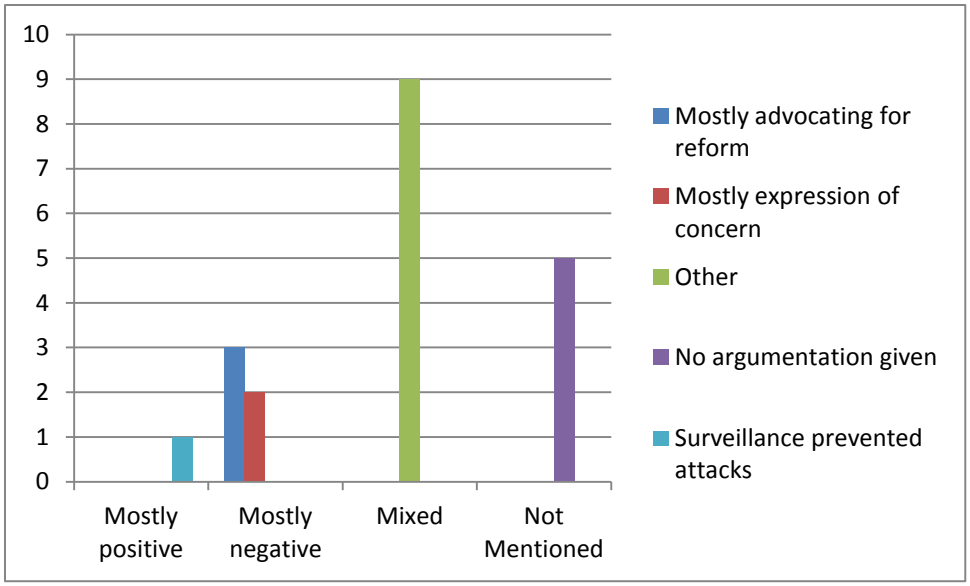

Figure 4.20: Supporting justification government representatives in mass media

As Figure 4.19 shows, in by far most of the mass media publications government officials expressed a mixed opinion – meaning that officials with a negative stance as well as officials with a positive stance regarding current state mass surveillance practices were mentioned in the texts. In addition, Figure 4.20 shows that these mixed stances thrived on supporting justifications classified under the category 'Other'. This indicates that several supporting justifications were used, since multiple stances were mentioned.

In addition, 25% of mass media publications cited government officials expressing a mostly negative stance towards state surveillance (Figure 4.19), mostly using the call for reform (60%) and the expression of concern (40%) as supporting justifications for substantiating their stance (Figure 4.20). And finally, with 5% a small minority of mass media publications included a mostly positive stance towards mass surveillance (Figure 4.19), which back up their stance with the claim that mass surveillance has prevented terrorist attacks (Figure 4.20).

In sum, the arguably intuitive expectation that corporations' and citizen group's own publications provided these sectors with more opportunity for expressing their (predominantly negative) views on current state mass surveillance practices than the mass media did, were confirmed by the publications included in the content analysis. More specifically, in only 35% of the mass media publications citizen group representatives were given the chance to express their opinion, for corporate sector representatives the figure was even lower with only 15% of publications.

Furthermore, it is noteworthy that mass media heavily draws on stances of government representatives (75% of mass media publications contained these citations), over representatives from citizen groups (35%) and the corporate sector (15%). In addition, regarding the sectors mostly negative towards mass surveillance, which were the corporate sector and citizen groups, mostly advocating for reform appeared most frequently as supporting justification.

4.2.2 Inferential statistics

In addition, any potential statistical significant difference in terms of what stance the corporate sector expresses in corporate publications and mass media publications was assessed. Furthermore, a potential significant difference in the stance of the citizen group sector in the citizen group's publications and mass media publications was explored. Also, a possible significant difference in the extent to which the representatives of the three sectors mention data collection and data monetization was assessed.

As the original variables in the codebooks (see Appendix A-C) were measured on a nominal scale, the appropriate method for making predictions about the relationship between variables in the population is the contingency table or crosstabs. Accordingly, the appropriate statistical test that is to be calculated is the Chi square (Sirkin, 2006).

	Corporate sector	Mass media	Total
Mostly critical	8 (40%)	3 (15%)	11 (27,5%)
Not mentioned	12 (60%)	17 (85%)	29 (72,5%)
Total	20 (100%)	20 (100%)	40

Chi square = 3.14; with 1 df; p = 0.08

Table 4.1: Stance of corporate sector regarding mass surveillance

Table 4.1 reports $\chi^2(1, N = 40) = 3.14$, $p = .08$, meaning the null hypothesis cannot be rejected. This means that any observed difference observed among corporate sector publications and mass media publications regarding the stance of the corporate sector in terms of mass surveillance, may be due to chance alone.

	Citizen groups	Mass media	Total
Neutral	2 (20%)	0 (0%)	2 (6,7%)
Mostly critical	1 (10%)	7 (35%)	8 (26,7%)
Other	7 (70%)	0 (0%)	7 (23,3%)
Not mentioned	0 (0%)	13 (65%)	13 (43,3%)
Total	10 (100%)	20 (100%)	30

Chi square = 14.25; with 3 df; p = 0.00

Table 4.2: Stance of citizen group sector regarding mass surveillance

Table 4.2 reports $\chi^2(3, N = 30) = 14.25$, $p = .00$. However, the null hypothesis cannot be rejected, because 6 cells have an expected count of less than 5 (see also Appendix K). This indicates a violation of the assumptions of the Chi square test (Sirkin, 2006), meaning that any difference observed among citizen groups publications and mass media publications in terms of the stance of the citizen group sector regarding mass surveillance, may be due to chance alone.

	Corporate sector	Mass media	Citizen groups	Total
Yes	3 (15%)	1 (5%)	1 (10%)	5 (10%)
No	17 (85%)	19 (95%)	9 (90%)	45 (90%)
Total	20 (100%)	20 (100%)	10 (100%)	50

Chi square = 1.11; with 2 df; p = 0.57

Table 4.3: Mentioning of corporate sector data collection

Table 4.3 reports $\chi^2(2, N = 50) = 1.11$, $p = 0.57$, meaning that the null hypothesis cannot be rejected. In addition, 3 cells have an expected count of less than 5 (see also Appendix K) –

violating Chi square's basic assumption (Sirkin, 2006). Therefore, any differences among the corporate sector, government, and citizen groups regarding the mentioning of corporate sector data collection could be due to chance alone.

	Corporate sector	Mass media	Citizen groups	Total
Yes	2 (10%)	0 (0%)	0 (0%)	2 (4%)
No	18 (90%)	20 (100%)	10 (100%)	48 (96%)
Total	20 (100%)	20 (100%)	10 (100%)	50

Chi square = 3.13; with 2 df; p = 0.21

Table 4.4: Mentioning of corporate sector data monetization

Table 4.4 reports $\chi^2(2, N = 50) = 3.13$, $p = .21$, meaning that the null hypothesis cannot be rejected. Furthermore, 3 cells were found to have an expected count of less than 5 (see also Appendix K). This indicates that the null hypothesis cannot be rejected, and thus any differences among corporate sector, government, and citizen groups regarding the mentioning of corporate sector data monetization, may be due to chance alone.

4.3 Discourse Analysis Findings

This section presents the interpretations of the discourse analysis, including the identified discourses and key signifiers. Prominent key signifiers included are *nodal points*; *master signifiers*; and *myths*; as well as the most important *moments* identified determining the meaning of the key signifiers in their respective discourses. The discourses identified within the order of discourse of surveillance are: *cyberlibertarian discourse*; *commercial discourse*; *national security discourse*; *surveillance discourse*; *legal discourse*; and finally, *activist discourse*.

4.3.1 Cyberlibertarian discourse

In cyberlibertarian discourse, the *myth* of technology assumes a central place, and most of the other key signifiers assume their position in relation to this myth. Indeed, the *nodal points* 'cybersecurity', 'privacy', and 'internet' are positioned in relation to technology. More

specifically, in cyberlibertarian discourse ‘internet’ derives its meaning prominently from moments such as ‘communication’, ‘information’, ‘network’, and ‘data’. ‘Internet users’ is the *master signifier* commonly associated with ‘internet’, ‘privacy’, and ‘cybersecurity’. ‘Cybersecurity’ and ‘privacy’ have a special relation in cyberlibertarian discourse, because ‘cybersecurity’ reinforces ‘privacy’. ‘Cybersecurity’ derives an important part of its meaning from the *moment* ‘encryption’. The central importance of ‘privacy’ in cyberlibertarian discourse comes from *interdiscursivity* with activist discourse.

4.3.2 Commercial discourse

Commercial discourse very importantly centers around the *myth* of market forces, explaining the dependency of business on ‘users’ and ‘customers’, which are both *master signifiers* in commercial discourse. This dependency is reflected in the two nodal points in commercial discourse, namely ‘trust’ and ‘transparency’. More specifically, users and customers should have trust in business. While trust may have been damaged by an outside entity named ‘government’ (*myth*), ‘transparency’ is ‘progress’ (*moment*) in the sense that it (partly) may restore trust. While users/customers should be protected (*moment*) from ‘government’, they should also be protected by government from outside threats such as ‘terrorists’ (*master signifier*). The adoption of the master signifier ‘terrorist’ by commercial discourse is due to *interdiscursivity* with national security discourse.

4.3.3 National security discourse

National security discourse centers around the *myths* ‘The Public’ and ‘The Nation’. The public in relation to the nation is specific in the *master signifier* ‘Americans’. These need protection (moment) from an out-group denoted with the *myth* ‘Enemies’. Notably, since in national security discourse enemy derives its meaning from the public, the nation, and Americans, it necessarily means that enemies are by default ‘foreign’ (moment). A very notable threat (*moment*) in national security discourse is ‘terrorist’ (*master signifier*) or ‘terrorism’ (*nodal point*). In order to provide a sufficient level of ‘security’ (*nodal point*) to protect (moment) Americans against these enemies, the nation collects (*moment*) ‘intelligence’ (*moment*). Intelligence in national security discourse denotes the same phenomenon as ‘surveillance’ in surveillance discourse and activist discourse. Intelligence is positioned in national security discourse in relation to the *moment* ‘classified’.

4.3.4 Surveillance discourse

'Privacy' (*nodal point*) assumes a very notable position in surveillance discourse, and is positioned in relation to the *moment* 'surveillance'. In turn, surveillance – also for its relation to privacy – is very prominently positioned by the *master signifier* 'intelligence agencies', and the *moments* 'secrecy', 'spying', 'data collection', 'interception', 'infiltration', and individual surveillance programs such as 'PRISM' and 'MUSCULAR'. Also, surveillance derives an important part of its meaning in surveillance discourse from the *myths* 'Government' and 'The American People'. Through the moment 'secrecy', surveillance is positioned in relation to the *nodal point* 'accountability', which in turn derives its meaning prominently from privacy and 'Americans' (*master signifier*).

4.3.5 Legal discourse

Arguably, the most prominent key signifier in legal discourse is the *nodal point* 'Law', which assumes a central position. Law is maintained by the judiciary/court (*master signifier*), and exercised over 'accused' ones (*master signifier*) in order to achieve 'justice' (*nodal point*). In the context of surveillance, legal discourse very prominently position law in relation to individual laws serving as *moments* such as the 'Foreign Intelligence Surveillance Act (FISA)', USA Patriot Act, and Executive Order 12333. In addition, in the context of surveillance, legal discourse very prominently positions the judiciary and courts in relation to specific courts dealing with surveillance issues such as the 'Foreign Intelligence Surveillance Court (FISC)' (*moment*) and the *moment* 'oversight', which itself also is positioned in relation to justice.

4.3.6 Activist discourse

In activist discourse, the *moment* of 'surveillance' is given meaning prominently in relation to other *moments* such as 'spying', 'data collection', 'data infiltration', 'interception', and specific surveillance programs, such as PRISM. In turn, these latter moments stabilize surveillance in activist discourse, and have *nodal points* such as 'Privacy' and 'Human Rights' derive their meaning partly from surveillance. In turn, surveillance is positioned in a governmental context in activist discourse by the *myth* 'government'. In addition, also through surveillance, the *master signifier* 'whistleblower' gives meaning to the nodal points of 'transparency' and 'accountability'. Furthermore, the nodal point of 'human rights' is also stabilized for an important part in relation to individual rights, such as 'right to privacy', 'right to free expression', and 'right to free association', which are moments. Finally, the myth of

technology, adopted from cyberlibertarian discourse through interdiscursivity also stabilizes 'surveillance'.

4.4 Discussion: Corporations

The stances of the corporate sector were indeed most prominently deduced from corporate sector publications and the statements of corporate sector representatives in mass media publications. Although as observed from Chapter 4.2.1 corporate sector publications themselves provided most opportunity for expressing a stance. Furthermore, from the network analysis (Figure 4.1) it was observed that corporate sector publications essentially draw on government for explaining their stance regarding mass surveillance. An observation that is contradicted by content analysis as well discourse analysis, however. Indeed, as the charts from content analysis of Chapter 4.2.1 have revealed, the corporate sector and the government take substantially different stances regarding mass surveillance, and their justifications also differ accordingly. Furthermore, the corporate sector was found to prominently refer to cyberlibertarian and commercial discourse. By contrast, the government does not draw on these discourses at all.

4.4.1 Damaged customer trust

As mentioned in Chapter 4.2.1 the corporate sector has a negative attitude towards mass surveillance practice. This is explained more in-depth by discourse analysis as damaged trust on the side of customers in the technology industry. Indeed, trust is a key signifier in commercial discourse (see Chapter 4.3.2), and explains for an important part the relation among customers and the myth of market forces.

More specifically, the corporate sector presents the current surveillance excesses as fully committed by the government. The price for decrease in customer trust is paid by technology companies accused of providing technologies that in some way facilitate government surveillance. This stance is well illustrated by Microsoft: "At Microsoft, establishing and sustaining trust with our customers is essential. If our customers can't rely on us to protect their data […] from […] excessive government intrusion – they will look elsewhere for a technology provider." (Text 2).

A prominent solution to the perceived trust damage in the technology industry is presented in cyberlibertarian discourse in the form of encryption (see Chapter 4.3.1). Good encryption heightens cybersecurity of the internet, which secures data flows across the

internet. Implicit in the solution presented is the fundamental myth of technology in cyberlibertarian discourse. More specifically, cyberlibertarian discourse explains technology as a force in society with a fundamental potential to have positive effect. This is illustrated by United Nations Commissioner Navi Pillay while she uses cyberlibertarian discourse when explaining her view on technology, stating: "Technological advancements have been powerful tools for democracy by giving access to all to participate in society." (Text 5). It may come as no surprise then, that the solution to the trust problem presented in cyberlibertarian discourse should be a technological one: encryption. This solution is formulated by Microsoft as follows: "[Technology] industry can help by continually updating and advancing technology options that enable greater data protection." (Text 2).

Another solution presented by the corporate sector is increased transparency – a key signifier in commercial discourse. More specifically, technology companies such as Facebook and Microsoft have asked the U.S. government for permission to officially publish numbers on national security-related requests received from governments for user data. Eventually this permission was granted, and as a result several U.S. technology companies publish these numbers in 'Transparency Reports'. More specifically, companies are authorized by law "To communicate about these numbers in aggregate, and as a range."(Text 1).

Notably, the latter solution presented by the corporate sector in the form of 'Transparency Reports' reveals an important inconsistency. To clarify, Facebook supports the publications of Transparency Reports with the following argumentation: So that "Our users around the world can understand how infrequently we are asked to provide user data on national security grounds." (Text 1). However, if the number of requests for user data were to be so surprisingly low, there would be no need to add an additional layer of secrecy by only permitting technology companies to publish numbers in aggregates and ranges. Indeed, arguably it would be in the best interest of both companies and governments to communicate univocally how little data is being provided by companies, as to facilitate customer trust. Instead, the technology industry is only allowed to publish numbers in ranges of 1,000.

4.4.2 'We versus them'

Furthermore, while in commercial discourse the corporate sector positions itself as the protector of the public on one side (see Chapter 4.3.2), and the government as the party that the public needs to be shielded from on the other side, the corporate sector positions a myth of government that is fundamentally ideological. Through logic of equivalence, the corporate

sector creates an artificial dichotomy among the general public and companies versus the government, which if naturalized may (have) become social imaginary. A good illustration of this logic of equivalence is used by Facebook: "We will continue to be vigilant in protecting our users' data from unwarranted government requests, and we will continue to push all governments to be as transparent as possible." (Text 1).

Simultaneously, by adopting terrorism as a key signifier from national security discourse through interdiscursivity with commercial discourse, the corporate sector engages in the contradictory activity of justifying an activity it also condemns through logic of equivalence. Indeed, while the corporate sector justifies government data requests on national security grounds, by stating that they help protect users "From criminal activity, including terrorism" (Text 2), it also through logic of equivalence creates a myth of government engaging in grave surveillance excesses. In addition, while Facebook argues that "national security-related cases are by their nature classified and highly sensitive" (Text 1), it also states that it pushes government to be as transparent as possible.

Furthermore, the discourse used by the corporate sector fundamentally omits its own role in current mass surveillance. Indeed, even though technology companies perceive a decrease in customer trust, it has been exactly the public's trust in commercial companies to facilitate the commercial infrastructure of internet for our communicative, informational - and since the web 2.0 and social media, increasingly also our social needs (Andrejevic, 2012a). Especially companies such as Facebook and Google have built their profit models around targeted third party advertising (Fuchs et al., 2012), which has turned the digital enclosure (Andrejevic, 2007) into a profitable business model. The result of this is what Cohen (2008) names the valorization of surveillance. In other words, many technology companies have built services for users that generate as much data on these customers as possible, which is the product they sell to advertisers, thereby effectively capitalizing on the activity of surveillance.

In this light, the logic of equivalence in a 'we versus them' representation of reality, where the corporate sector together with the public situates themselves as opposed to government becomes fundamentally ideological. Notwithstanding the inconsistencies within discourses.

4.5 Discussion: Government

The rather ambivalent stance of government towards mass surveillance practice is reflected in the results of the content analysis (Chapter 4.2.1), as well as the results of discourse analysis.

Government is fundamentally divided along ideological lines in two groups with on the one hand staunch supporters of the current surveillance programs who mostly draw on national security discourse (see Chapter 4.3.3) for justifying why the programs are in place. On the other hand, troubled Members of U.S. Congress question the legal validity of the surveillance programs, and they worry to what extent U.S. citizens themselves are subjected to surveillance. This group has been found to mostly draw on surveillance discourse (see Chapter 4.3.4).

4.5.1 Defending the Nation

The supporters of current surveillance programs in the government sector mostly stress the importance of security – which is a key signifier in national security discourse (see Chapter 4.3.3). In particular, the security of the nation and its people against outside threats are emphasized in national security discourse. These outside threats are often envisioned under the general term 'enemies' and sometimes referred to in more specific terms such as 'terrorist'. As a result, the part of government that draws on national security discourse succeeds to create a highly simplified division among the nation (and its people, more specifically: Americans) and outside enemies, such as terrorists, and surveillance programs are instrumental to this end. To illustrate, Senator Dianne Feinstein of California suggests that the surveillance programs are instrumental, because "terrorist plots might have been foiled" (Text 3). In addition, the content analysis confirms this trend, as those with a positive stance towards mass surveillance indeed justify the programs with the argument that it has prevented terrorist attacks (see Chapter 4.2.1). As a result, the dichotomy that is artificially created among Americans and outside threats suggests the use of logic of equivalence, which results in the creation of the myth of enemy. This is a hegemonic intervention with ideological consequences, and the logic of equivalence representing Americans and 'enemies' as opposing forces may become social imaginary if the national security discourse were to become hegemonic.

4.5.2 Advocating for Americans' privacy

It may come as a surprise then, that surveillance discourse also makes a clear distinction among those with U.S. citizenship and those without, albeit articulated a different context. Indeed, while in national security discourse the prominence of the security of the nation is highlighted in relation to the American people, in surveillance discourse the prominence of

privacy is highlighted in this relation. Accordingly, privacy is an important key signifier in surveillance discourse (see Chapter 4.3.4). By contrast, the emphasis on the public in surveillance discourse – identifying them as Americans – is evidence of the presence of interdiscursivity of surveillance discourse with national security discourse. The emphasis on privacy however, is the result of interdiscursivity with activist discourse, whereby the key signifier 'privacy' is adopted by surveillance discourse.

As a result, while national security discourse advocates the security of the American public, surveillance discourse advocates the privacy of Americans – which has become problematic under current mass surveillance programs according to critics of surveillance within the U.S. government. Rather than opposition in the government sector claiming that intentional damage is inflicted to the privacy of the public, they instead consider the inability of surveillance programs to distinguish among U.S. citizens and non-U.S. citizens as an inevitable consequence of today's global communication structures. To illustrate, U.S.Senator of Oregon Ron Wyden, who has been a longtime critic of intrusive surveillance activities, argues that "Today there's a global communications infrastructure, so there's a greater risk of collecting on Americans when the NSA collects overseas." (Text 4).

4.5.3 Intelligence vs. surveillance

Another stark difference between the two discourses used in government, is how the mass surveillance programs themselves are referred to discursively. To specify, while the mass surveillance programs are articulated to a different set of key signifiers and in a different structure in each discourse – less subtly so each discourse names the key signifier of mass surveillance activity different. Indeed, while surveillance discourse refers to 'surveillance', national security discourse refers to 'intelligence' (see Chapter 4.3.3 and Chapter 4.3.4). To illustrate, while surveillance discourse refers to surveillance activities, the NSA drawing on national security discourse in this instance, claims that the programs are "focused on discovering and developing intelligence about valid foreign intelligence targets only" (Text 4). Arguably, this different naming of the same activity of mass data collection highlights the discursive struggle between both discourses to have the way the contested signifier is fixed in each discourse achieve hegemony. As a result, the articulation of surveillance in surveillance discourse – constructing its meaning in relation to privacy, and the articulation of intelligence in national security discourse constructing its meaning in relation to security, can be seen as fundamentally ideological. However, the fact that both discourses struggle so fiercely within

in the same domain of government suggests that none of the two has succeeded in hegemonic intervention. Instead, both discourses are engaged in a discursive struggle within the order of discourse.

4.5.4 Classified information

Another important difference between surveillance discourse and national security discourse is the way in which information, collected through mass surveillance, that is hidden from the public eye is being treated by each respective discourse. Also here, the different articulation of the phenomenon in each discourse is highlighted by a different naming of it. Indeed, while national security discourse refers to information that is hidden from the public eye as classified, surveillance discourse refers to it as secrecy (see Chapter 4.3.3 and Chapter 4.3.4).

In addition, both classified and secrecy are articulated differently in each respective discourse by their different positioning in relation to other key signifiers. Indeed, the classified status in national security discourse is descriptive for the role of covert intelligence in ensuring the security of the nation (see Chapter 4.3.3). This is illustrated by the statement from U.S. Senator McConnell from Kentucky addressing the disclosure of classified documents with help of whistleblower Edward Snowden: "What's difficult to understand is the motivation of somebody who intentionally would seek to the nation's enemies of lawful programs created to protect the American people." (Text 3).

By contrast, surveillance discourse articulates secrecy of collected information as contributing to the violation of Americans' privacy, and in particular, to the lack over oversight of mass surveillance programs. In relation to this, accountability is a key signifier in surveillance discourse (see Chapter 4.3.4), which fundamentally relies on the extent to which mass surveillance is subjected to oversight. An illustration of the role of accountability in surveillance discourse is the instance where U.S. Senator of Oregon Ron Wyden addresses the perceived lack of governmental oversight over mass surveillance practices used by government. Wyden: "The American people have the right to expect straight answers from the intelligence leadership to the questions asked by their representatives." (Text 3). Furthermore, this citation illustrates the ambivalent position of government itself in surveillance discourse. While government is positioned as a myth (see Chapter 4.3.4) in surveillance discourse, it is at the same time dissolved through logic of difference. Indeed, while one part of government (citizen's representatives in U.S. congress) should enforce

oversight on mass surveillance programs, another part of government (intelligence agencies) should run them.

In addition, in surveillance discourse the mass surveillance programs should also be accountable to courts – more specifically to the Foreign Intelligence Surveillance Court (FISC). This highlights interdiscursivity between surveillance discourse and legal discourse, because surveillance adopts the key signifier 'judiciary' from legal discourse here. The substantial lack of accountability of mass surveillance programs to the judiciary is highlighted by U.S. Representative Brad Sherman of California then, while he states that: "We don't have the courts making sure that […] standards are always followed." (Text 3).

4.6 Discussion: Citizen groups

As expected, the stances of the citizen group sector were most prominently deduced from citizen groups' own publications and mass media publications. The charts in Chapter 4.2.1 (more specifically, Figure 4.15 and 4.16), reveal that the citizen groups are rather univocal in their negative stance towards current mass surveillance practice, and also their call for reform. Albeit the mass media publications are an exception to this, because here the citizen group representatives cited had a much more moderate justification for their negative stance: primarily an expression of concern.

Furthermore, the univocal stance of the citizen group sector regarding mass surveillance was further confirmed by its univocal use of activist discourse. In addition, the network analysis (see Chapter 4.1.1; Figure 4.3) suggests that the unified stance of the citizen group sector is reflected in its online network.

4.6.1 Transparency

Activist discourse articulates a few nodal points in roughly the same way in relation to current mass surveillance as surveillance discourse, which makes the two discourses comparable in some respects. Notable key signifiers in this regards are 'privacy', 'government', and 'accountability', although the notable differences between the two discourses are more descriptive. Indeed, while surveillance discourse emphasizes the importance of accountability of surveillance programs to U.S. citizens through governmental and judicial oversight, this point is explicitly rejected in activist discourse. To illustrate, citizen group The Electronic Frontier Foundation (EFF) states that "All too often, the NSA's official position is that

foreigners-or anybody deemed sufficiently likely to not to be a "U.S. person"-are not given any legal protections under surveillance laws. This situation is unacceptable." (Text 6).

In relation to this, citizen groups advocate a form of transparency and accountability – both are key signifiers in activist discourse (see Chapter 4.3.6), that is not confined to any state border. As opposed to surveillance discourse, which emphasizes the role of U.S. government and U.S. judiciary in the accountability process. This important distinction is most clearly illustrated in relation to the phenomenon 'whistleblower'. Indeed, arguably due to the whistleblowing of Edward Snowden the global mass surveillance practice has been made more transparent, and as a result of this more accountable to the public. Activist discourse then, takes an explicit stance towards whistleblowing by advocating the importance of additional transparency and accountability. To illustrate, EFF states that "There is little question that this debate would not have happened without the evidence brought to light by Snowden and other whistleblowers. […] If Obama welcomes this debate, he should stop his attack on the people who have risked so much to help make it happen." (Text 6).

4.6.2 Human Rights

In addition, citizen groups takes a more assertive approach towards their review of current mass surveillance programs than the government sector drawing on surveillance discourse, and as a result citizen groups actively advocate for reform of the programs. For instance, EFF has even compiled a list of "12 common sense fixes that should be a minimum for reforming NSA surveillance" (Text 6).

In general, citizen groups claim that surveillance programs should be better aligned with human rights, including privacy rights. Notably, the key signifier human rights in activist discourse (see Chapter 4.3.6) derives much of its meaning from individual rights. Spokesperson for Privacy International, Carly Nyst, addresses the problematic relationship between surveillance and individual human rights: "State surveillance severely threatens individuals' rights to privacy, free expression and free association; impedes an open and democratic society, hinders a free press; breeds conformity and undermines innovation; and strikes at the heart of human dignity and autonomy." (Text 5).

4.6.3 Technological optimism

Throughout citizen groups' criticism of mass surveillance programs, a fundamental technological optimism is noticeable, that in many ways shows striking similarities to the

myth of technology as articulated in cyberlibertarian discourse used by the corporate sector. Indeed, activist discourse used by citizen groups has through interdiscursivity adopted the myth of technology from cyberlibertarian discourse. As a result, activist discourse also presents technology as a force with a fundamentally good potential for society, that is however currently being abused by government for worse. This technological optimism of activist discourse is well illustrated by the statement from Researcher at Human Rights Watch Cynthia Wong: "Every government should ensure people can use these technologies without fear of invasive and disproportionate intrusions into their private lives." (Text 5).

Very noticeable here is the contention from citizen groups that the people's untroubled use of technology is somehow impeded by goverm
nment, without questioning the very commodified fundament of many web 2.0 technologies, government is said to abuse. It has been the public's trust in commercial companies to provide the fundamental infrastructure for much of the communication online (Andrejevic, 2012a) today, that has fueled the emergence of what has been recognized as the valorization of surveillance (Cohen, 2008). That is, that the digital enclosure integrated in many web 2.0 applications (Andrejevic, 2007) allow companies to transform data collection on a mass scale into a profitable business model (Fuchs et al., 2012).

4.7 General Discussion

Perhaps, most notable in the previous discussion of discourses among societal sectors is the complete failure to mention the corporate sector's role in the surveillance process, for it is the corporate sector that amasses and transmits the data that government is accused of tapping into on such a mass scale. Especially the fact that the citizen group sector has been found to adopt much of the corporate sector's technological optimism, and in doing so fails to address the fundamental commercial infrastructure underlying much of today's communication through internet. As a result, the fundamentally ideological positioning of the myth of government in corporate sector discourse is reinforced by citizen group discourse. The complete absence of any mention to the role of the corporate sector in current mass surveillance suggests hegemonic intervention by corporate sector discourse.

Furthermore, considering the emphasis on human rights for a global audience in citizen group discourse it is especially striking that the phenomenon of prosumer commodification (Fuchs, 2011) by the corporate sector is entirely omitted by citizen groups. As Fuchs (2011) argues, while prosumers use services of web 2.0 applications, their data is

collected and sold as a commodity. The laborers in this context are users themselves who while using the web 2.0 services also effectively produce data that companies reap the benefits from in the form of monetary profit (Fuchs, 2011). In this context, "prosumers are digitally enclosed and digitally exploited" (Fuchs, 2011, p. 299).

A prominent explanation for the widespread failure to acknowledge this new form of capitalist exploitation is the transformation of the role of work itself in society. Indeed, towards the middle of the 1970s capitalism gradually moved from the traditional 'Fordist' form of organizing work to a post-Fordist network structure characterized by more flexible labor systems and relative work autonomy. While the traditional structures of capitalism and bureaucracy were critiqued, the gradually evolved network structure triumphed while the hierarchical division of labor effectively remained the same. As a result, while traditional exploitation was extensively addressed and critiqued after the 1960s, the newly emerged neocapitalism effectively continued exploitation while going relatively uncontested (Boltanski & Chiapello, 2006). The ignoring of capitalism in citizen groups' critique of mass surveillance suggests that the neocapitalist hegemonic intervention is replicated discursively by the societal sectors in the triangle.

Notwithstanding the stark differences between surveillance discourse and national security discourse on issues of privacy or secrecy, very notably both univocally present U.S. citizenship as a privileged status that positions one's privacy or protection from mass surveillance as superior to those of non-U.S. citizens. This is a stance from the government sector that has potentially profound ideological implications. While the U.S. politicians are very prominently covered in the governmental sector, the relatively large coverage of their stances in global mass media potentially reinforces the ideological influence of their articulations of reality on public discourse.

Furthermore, while both commercial discourse as well as activist discourse include the key signifier of transparency, both articulate it fundamentally different in their respective discourses. To clarify, activist discourse advocates for more transparency, for instance with help of whistleblowers, in order to aide increased accountability to a global public. By contrast, the corporate sector hopes increased 'transparency' will reinforce customer trust in their product. More specifically, the corporate sector publishes Transparency Reports including very undetailed information about government requests for customer data. Arguably, this practice of publishing Transparency Reports has two immediate effects. First, the attention is distracted from corporate involvement in mass surveillance by reinforcing the myth of government through logic of equivalence in a 'we versus them' structure. And

secondly, the corporate sector emphasizes the impression that their minimum act of transparency helps to solve a program that they help to maintain to exist in the first place.

Furthermore, the combination of the technological optimism regarding the role of technology in society with the firm belief in neoliberalist free market forces shows rather large resemblance to the *Californian Ideology* as posited by Barbrook and Cameron (1996). Their critique on dotcom companies argues that Silicon Valley companies univocally promote an ideology which can be characterized as a combination of technological optimism and neoliberalism.

4.8 Reflexivity

As Jørgensen and Phillips (2002) argue, "in working with discourses close to oneself with which one is very familiar, it is particularly difficult to treat them as discourses" (p.21). Indeed, in the researcher role especially those common sense understandings ought to be studied, which are naturalized. This paradox ought to be resolved reflexively, which this short section is a contribution to.

First of all, while exploring surveillance discourse used by the government sector it was difficult to name the discourse because some names might be value laden themselves. For instance, it was considered to name it 'mass surveillance discourse' specifically because it articulates surveillance in a problematic relation to privacy and oversight. However, the decision was made to instead adopt the more 'neutral' term of surveillance discourse.

Furthermore, the naming of commercial discourse was a deliberate choice, within the context of the researchers 'knowledge'. For instance, in the scientific community of discourse analysts the term neoliberalism may be more common.

Chapter 5: Conclusions

This chapter presents the conclusions drawn from the analysis presented in the previous chapter. Alongside a summarizing of the key findings of this study, the sub-research questions, and main research question are being answered. Furthermore, the theoretical and practical implications of the conclusions presented in this chapter are presented. Finally, acknowledgments are made regarding certain limitations of the project, and suggestions for future research will be given.

5.1 Conclusions

This study features a comprehensive design, both conceptually as well as methodological, in order to uncover surveillance discourses in different sectors throughout society after the groundbreaking disclosures on global mass surveillance. These disclosures were fundamentally aided by the whistleblowing activities of Edward Snowden. Through a triangular conceptual design, this study investigated the discourses used by the corporate sector, government, and citizen groups. The study features a mixed methods design including network analysis, content analysis, and in-depth discourse analysis. While moving forward through the research process from network analysis towards discourse analysis, the data collected enhanced an increasingly depth of understanding about the discourses used by the respective triangular sectors. This data was collected from three sources: corporate sector publications, mass media publications, and citizen group publications.

As a result, the surveillance scandal was the most popular online during five key moments in time, as identified from the Google Trends analysis, which monitors online interest in the scandal. These key moments in time were the weeks of June 9, 2013 until June 15, 2013; September 8, 2013 until September 14, 2013; October 27, 2013 until November 2, 2013; December 15, 2013 until December 21, 2013; and January 12, 2014 until January 18, 2014 . This answers the second sub-research question (sub-RQ 2). As a result, the network analysis reveals that citizen groups publications primarily draw on a large, densely connected network of citizen groups. By contrast, the key sources in the network mass media publications primarily draw on are news agencies Reuters and The New York Times, and the corporate sector publications primarily draw on a densely connected network of governmental websites. This answers the first sub-research question (sub-RQ 1).

The latter conclusion – that the corporate sector publications draw primarily on the government, is contradicted by content analysis however. Indeed, while the corporate sector situates itself primarily negative towards mass surveillance practice, the government takes a fundamental ambivalent stance towards it, with one part of government in favor of mass surveillance programs, and another part opposing current mass surveillance. Similar to the corporate sector, the citizen groups are fundamentally critical of mass surveillance programs, and very assertively advocate for reforms. Hereby, the third sub-research question (sub-RQ 3) has been answered.

In addition, the corporate sector takes a deeply negative stance towards mass surveillance, arguing that it has negatively influenced customer trust. While on one hand, the corporate sector argues that being occasionally required to hand over customer data is a necessary evil to prevent for example terrorist attacks, on the other hand the corporate sector strongly condemns mass surveillance because it impedes free use of technology. As a result, intensified encryption and more transparency in the form of Transparency Reports are presented as primary solutions. Furthermore, the corporate sector primarily draws on commercial discourse and cyberlibertarian discourse. Consequently, sub-research question four (sub-RQ 4) has been answered.

The government sector is fundamentally divided in terms of its stance towards mass surveillance. While staunch defenders of mass surveillance argue that surveillance of foreign targets is an absolute requirement in order to ensure the security of the country, the opposition claims that surveillance has become too invasive for Americans and that in the age of global communication through the internet intelligence agencies cannot guarantee to not collect data on Americans. By contrast, one thing both defenders and opposition in the government agree upon, is that in contrast to mass surveillance of foreign targets, the privacy of Americans should be privileged and safeguarded. In addition, the defenders of surveillance draw primarily on national security discourse, and the opposition most prominently uses surveillance discourse. Hereby, sub-research question five (sub-RQ 5) has been answered.

In addition, citizen groups univocally advocate for reform of state surveillance. While they emphasize the importance of global human rights, the act of whistleblowing is applauded for its fundamental contributions to transparency and accountability of mass surveillance. Many citizen groups assertively suggest improvements to current mass surveillance practice, in order to better align the programs with privacy and other human rights. The citizen groups univocally draw on activist discourse. This answers sub-research question six (sub-RQ 6).

Most notably, the three triangular sectors univocally omit the role of web 2.0 commodification in current mass surveillance. Indeed, while the corporate sector presents the government as the party to blame for mass surveillance, citizen groups in fact reinforce this position by a failure to address the corporate sector involvement in mass surveillance. More specifically, the failure to acknowledge the fundamental consequences of the trust citizens have in the corporate sector for providing the infrastructure citizens use for their communicative, informational, and social needs leads to omission of the central issue of valorization of surveillance. Instead, the corporate sector presents solutions such as increased encryption, or occasional Transparency Reports; a part of the government sector argues for more oversight; and citizen groups advocate for more transparency and accountability. As a result, all of the parties fail to address the fundamental issue of data commodification. Hereby, the main research question (RQ) has been answered.

5.2 Theoretical Implications

Due to the relatively recent public availability of new information made possible with help of Edward Snowden, this study addresses a time range that likely has not been fully addressed during the short amount of time since the disclosures. Hence, the vital opportunity to contribute to knowledge. Most notably, the comprehensiveness of the conceptual design, and the mixed methods are innovative and contribute to the body of empirical studies available on the topic.

In addition, the different identified discourses, as well as the ways discursive struggles emerge, and on the other hand discourses draw on each other through interdiscusivity may confirm or contrast with currently existing studies. The contrasting of the presentation of mass surveillance among the three sectors in the innovative triangle design is the most vital contribution to surveillance studies though.

5.3 Practical Implications

Considering the central premise of discourse constituting the way one perceives reality, the importance of awareness about discourse and its influence on public opinion can hardly be overstated. Once discourse has become naturalized, it is indistinguishable from reality, because discourse in this position constitutes they way one perceives reality. As a result, discourse may go uncontested and unchallenged, and may in fact be considered knowledge.

Providing insight into the way different competing 'realities' are constructed in the current surveillance debate is paramount to having an informed debate about potential consequences and solutions. In addition, insight into contested signifiers and hegemonic interventions may encourage supporters of discourses currently situated in the order of discourse due to strong hegemonic interventions by competing discourses, to approach communication more strategically. As a result, this study may contribute the empowerment of groups currently finding themselves in an oppressed position in the debate.

5.4 Limitations

First, in absence of a sampling frame it proved beyond possibilities of this project to use probability sampling techniques in the content analysis part of the study in order to produce statistical significant results that in a strict sense may be generalized to a larger population. Instead, this study attempts to make up for this by using a mixed methods design, and in addition by meticulously addressing how and why the choices were made in the mostly purposive sampling strategy.

Furthermore, even though the choices made for starting points in the digital research methods part of the study – and the selection texts in the content analysis-and discourse analysis part afterwards were carefully justified with arguments, the sample of texts used for content analysis and discourse analysis in the end exclusively included U.S.-based and U.K.-based news outlets and companies as a source. The consequences of this are thought to be rather limited however, because the vast majority of texts from news outlets and companies were international in scope, and texts from news outlets were in many cases published in the 'international news' section of the website.

5.5 Future Research

As Laclau & Mouffe argue, discourses are in constant flux and never completely stabilize (Jørgensen & Phillips, 2002), it would be fruitful to perform a longitudinal study and research the potential evolution of surveillance discourse over time. As a result of this, one could potentially point out how and where discourses are contingent, and thus change over time.

In addition, one could perform a study where surveillance discourse prior to as well as after the first leaking by Edward Snowden are observed. As a result, it potentially would give insight into how reality is constructed in discourse before and after the disclosures made with help of whistleblower Snowden.

Furthermore, a cross-country comparison could add to present knowledge by comparing the surveillance discourse presented by different media outlets from different geographical regions around the world. Perhaps, comparing countries with different dominant political ideologies could add insight. Also, comparing surveillance discourse in private sectors, governments, and citizen groups from different regions around the globe could add insight.

References

Akerlof, G. (1970). The market for lemons: Quality uncertainty and the market mechanism. *Quaterly Journal of Economics*, *84*(3), 488-500.

Andrejevic, M. (2007). *iSpy: Surveillance and power in the interactive era*. Lawrence, KS: University Press of Kansas.

Andrejevic, M. (2012a). Exploitation in the Data Mine. In C. Fuchs, K. Boersma, A. Albrechtslund & M. Sandoval (Ed.), *Internet and Surveillance: The Challenges of Web 2.0 and Social Media* (pp. 71-88). NYC, NY: Routledge.

Andrejevic, M. (2012b). Ubiquitous surveillance. In K. Ball, K. Haggerty & D. Lyon (Ed.), *Routledge Handbook of Surveillance Studies* (pp. 91-98). UK: Routledge.

Arutunyan, A. & Stanglin, D. (2013, Jul. 24). Snowden remains stuck at Moscow airport. *USA Today*. Retrieved from http://www.usatoday.com.

Associated Press. (2014, Apr. 14). Washington Post, Guardian win Pulitzers for NSA revelations. *Washington Examiner*. Retrieved from http://www.washingtonexaminer.com.

Babbie, E. (2007). *The Basics of Social Research* (4th ed.). Belmont: Thomson Wadsworth.

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

Ball, J. (2014, Jan. 16). NSA collects millions of text messages daily in 'untargeted' global sweep. *The Guardian*. Retrieved from http://www.theguardian.com.

Barbrook, R. & Cameron, A. (1996). The Californian ideology. *Science as Culture*: *6*(1), 44-72.

Beniger, J. (1986). *Control Revolution: Technological and Economic Origins of the Information Society*. London, UK: Harvard University Press.

Benkler, Y., Roberts, H., Faris, R., Solow-Niederman, A. & Etling, B. (2013). Social mobilization and the networked public sphere: Mapping the SOPA-PIPA debate (Research Publication No. 2013-16). Retrieved from The Berkman Centre for Internet & Society website: http://cyber.law.harvard.edu/publications/2013/social_mobilization_and_the_networked_public_sphere.

Benkler, Y. (2006). *The wealth of networks.* New Haven, CT: Yale University Press.

Bennett, C.J. (2012). Privacy advocates, privacy advocacy and the surveillance society. In K. Ball, K. Haggerty & D. Lyon (Ed.), *Routledge Handbook of Surveillance Studies* (pp. 412-419). UK: Routledge.

Berry, D.M. (2012). Introduction: Understanding the digital humanities. In D.M. Berry (Ed.), *Understanding Digital Humanities* (pp. 1-20). NYC, NY: Palgrave Macmillan.

Bogard, W. (2012). Simulation and post-panopticism. In K. Ball, K. Haggerty & D. Lyon (Ed.), *Routledge Handbook of Surveillance Studies* (pp. 30-37). UK: Routledge.

Boltanski, L. & Chiapello, E. (2006). *The New Spirit of Capitalism*. London, UK: Verso.

Borger, J. (2013, Nov. 1). GCHQ and European spy agencies worked together on mass surveillance. *The Guardian*. Retrieved from http://www.theguardian.com.

Burr, V. (1995). *An Introduction to Social Constructionism.* London, UK: Sage.

Castells, M. (1996). *The Rise of The Network Society, The Information Age: Economy, Society and Culture Vol. 1* (1st ed.). Oxford, UK: Blackwell.

Ceyhan, A. (2012). Surveillance as biopower. In K. Ball, K. Haggerty & D. Lyon (Ed.), *Routledge Handbook of Surveillance Studies* (pp. 38-45). UK: Routledge.

Chumley, C.K. (2014, Jan. 24). Russia extends asylum for Edward Snowden. *The Washington Times*. Retrieved from http://www.washingtontimes.com.

Clarke, R. (1994). Dataveillance: delivering '1984'. In L. Green & R. Guinery (Ed.), *Framing technology: Society, choice and change* (pp. 117-130). Sydney, NSW: Allen & Unwin.

Cohen, N.S. (2008). The valorization of surveillance: Towards a political economy of Facebook. *Democratic Communiqué*, *22*(1), 5-22.

Cox, J. (2012). *Canada and the Five Eyes intelligence community* (December 2012). Retrieved from the Canadian Defence & Foreign Affairs Institute (CDFAI) website: http://www.cdfai.org/PDF/Canada%20and%20the%20Five%20Eyes%20Intelligence%20Community.pdf.

Deleuze, G. (1988). *Foucault*. Minneapolis, MN: University of Minnesota Press.

Deleuze, G. (1992). Postscript on the societies of control. *October*, *59*, 3-7.
Deuze, M. (2007). *Media Work*. Cambridge, UK: Polity.

Denzin, N.K. (1978). *The Research Act: A Theoretical Introduction to Sociological Methods*. New York City, NY: McGraw-Hill.

Dinev, T., Hart, P. & Mullen, M.R. (2008). Internet privacy concerns and beliefs about government surveillance. *Journal of Strategic Information Systems*, *17*, 214-233.

DmiAbout. (2014). Retrieved from https://wiki.digitalmethods.net/Dmi/DmiAbout.

DW. (2014, Mar. 29). Spiegel report: NSA spied on 122 world leaders, kept 300 files on Merkel. *DW*. Retrieved from http://www.dw.de.

Elmer, G. (2012). Panopicon-discipline-control. In K. Ball, K. Haggerty & D. Lyon (Ed.), *Routledge Handbook of Surveillance Studies* (pp. 21-29). UK: Routledge.

Esposito, R., Cole, M., Schone, M. & Greenwald, G. (2014, Jan. 27). Snowden docs reveal British spies snooped on YouTube and Facebook. *NBC News*. Retrieved from http://www.nbcnews.com.

Fairclough, N. (1989). *Language and Power*. London, UK: Longman.

Finn, P. & Horwitz, S. (2013, Jun. 21). U.S. charges Snowden with espionage. *The Washington Post*. Retrieved from http://www.washingtonpost.com.

Fleiss, J.L. (1981). *Statistical Methods for rates and proportions* (2nd ed.). Hoboken, NJ: Wiley.

Foucault, M. (1977). *Discipline and Punish: The Birth of the Prison* (1st ed.). NYC, NY: Doubleday.

Fuchs, C. (2011). Web 2.0, Prosumption, and Surveillance. *Surveillance & Society, 8*(3), 288-309.

Fuchs, C., Boersma, K., Albrechtslund, A. & Sandoval, M. (2012). Introduction: Internet and Surveillance. In C. Fuchs, K. Boersma, A. Albrechtslund & M. Sandoval (Ed.), *Internet and Surveillance: The Challenges of Web 2.0 and Social Media* (pp. 1-28). NYC, NY: Routledge.

Gellman, B., Blake, A. & Miller, G. (2013, Jun. 9). Edward Snowden comes forward as source of NSA leaks. *The Washington Post*. Retrieved from http://www.washingtonpost.com.

Gellman, B. & Soltani, A. (2013a, Oct. 30). NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. *The Washington Post*. Retrieved from http://www.washingtonpost.com.

Gellman, B. & Soltani, A. (2013b, Dec. 4). NSA tracking cellphone locations worldwide, Snowden documents show. *The Washington Post*. Retrieved from http://www.washingtonpost.com.

Giddens, A. (1990). *The Consequences of Modernity*. Cambridge, UK: Polity.

GOVCOM.ORG. (n.d.). Retrieved from http://www.govcom.org/Issuecrawler_instructions.htm.

Greenwald, G. (2013a, Jun. 6). NSA collecting phone records of millions of Verizon customers daily. *The Guardian*. Retrieved from http://www.theguardian.com.

Greenwald, G. (2013b, Jul. 31). XKeyscore: NSA tool collects 'nearly everything a user does on the internet'. *The Guardian*. Retrieved from http://www.theguardian.com.

Greenwald, G. & MacAskill, E. (2013a, Jun. 7). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Retrieved from http://www.theguardian.com.

Greenwald, G. & MacAskill, E. (2013b, Jun. 11). Boundless Informant: The NSA's secret tool to track global surveillance data. *The Guardian*. Retrieved from http://www.theguardian.com.

Greenwald, G., MacAskill, E. & Poitras, L. (2013, Jun. 10). Edward Snowden: The whistleblower behind the NSA surveillance revelations. *The Guardian*. Retrieved from http://www.theguardian.com.

Haggerty, K.D. & Ericson, R.V. (2000). The surveillance assemblage. *British Journal of Sociology, 51*(4), 605-622.

Introduction to Social Network Methods. (n.d.). Retrieved from http://faculty.ucr.edu/~hanneman/nettext/C1_Social_Network_Data.html.

Jick, T.D. (1979). Mixing qualitative and quantitative methods: Triangulation in action. *Administrative Science Quarterly, 24*(4), 602-611.

Johnson, R.B., Onwuegbuzie, A.J. & Turner, L.A. (2007). Toward a definition of mixed methods research. *Journal of Mixed Methods Research, 1*(2), 112-133.

Jørgensen, M. & Phillips, L. (2002). *Discourse Analysis as Theory and Method* (1st ed.). Thousand Oaks, CA: Sage.

Kammerer, D. (2012). Surveillance in literature, film and television. In K. Ball, K. Haggerty & D. Lyon (Ed.), *Routledge Handbook of Surveillance Studies* (pp. 99-106). UK: Routledge.

Laclau, E. & Mouffe, C. (1985). *Hegemony and Socialist Strategy. Towards a Radical Democratic Politics*. London, UK: Verso.

Lyon, D. (1994). *The electronic eye: The rise of surveillance society*. Cambridge, UK: Polity.

MacAskill, E., Borger, J., Hopkins, N., Davies, N. & Ball, J. (2013, Jun. 21). GCHQ taps fibre-optic cables for secret access to the world's communications. *The Guardian*. Retrieved from http://www.theguardian.com.

Mann, S., Nolan, J. & Wellman, B. (2003). "Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance and Society*, *1*(3), 331-355.

Marx, G.T. (2012). Preface: "Your papers please": Personal and professional encounters with surveillance. In K. Ball, K. Haggerty & D. Lyon (Ed.), *Routledge Handbook of Surveillance Studies* (pp. xx-xxxi). UK: Routledge.

McGrath, J. (2012). Performing surveillance. In K. Ball, K. Haggerty & D. Lyon (Ed.), *Routledge Handbook of Surveillance Studies* (pp. 83-90). UK: Routledge.

Morse, J.M. (1991). Approaches to qualitative-quantitative methodological triangulation. *Nursing Research*, *40*(2), 120-123.

NSA Prism program slides. (2013). Retrieved from http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document.

NSA Secrets. (2014). Retrieved from http://www.washingtonpost.com/nsa-secrets/.

Perlroth, N. & Goel, V. (2014, Feb. 27). British spies said to intercept Yahoo webcam images. *The New York Times*. Retrieved from http://www.nytimes.com.

Poitras, L., Rosenbach, M. & Stark, H. (2014, Mar. 29). 'A' for Angela: GCHQ and NSA targeted private German companies and Merkel. *Spiegel Online*. Retrieved from http://www.spiegel.de.

Privacy Advocates List. (n.d.). Retrieved from http://www.privacyadvocates.ca/privacy-advocates/list.

Report on Government Information Requests. (2013). Retrieved from http://images.apple.com/pr/pdf/131105reportongovinforequests3.pdf.

Reuters. (2013a, Jun. 23). U.S. revokes Snowden's passport: official source. *Reuters*. Retrieved from http://www.reuters.com.

Reuters. (2013b, Aug. 26). Snowden got stuck in Russia after Cuba blocked entry: newspaper. *Reuters*. Retrieved from http://www.reuters.com.

Rogers, R. (2013). *Digital Methods*. Boston, MA: MIT Press.

Rule, J.B. (2012). "Needs" for surveillance and the movement to protect privacy. In K. Ball, K. Haggerty & D. Lyon (Ed.), *Routledge Handbook of Surveillance Studies* (pp. 64-71). UK: Routledge.

Sechrest, L. & Sidana, S. (1995). Quantitative and qualitative methods: Is there an alternative? *Evaluation and Program Planning*, *18*(1), 77-87.

Sirkin, R.M. (2006). *Statistics for the Social Sciences* (3rd ed.). Thousand Oaks, CA: Sage Publications.

Tapscott, D. & Williams, A.D. (2006). *Wikinomics: How mass collaboration changes everything.* London, UK: Penguin.

The NSA files. (2013). Retrieved from http://www.theguardian.com/world/the-nsa-files.

Trottier, D. & Lyon, D. (2012). Key Features of Social Media Surveillance. In C. Fuchs, K. Boersma, A. Albrechtslund & M. Sandoval (Ed.), *Internet and Surveillance: The Challenges of Web 2.0 and Social Media* (pp. 89-105). NYC, NY: Routledge.

Wall, D.S. (2006). Surveillant Internet technologies and the growth in information capitalism: spams and public trust in the information society. In K. Haggerty & R. Ericson (Ed.), *Surveillance and visibility* (pp. 340-362). Canada: University of Toronto Press.

Wasserman, S. & Faust, K. (1994). Social Network Analysis in the Social and Behavioral Sciences. In S. Wasserman & K. Faust (Ed.), *Social Network Analysis: Methods and Applications* (pp. 1-27). Cambridge, UK: Cambridge University Press.

Weller, T. (2012). The information state: An historical perspective on surveillance. In K. Ball, K. Haggerty & D. Lyon (Ed.), *Routledge Handbook of Surveillance Studies* (pp. 57-63). UK: Routledge.

Appendices

Appendix A: Corporate Sector Codebook

Text Descriptives

- Assigned number
- Title
- Date of publication
- Author(s)
- Word count
- Coder (in case of intercoder reliability)

Variables

(1) Function of author (more options)

1) Board/Executive position
2) Law position
3) Communications or public relations position
4) Technical position
5) Not identifiable
6) More than one author
7) Other

(2) Publication

1) Press release
2) Corporate blog post
3) Other

(3) Purpose of press release

1) Reactive
2) Proactive
3) Other

(4) Main issue of the text

_____

(5) Stance regarding current mass surveillance practice

1) Mostly positive
2) Neutral
3) Mostly negative
4) Not Present
5) Other

(6) Supporting argumentation regarding stance

_____

(7) Stance regarding more data collection transparency in the privacy sector

1) Mostly positive
2) Neutral
3) Mostly negative
4) Not present
5) Other

(8) Supporting argumentation regarding stance

_____

(9) Company/organization indicates to cherish and respect privacy

1) Present
2) Absent

(10) How the role of mass surveillance in relation to national security is articulated, if mentioned

_____

(11) Actors named in the coverage

_____

(12) How they are referred to

_____

(13) Mentioning of data collection by the corporate sector

1) Yes
2) No

(14) Mentioning of data monetization by the corporate sector

1) Yes
2) No

(15) Justification for companies'/organization's own use of user data for marketing purposes

1) Yes
2) No

Appendix B: Mass Media Codebook

Text Descriptives

- Assigned number
- Title
- Date of publication
- Author(s)
- Word count
- Coder (in case of intercoder reliability)

Variables

(1) Scope of coverage

1) Domestic
2) International
3) Other

(2) Main issue of the text

_____

(3) Government and/or institutions official(s) cited

_____

(4) Stance regarding current mass surveillance practice (for each government official cited)

1) Mostly positive
2) Neutral
3) Mostly negative
4) Not present
5) Other

(5) Supporting argumentation regarding stance

_____

(6) Corporate sector and/or company representative(s) cited

_____

(7) Stance regarding current mass surveillance practice (for each corporate sector representative cited)

1) Mostly positive
2) Neutral
3) Mostly negative
4) Not present
5) Other

(8) Supporting argumentation regarding stance

_____

(9) Citizen Groups representative(s) cited

_____

(10) Stance regarding current mass surveillance practice (for each citizen group representative cited)

1) Mostly positive
2) Neutral
3) Mostly negative
4) Not present
5) Other

(11) Supporting argumentation regarding stance

_____

(12) Whistleblower cited

_____

(13) Stance regarding current mass surveillance practice (for each whistleblower cited)

1) Mostly positive
2) Neutral
3) Mostly negative
4) Not present
5) Other

(14) Supporting argumentation regarding stance

_____

(15) Mentioning of data collection by corporate sector

1) Yes
2) No

(16) Mentioning of data monetization by corporate sector

1) Yes
2) No

(17) Actors named in the coverage

_____

(18) How they are referred to

_____

(19) Article includes stance criticizing (more options)

1) Government
2) Whistleblower Snowden
3) Commercial companies
4) Users/citizens
5) Other

(20) Framing Edward Snowden (word[s] associated to him)

_____

Appendix C: Citizen Groups Codebook

Text Descriptives

- Assigned number
- Title
- Date of publication
- Author(s)
- Word count
- Coder (in case of intercoder reliability)

Variables

(1) Publication form

1) Press release
2) Corporate blog post
3) Other

(2) Main issue of the text

_____

(3) Stance regarding current mass surveillance practice

1) Mostly positive
2) Neutral
3) Mostly negative
4) Not present
5) Other

(4) Supporting argumentation regarding stance

_____

(5) Actors named in the coverage

_____

(6) How they are referred to

_____

(7) Privacy invasion addressed as a problem

_____

(8) Other citizen groups named in the coverage

_____

(9) Their stances regarding mass surveillance

_____

(10) Laws or acts mentioned

_____

(11) Stance regarding the law or act

_____

(12) Mentioning of data collection by corporate sector

1) Yes
2) No

(13) Mentioning of data monetization by corporate sector

1) Yes
2) No

Appendix D: Content Analysis Texts

1 = Corporate publications

2 = Mass media publications

3 = Citizen group publications

	Source	Date	Title
1	Apple	Jun. 16, 2013	Apple's Commitment to Customer Privacy
1	Apple	Nov. 5, 2013	Report on Government Information Requests
1	Apple	Jan. 27, 2014	Update on National Security and Law Enforcement Orders
1	Facebook	Jun. 8, 2013	Personal Response From Mark Zuckerberg About PRISM
1	Facebook	Jun. 14, 2013	Facebook Releases Data, Including All National Security Requests
1	Facebook	Sept. 9, 2013	Facebook Joins Industry in Petitioning Foreign Intelligence Surveillance Court
1	Facebook	Feb. 3, 2014	Facebook Releases New Data About National Security Requests
1	Google	Jun. 7, 2013	What the …?
1	Google	Jun. 11, 2013	Asking the U.S. government to allow Google to publish more national security request data
1	Google	Sept. 9, 2013	A petition for greater transparency
1	Google	Nov. 14, 2013	Government requests for user information double over three years
1	Microsoft	Sept. 9, 2013	Microsoft amends petition to US Foreign Intelligence Service Court
1	Microsoft	Dec. 4, 2013	Protecting customer data from government snooping
1	Microsoft	Dec. 8, 2013	Reforming government surveillance
1	Microsoft	Feb. 25, 2014	Conundrums in cyberspace – exploiting security in the name of, well, security
1	Yahoo!	Nov. 18, 2013	Our Commitment to Protecting Your Information
1	Yahoo!	Feb. 3, 2014	More Transparency For U.S. National Security Requests
1	Yahoo!	Mar. 27, 2014	Users First: Sharing Our Transparency Report
1	Verizon	Dec. 19, 2013	Verizon to Publish Transparency Report Disclosing Law Enforcement Requests for Customer Information
1	Verizon	Jan. 22, 2014	Verizon Releases Transparency Report
2	The Guardian	Jun. 9, 2013	Edward Snowden: the whistleblower behind the NSA revelations
2	The Guardian	Sept. 12, 2013	Zuckerberg: US government 'blew it' on NSA surveillance
2	The Guardian	Nov. 1, 2013	NSA surveillance may cause breakup of internet, warn experts
2	The Guardian	Dec. 16, 2013	Edward Snowden says judge's ruling vindicates NSA surveillance disclosures
2	The Guardian	Jan. 17, 2014	NSA surveillance: privacy board denies being sidelined by Obama

2	The New York Times	Jun. 11, 2013	Earlier Denials Put Intelligence Chief in Awkward Position
2	The New York Times	Sept. 13, 2013	Judge Urges U.S. to Consider Releasing N.S.A. Data on Calls
2	The New York Times	Oct. 29, 2013	N.S.A. Head Says European Data Was Collected by Allies
2	The New York Times	Dec. 18, 2013	Obama Is Urged to Sharply Curb N.S.A. Data Mining
2	The New York Times	Jan. 14, 2014	N.S.A. Devises Radio Pathway Into Computers
2	Reuters	Jun. 12, 2013	NSA director says surveillance helped stop 'dozens' of attacks
2	Reuters	Sept. 9, 2013	NSA spying on Petrobras, if proven, is industrial espionage
2	Reuters	Oct. 28, 2013	Senate intelligence panel chair pledges 'major review' of NSA surveillance
2	Reuters	Dec. 16, 2013	U.S. judge rules phone surveillance program is likely unlawful
2	Reuters	Jan. 17, 2014	Obama bans spying on leader of U.S. allies, scales back NSA program
2	The Washington Post	Jun. 11, 2013	ACLU sues over NSA surveillance program
2	The Washington Post	Sept. 10, 2013	Declassified court documents highlight NSA violations in data collection for surveillance
2	The Washington Post	Oct. 30, 2013	NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say
2	The Washington Post	Dec. 17, 2013	Snowden claims NSA surveillance 'collapsing'
2	The Washington Post	Jan. 12, 2014	NSA phone record collection does little to prevent terrorist attacks, group says
3	EDRi	Jun. 19, 2013	EDRi letter to the US Embassy on PRISM
3	Consumers International	Jun. 22, 2013	PRISM surveillance: Unpicking the myths and identifying the threats
3	StopWatching.Us	Sept. 18, 2013	Announcing the rally against mass surveillance
3	Privacy International	Sept. 21, 2013	Governments break silence on surveillance as activists launch human rights principles
3	ACLU	Oct. 28, 2013	Is the Security State Mainly Looking Out For Us, Or For Itself? Two Paradigms Compared
3	Big Brother Watch	Nov. 7, 2013	Time for Surveillance Transparency
3	CDT	Dec. 17, 2013	NSA Bulk Collection Loses Its Legal Footing
3	freepress	Dec. 19, 2013	United We Stand --- and encrypt
3	Electronic Frontier Foundation	Jan. 17, 2014	Rating Obama's NSA Reform Plan: EFF Scorecard Explained
3	The Day We Fight Back	Feb. 6, 2014	Host an Event in Your Local Community on February 11, 2014 as Part of The Day We Fight Back

Appendix E - J: Exemplary Texts

Appendix E: Exemplary Text 1

Facebook Releases Data, Including All National Security Requests

Over the last week, in press statements as well as Mark's post last Friday, we've repeatedly called for governments worldwide to be willing to provide more details about programs aimed at keeping the public safe. We've also urged them to allow companies to divulge appropriate information about government orders and requests that we receive, in a manner that does not compromise legitimate security concerns.

Requests from law enforcement entities investigating national security-related cases are by their nature classified and highly sensitive, and the law traditionally has placed significant constraints on the ability of companies like Facebook to even confirm or acknowledge receipt of these requests – let alone provide details of our responses.

We've reiterated in recent days that we scrutinize every government data request that we receive – whether from state, local, federal, or foreign governments. We've also made clear that we aggressively protect our users' data when confronted with such requests: we frequently reject such requests outright, or require the government to substantially scale down its requests, or simply give the government much less data than it has requested. And we respond only as required by law.

But particularly in light of continued confusion and inaccurate reporting related to this issue, we've advocated for the ability to say even more.

Since this story was first reported, we've been in discussions with U.S. national security authorities urging them to allow more transparency and flexibility around national security-related orders we are required to comply with. We're pleased that as a result of our discussions, we can now include in a transparency report all U.S. national security-related requests (including FISA as well as National Security Letters) – which until now no company has been permitted to do. As of today, the government will only authorize us to communicate about these numbers in aggregate, and as a range. This is progress, but we're continuing to push for even more transparency, so that our users around the world can understand how infrequently we are asked to provide user data on national security grounds.

For the six months ending December 31, 2012, the total number of user-data requests Facebook received from any and all government entities in the U.S. (including local, state, and federal, and including criminal and national security-related requests) – was between 9,000 and 10,000. These requests run the gamut – from things like a local sheriff trying to find a missing child, to a federal marshal tracking a fugitive, to a police department investigating an assault, to a national security official investigating a terrorist threat. The total number of Facebook user accounts for which data was requested pursuant to the entirety of those 9-10 thousand requests was between 18,000 and 19,000 accounts.

With more than 1.1 billion monthly active users worldwide, this means that a tiny fraction of one percent of our user accounts were the subject of any kind of U.S. state, local, or federal U.S. government request (including criminal and national security-related requests) in the past six months. We hope this helps put into perspective the numbers involved, and lays to rest some of the hyperbolic and false assertions in some recent press accounts about the frequency and scope of the data requests that we receive.

We will continue to be vigilant in protecting our users' data from unwarranted government requests, and we will continue to push all governments to be as transparent as possible.

Appendix F: Exemplary Text 2

Conundrums in cyberspace — exploiting security in the name of, well, security

At Microsoft, establishing and sustaining trust with our customers is essential. If our customers can't rely on us to protect their data—whether from crooks, mismanagement or excessive government intrusion—they will look elsewhere for a technology provider.

Government access to data is a hot topic. But it's not new. In fact, our General Counsel, Brad Smith, has addressed the issue in a series of blog posts covering, among other topics, our efforts to protect customers and our support for reforming government surveillance.

On Tuesday at the RSA Security Conference in San Francisco, I gave a speech on the changing cybersecurity landscape and the respective roles of governments, users and the IT industry. I'd like to share some of my thoughts here.

When I think about how governments relate to the Internet, it's in the following four ways:

Users: Governments use the Internet extensively. They use it to communicate and store sensitive information, and as a result, they have a vested interest in Internet privacy and security.

Protectors: Governments protect the rights of Internet users -- protecting the security and privacy of their populations -- and the Internet itself.

Exploiters: Military espionage and other surreptitious activity reminds us that governments often have other interests that conflict with their role as protectors. These overlapping and conflicting roles have given rise to the thorny issue that underpins much of the current dialogue on cybersecurity: How should governments act when they have competing objectives?

Investigators: Governments may seek access to their citizens' digital data, or data in other countries. This raises questions about the rules covering such access.

Cross-border questions add an additional layer of complexity. Governments investigating local citizens for committing a local crime against local people sometimes find that the evidence is in another country. In these circumstances, the question becomes - how can the legitimate law enforcement needs of countries be met, while also protecting the privacy of Internet users and respecting the laws of the country where the data is stored.

The ongoing surveillance disclosures have brought these issues into stark relief and provided stimuli for a robust debate. The situation is full of conundrums with no clear resolution. Consider these perspectives:

Governments want to both secure the Internet and exploit it.

Users want to embrace the cloud, preserve their privacy, and be protected from criminal activity, including terrorism.

Industry wants to protect the security and privacy of users, and support efforts to protect public safety and national security.

So where do we go from here? Everyone has a part to play, including governments, users and industry.

Governments need to conduct serious conversations about norms for acceptable action in cyberspace. Governments should enact reforms to ensure that all surveillance is narrowly tailored, governed by the rule of law, transparent, and subject to oversight. We believe this can best be accomplished by building an international framework to set norms for government behavior.

Users must help government and industry strike the right balance between conflicting priorities. They should also take basic steps to protect their devices and data, including the use of encryption tools.

Industry can help by continually updating and advancing technology options that enable greater data protection and by sharing information that promotes an informed public dialogue. It must be responsive to both customer and government concerns, encouraging transparency and promoting legal processes that help ensure appropriate oversight exists when customer data is sought.

Having led Microsoft's Trustworthy Computing group for more than a decade, I can assure you that we fully embrace the mission to expand trust on the internet, in accordance with our guiding trust principles: security, privacy and transparency. Let me briefly expand on each of those.

Security: We begin with a focus on information assurance, continually building and enhancing security protections in our products and services. Microsoft has not and will not put "back doors" in our products and services, and we don't weaken our products to enable government spying. Our security efforts are focused on defense, not offense.

To increase customer protections, we continue to advance security technology and innovation. For the last decade, we have implemented the Security Development Lifecycle and we have extended our secure design methodology to cloud services. We are increasing our use of data encryption across services like Outlook.com, Office 365, OneDrive and Windows Azure. We have previously announcedthat by the end of 2014, all content moving across our networks will be encrypted by default.

Privacy: Regarding requests for customer data from law enforcement or other governmental entities, Microsoft is firm in its commitment to protect customer data.

We will only provide data in response to lawful requests for specific accounts or identifiers. Where appropriate, we will refer law enforcement requests directly to the customer, rather than attempting to fulfill the requests ourselves. Additionally, we require governments to live within the limits the law imposes on them, and will fight data requests that lack a jurisdictional basis or demand the production of bulk data.

Transparency: We are committed to transparency and strongly support a more open discussion on current data access policies.

One example of our transparency is our Government Security Program (GSP), which enables government customers to review our source code, in order to reassure them of its integrity. We recently announced plans to expand this access by opening several international Transparency Centers.

Microsoft also publishes a Law Enforcement Requests Report twice a year which details the number of law enforcement requests we receive (notably, only a tiny fraction of accounts are affected by government requests for data). Additionally, following a lawsuit filed by Microsoft and other large technology companies, the U.S. government agreed to let companies disclose figures on the national security orders received under the Foreign Intelligence Surveillance Act.

Wherever society nets out on this important debate on the appropriate degree of government involvement in the Internet, it's vital that industry remains principled in its approach to security, privacy and transparency.

We believe it is time for an international convention on privacy and government access to data, and have joined with others across the industry to recommend clear principles for government surveillance reform at ReformGovernmentSurveillance.com.

Microsoft will continue to push for policy and technical progress to restore public trust in technology, supporting increased transparency, sensible limits on data access and appropriate oversight. We will also push for greater coordination among governments. We believe that these steps are necessary to help restore the trust that is critical to the future growth of global IT systems, and that these steps can be achieved without undermining important public safety and national security concerns.

Appendix G: Exemplary Text 3

Earlier Denials Put Intelligence Chief in Awkward Position

WASHINGTON — For years, intelligence officials have tried to debunk what they called a popular myth about the National Security Agency: that its electronic net routinely sweeps up information about millions of Americans. In speeches and Congressional testimony, they have suggested that the agency's immense power is focused exclusively on terrorists and other foreign targets, and that it does not invade Americans' privacy.
Many top lawmakers, including Senator Harry Reid, have responded cautiously to the revelations. Senator Ron Wyden of Oregon has long been suspicious of N.S.A. activities.

But since the disclosures last week showing that the agency does indeed routinely collect data on the phone calls of millions of Americans, Obama administration officials have struggled to explain what now appear to have been misleading past statements. Much of the attention has been focused on testimony by James R. Clapper Jr., the director of national intelligence, to the Senate in March that the N.S.A. was not gathering data on millions of Americans.

When lawmakers returned to the Capitol on Tuesday for the first time since the N.S.A. disclosures, however, the criticism was muted.

In carefully delivered statements, Speaker John A. Boehner of Ohio; Senator Harry Reid of Nevada, the majority leader; and Senator Mitch McConnell of Kentucky, the Republican leader, all said the programs were authorized by law and rigorously overseen by Congress and courts.

In contrast, Senator Ron Wyden of Oregon, a Democrat whose questioning prompted Mr. Clapper's statement in March, stepped up his criticism of how intelligence officials portrayed the surveillance programs and called for public hearings to address the disclosures. "The American people have the right to expect straight answers from the intelligence leadership to the questions asked by their representatives," he said in a statement.

And Representative Brad Sherman, Democrat of California, said he had come away from a closed-door briefing by intelligence officials for House members believing that the N.S.A. had too much latitude and too little oversight.

"Right now we have a situation where the executive branch is getting a billion records a day, and we're told they will not query that data except pursuant to very clear standards," Mr. Sherman said. "But we don't have the courts making sure that those standards are always followed."

Many lawmakers trained their sights on Edward J. Snowden, the intelligence contractor who leaked classified documents to The Guardian and The Washington Post. Mr. Boehner called him a traitor.

Mr. McConnell told reporters: "Given the scope of these programs, it's understandable that many would be concerned about issues related to privacy. But what's difficult to understand is the motivation of somebody who intentionally would seek to warn the nation's enemies of lawful programs created to protect the American people. And I hope that he is prosecuted to the fullest extent of the law."

The comments of the Senate leaders showed a coordinated effort to squelch any legislative move to rein in the surveillance programs. Mr. Reid took the unusual step of publicly slapping back at fellow senators — including senior Democrats — who have suggested that most lawmakers have been kept in the dark about the issue.

“For senators to complain that they didn’t know this was happening, we had many, many meetings that have been both classified and unclassified that members have been invited to,” Mr. Reid said. “They shouldn’t come and say, ‘I wasn’t aware of this,’ because they’ve had every opportunity.”

Among lawmakers who have expressed concerns in the past, however, the issues have not been laid to rest. When reporters pressed Mr. Wyden on whether Mr. Clapper had lied to him, he stopped short of making that accusation, but made his discontent clear.

“The president has said — correctly, in my view — that strong Congressional oversight is absolutely essential in this area,” he said. “It’s not possible for the Congress to do the kind of vigorous oversight that the president spoke about if you can’t get straight answers.”

At the March Senate hearing, Mr. Wyden asked Mr. Clapper, “Does the N.S.A. collect any type of data at all on millions or hundreds of millions of Americans?”

“No, sir,” Mr. Clapper replied. “Not wittingly.”

Mr. Wyden said on Tuesday that he had sent his question to Mr. Clapper’s office a day before the hearing, and had given his office a chance to correct the misstatement after the hearing, but to no avail.

In an interview on Sunday with NBC News, Mr. Clapper acknowledged that his answer had been problematic, calling it “the least untruthful” answer he could give.

Michael V. Hayden, the former director of both the N.S.A. and the C.I.A., said he considered Mr. Wyden’s question unfair, given the classified subject. “There’s not another country in the world where that question would have been asked and answered in a public session,” he said.

Some other statements of N.S.A. officials appear in retrospect to offer a mistaken impression of the agency’s collection of information about Americans. Mr. Wyden said he had pressed Mr. Clapper on the matter because he had been dissatisfied with what he felt were misleading answers from Gen. Keith B. Alexander, the N.S.A. director. And in a recent speech, the N.S.A.’s general counsel, Rajesh De, sought to debunk what he called “false myths” about the agency, including the idea that “N.S.A. is spying on Americans at home and abroad with questionable or no legal basis.”

While that may be literally true — there is a legal basis — it appears awkward in retrospect that Mr. De’s defense of the agency failed to mention its collection of phone data on Americans.

“It’s a fine line he was treading,” said Matthew M. Aid, an intelligence historian and author of “The Secret Sentry,” a 2009 book on the N.S.A. “But trying to talk around these secret programs just makes matters worse.”

The solution, he said, is for intelligence officials to share more information about what the N.S.A. does and why. “Actually be forthright with the American people,” he said.

Senator Dianne Feinstein of California, chairwoman of the Intelligence Committee, told reporters on Tuesday that she had asked General Alexander to declassify more information about the surveillance programs — like terrorist plots that might have been foiled — to help explain their usefulness.

“If we can get that declassified, we can speak much more clearly,” she said.

Appendix H: Exemplary Text 4

NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say

The National Security Agency has secretly broken into the main communications links that connect Yahoo and Google data centers around the world, according to documents obtained from former NSA contractor Edward Snowden and interviews with knowledgeable officials.

By tapping those links, the agency has positioned itself to collect at will from hundreds of millions of user accounts, many of them belonging to Americans. The NSA does not keep everything it collects, but it keeps a lot.

According to a top-secret accounting dated Jan. 9, 2013, the NSA's acquisitions directorate sends millions of records every day from internal Yahoo and Google networks to data warehouses at the agency's headquarters at Fort Meade, Md. In the preceding 30 days, the report said, field collectors had processed and sent back 181,280,466 new records — including "metadata," which would indicate who sent or received e-mails and when, as well as content such as text, audio and video.

The NSA's principal tool to exploit the data links is a project called MUSCULAR, operated jointly with the agency's British counterpart, the Government Communications Headquarters . From undisclosed interception points, the NSA and the GCHQ are copying entire data flows across fiber-optic cables that carry information among the data centers of the Silicon Valley giants.

The infiltration is especially striking because the NSA, under a separate program known as PRISM, has front-door access to Google and Yahoo user accounts through a court-approved process.

The MUSCULAR project appears to be an unusually aggressive use of NSA tradecraft against flagship American companies. The agency is built for high-tech spying, with a wide range of digital tools, but it has not been known to use them routinely against U.S. companies.

In a statement, the NSA said it is "focused on discovering and developing intelligence about valid foreign intelligence targets only."

"NSA applies Attorney General-approved processes to protect the privacy of U.S. persons — minimizing the likelihood of their information in our targeting, collection, processing, exploitation, retention, and dissemination," it said.

In a statement, Google's chief legal officer, David Drummond, said the company has "long been concerned about the possibility of this kind of snooping" and has not provided the government with access to its systems.

"We are outraged at the lengths to which the government seems to have gone to intercept data from our private fiber networks, and it underscores the need for urgent reform," he said.

A Yahoo spokeswoman said, "We have strict controls in place to protect the security of our data centers, and we have not given access to our data centers to the NSA or to any other government agency."

Under PRISM, the NSA gathers huge volumes of online communications records by legally compelling U.S. technology companies, including Yahoo and Google, to turn over any data that match court-approved search terms. That program, which was first disclosed by The Washington Post and the

Guardian newspaper in Britain, is authorized under Section 702 of the FISA Amendments Act and overseen by the Foreign Intelligence Surveillance Court (FISC).

Intercepting communications overseas has clear advantages for the NSA, with looser restrictions and less oversight. NSA documents about the effort refer directly to "full take," "bulk access" and "high volume" operations on Yahoo and Google networks. Such large-scale collection of Internet content would be illegal in the United States, but the operations take place overseas, where the NSA is allowed to presume that anyone using a foreign data link is a foreigner.

Outside U.S. territory, statutory restrictions on surveillance seldom apply and the FISC has no jurisdiction. Senate Intelligence Committee Chairman Dianne Feinstein (D-Calif.) has acknowledged that Congress conducts little oversight of intelligence-gathering under the presidential authority of Executive Order 12333 , which defines the basic powers and responsibilities of the intelligence agencies.

John Schindler, a former NSA chief analyst and frequent defender who teaches at the Naval War College, said it is obvious why the agency would prefer to avoid restrictions where it can.

"Look, NSA has platoons of lawyers, and their entire job is figuring out how to stay within the law and maximize collection by exploiting every loophole," he said. "It's fair to say the rules are less restrictive under Executive Order 12333 than they are under FISA," the Foreign Intelligence Surveillance Act.

In a statement, the Office of the Director of National Intelligence denied that it was using executive authority to "get around the limitations" imposed by FISA.

The operation to infiltrate data links exploits a fundamental weakness in systems architecture. To guard against data loss and system slowdowns, Google and Yahoo maintain fortresslike data centers across four continents and connect them with thousands of miles of fiber-optic cable. Data move seamlessly around these globe-spanning "cloud" networks, which represent billions of dollars of investment.

For the data centers to operate effectively, they synchronize large volumes of information about account holders. Yahoo's internal network, for example, sometimes transmits entire e-mail archives — years of messages and attachments — from one data center to another.

Tapping the Google and Yahoo clouds allows the NSA to intercept communications in real time and to take "a retrospective look at target activity," according to one internal NSA document.

To obtain free access to data- center traffic, the NSA had to circumvent gold-standard security measures. Google "goes to great lengths to protect the data and intellectual property in these centers," according to one of the company's blog posts, with tightly audited access controls, heat-sensitive cameras, round-the-clock guards and biometric verification of identities.

Google and Yahoo also pay for premium data links, designed to be faster, more reliable and more secure. In recent years, both of them are said to have bought
or leased thousands of miles of fiber-optic cables for their own exclusive use. They had reason to think, insiders said, that their private, internal networks were safe from prying eyes.

In an NSA presentation slide on "Google Cloud Exploitation," however, a sketch shows where the "Public Internet" meets the internal "Google Cloud" where their data reside. In hand-printed letters, the drawing notes that encryption is "added and removed here!" The artist adds a smiley face, a cheeky celebration of victory over Google security.

Two engineers with close ties to Google exploded in profanity when they saw the drawing. “I hope you publish this,” one of them said.

For the MUSCULAR project, the GCHQ directs all intake into a “buffer” that can hold three to five days of traffic before recycling storage space. From the buffer, custom-built NSA tools unpack and decode the special data formats that the two companies use inside their clouds. Then the data are sent through a series of filters to “select” information the NSA wants and “defeat” what it does not.

PowerPoint slides about the Google cloud, for example, show that the NSA tries to filter out all data from the company’s “Web crawler,” which indexes Internet pages.

According to the briefing documents, prepared by participants in the MUSCULAR project, collection from inside Yahoo and Google has produced important intelligence leads against hostile foreign governments that are specified in the documents.

Last month, long before The Post approached Google to discuss the penetration of its cloud, Eric Grosse, vice president for security engineering, said the company is rushing to encrypt the links between its data centers. “It’s an arms race,” he said then. “We see these government agencies as among the most skilled players in this game.”

Yahoo has not announced plans to encrypt its data-center links.

Because digital communications and cloud storage do not usually adhere to national boundaries, MUSCULAR and a previously disclosed NSA operation to collect Internet address books have amassed content and metadata on a previously unknown scale from U.S. citizens and residents. Those operations have gone undebated in public or in Congress because their existence was classified.

The Google and Yahoo operations call attention to an asymmetry in U.S. surveillance law. Although Congress has lifted some restrictions on NSA domestic surveillance on grounds that purely foreign communications sometimes pass over U.S. switches and cables, it has not added restrictions overseas, where American communications or data stores now cross over foreign switches.

“Thirty-five years ago, different countries had their own telecommunications infrastructure, so the division between foreign and domestic collection was clear,” Sen. Ron Wyden (D-Ore.), a member of the intelligence panel, said in an interview. “Today there’s a global communications infrastructure, so there’s a greater risk of collecting on Americans when the NSA collects overseas.”

It is not clear how much data from Americans is collected and how much of that is retained. One weekly report on MUSCULAR says the British operators of the site allow the NSA to contribute 100,000 “selectors,” or search terms. That is more than twice the number in use in the PRISM program, but even 100,000 cannot easily account for the millions of records that are said to be sent to Fort Meade each day.

In 2011, when the FISC learned that the NSA was using similar methods to collect and analyze data streams — on a much smaller scale — from cables on U.S. territory, Judge John D. Bates ruled that the program was illegal under FISA and inconsistent with the requirements of the Fourth Amendment.

Appendix I: Exemplary Text 5

Governments break silence on surveillance as activists launch human rights principles

Civil society organisations today called upon the members of the Human Rights Council to assess whether national surveillance laws and activities are in line with their international human rights obligations.

The Snowden revelations have confirmed that governments worldwide continue to expand their spying capabilities, at home and abroad. Widespread surveillance is being conducted in violation of individuals' rights to privacy and free expression, and is seldom regulated by strong legal frameworks that respect human rights.

With this in mind, a coalition of civil society organisations today launched the "International Principles on the Application of Human Rights to Communications Surveillance," a set of standards that interpret States' human rights obligations in light of new technologies and surveillance capabilities. The Principles are endorsed by over 260 civil society organisations around the world, and for the first time set out an evaluative framework for assessing surveillance practices in the context of international human rights law.

Civil society organisations presented the Principles during an event on the right to privacy, hosted by the governments of Germany, Norway, Austria, Hungary, Liechtenstein and Switzerland, at the 24th session of the Human Rights Council in Geneva.

Navi Pillay, the United Nations High Commissioner for Human Rights, speaking at the event, said that: "technological advancements have been powerful tools for democracy by giving access to all to participate in society, but increasing use of data mining by intelligence agencies blurs lines between legitimate surveillance and arbitrary mass surveillance."

Acknowledging that States have a legitimate task of protecting national security, the High Commissioner stressed that this must done in compliance with the law and any actions must be regulated and monitored by the judiciary.

Joining the High Commissioner was Frank La Rue, the UN Special Rapporteur on freedom of opinion and expression, who recently released a report which details the widespread use of state surveillance of communications, stating that such surveillance severely undermines citizens' ability to enjoy a private life, freely express themselves and enjoy their other fundamental human rights.

Speaking at the event, the UN Special Rapporteur remarked that: "previously surveillance was carried out on targeted basis but the Internet has changed the context by providing the possibility for carrying out mass surveillance. This is the danger."

In this new context, Frank La Rue stressed that all restrictions to rights have to be established by law, and implemented by legal institutions as well as supported by independent judicial and parliamentary oversight mechanisms. With the aim of taking the discussion forward and ensuring concrete actions, the Special Rapporteur suggested the organisation of a special session at the Human Right Council on surveillance and the right to privacy, and a preparatory multi-stakeholder seminar, as well as the appointment of a temporary special expert to lead the initiative.

Representatives of Privacy International, the Electronic Frontier Foundation, Access, Human Rights Watch, Reporters Without Borders, Association for Progressive Communications, and the Center for Democracy and Technology all took part in the event.

Carly Nyst, Head of International Advocacy at Privacy International, emphasised the fundamental importance of the right to privacy: “State surveillance severely threatens individuals’ rights to privacy, free expression and free association; impedes an open and democratic society; hinders a free press; breeds conformity and undermines innovation; and strikes at the heart of human dignity and autonomy. It must only be conducted in the most exceptional circumstances, under the watchful eye of an independent judicial authority and strong oversight mechanisms.”

Cynthia Wong, Senior Internet Researcher at Human Rights Watch, warned: “Without stronger protections for online privacy, we are quickly headed toward a world where pervasive surveillance is the norm and privacy disappears the second we go online. As mobile and Internet adoption expands globally, every government should ensure people can use these technologies without fear of invasive and disproportionate intrusions into their private lives.”

Lucie Morillion, Head of Reporters Without Borders Advocacy Department, stressed that: “more efforts must be done to regulate and monitor the export of surveillance technologies to countries which utilise them to identify and track down dissidents, human right defenders and journalists, who are disclosing public interest information. Without the adoption and implementation of adequate protection mechanisms of these individuals, the right to information is challenged and investigatory journalism is at risk.”

In presenting the 13 Principles, Katitza Rodriguez, International Rights Director at the Electronic Frontier Foundation, urged: “member states to assess their national surveillance laws and bring them into compliance with the 13 benchmarks. We must put an end to unchecked, suspicionless, mass spying online and worldwide. Privacy is a human right, and needs to be protected as fiercely as all other rights”.

Fabiola Carrion, Policy Counsel at Access, while presenting the Principles, concluded: “In Access - an organization that defends and extends the fundamental rights of digital users at risk - we are extremely concerned with the massive surveillance practices perpetrated by States, from authoritarian regimes to those with democratic institutions. As such, we enthusiastically join this proactive effort to place a framework for States to fulfill their human rights obligations under international law.”

Following the event remotely from South Africa, Anriette Esterhuysen, Executive Director of the Association for Progressive Communications wrote: "Privacy and security should not be set off against one another. A robust and trusted internet needs both, and they are mutually reinforcing. The same cannot be said for privacy and mass surveillance. Mass surveillance undermines privacy in every possible sense of what the term means: from a human rights perspective and the perspective of a robust, secure and trusted internet."

Matthew Shears, Director for Global Internet Policy and Human Rights with the Center for Democracy & Technology, said: “We believe these principles outline the essential elements for applying human rights to communications surveillance and look forward to collaborating with human rights institutions and human rights advocates to promote these principles globally.”

Appendix J: Exemplary Text 6

Rating Obama's NSA Reform Plan: EFF Scorecard Explained

Earlier today, President Obama announced a series of reforms to address abuses by the National Security Agency. We were heartened to see Obama recognized that the NSA has gone too far in trampling the privacy rights of people worldwide. In his speech, the President ensured that National Security Letters would not come with perpetual gag orders, brought new levels of transparency and fairness to the FISA court, and ended bulk collection of telephone records by the NSA. However, there is still much more to be done.

We've put together a scorecard showing how Obama's announcements stack up against 12 common sense fixes that should be a minimum for reforming NSA surveillance. Each necessary reform was worth 1 point, and we were willing to award partial credit for steps in the right direction. On that scale, President Obama racked up 3.5 points out of a possible 12.

1. Stop mass surveillance of digital communications and communication records.
Score: .2

There are three types of mass surveillance that we know about that we were using to evaluate Obama's promises in this category: surveillance of millions of phone records under Section 215 of the PATRIOT Act; surveillance of Internet communications internationally under Section 702 of the FISA Amendments Act; and surveillance of communications overseas under Executive Order 12333.

In order to score a full point in this category, Obama would have needed to declare that the executive branch would no longer be using any of these authorities to engage in mass surveillance. He tackled only one of these issues somewhat: the surveillance of telephony metadata under Section 215 of the Patriot Act. Specifically, he acknowledged the recommendations of his review group that the government cease to collect and maintain a database of all Americans' telephone records. He is ending that program, which is laudable. However, he left open the door to having telecom companies or another third party maintain a similar set of mass data, so even as to 215, we could not give him the full ⅓ of the point.

2. Protect the privacy rights of foreigners.
Score: .3

All too often, the NSA's official position is that foreigners—or anybody deemed sufficiently likely to not be a "U.S. person"—are not given any legal protections under surveillance laws. This situation is unacceptable and out of line with international human rights law, as we've put forth in our Necessary and Proportionate Principles, now supported by over 300 organizations worldwide. We demanded that individualized targeting be conducted for non-US persons.

Obama nodded a bit to this situation, and proposed that some reforms be made, but did not give real specifics. While he also did not acknowledge any legal obligations, he did recognize a "special obligation" on U.S. intelligence agencies, and specifically called out a new, higher standard on eavesdropping on foreign leaders. But that's not enough: privacy consideration should not be a privilege afforded only to top officials. Given these small steps forward but ongoing problems, we've given Obama .3 points in this category.

3. No data retention mandate.
Score: 0

Obama's review group recommended that the telephone metadata surveillance program be taken away from the government, suggesting that a third party or even telecom companies themselves be responsible for maintaining a searchable list of our calling records. This approach—mandating companies act as Big Brother's little helper—won't alleviate the serious privacy concerns with maintaining a digital record of every call we make.

We had hoped that Obama would make clear that he would reject any form of mandatory data retention. Instead, Obama acknowledged some of the concerns with a data retention mandate but

called for "options for a new approach that can match the capabilities and fill the gaps that the Section 215 program was designed to address, without the government holding this metadata itself." He never specifically rejected the idea of forcing companies or a third party to hold this data, and so he does not receive a point in this category.

4. Ban no-review National Security Letters.
Score: .5
The President gets half a point here, since he endorsed ending the permanent gag orders that accompany administrative subpoenas known as National Security Letters, under which the FBI can on its own demand information about you from your communications service providers. We still need specifics, and the details really matter—even fixed-length gags would violate the First Amendment, for example, and gags would still need to be approved by courts—but this was a good and necessary step. Obama didn't get the other half, though, because he did not agree with EFF and his own review panel that NSLs should only issue after judicial approval. Early in 2014, EFF will ask the 9th Circuit Court of Appeals to find, like the District Court for the Northern District of California already did, that the NSL statute is unconstitutional in its current form.

5. Stop undermining Internet security.
Score: 0
The NSA's systematic efforts to weaken and sabotage the encryption and security technologymake us all less safe. But in contrast to his review group's recommendations to stop those practices, Obama was silent on the issue. That silence is disappointing, as this is a critical problem that has not just undermined the privacy of millions around the world, but poisoned our collective trust in institutions that depend most on it. Zero points.

6. Oppose the FISA Improvements Act.
Score: 1
The FISA Improvements Act seeks to codify into law the NSA's controversial and illegal practice of collecting and storing the telephone records of hundreds of millions of Americans. While Obama's administration had earlier indicated support for the bill, today's announcement made clear that Obama was not going to support this program going forward and thus was not supporting the FISA Improvements Act. We would have preferred it if Obama had stated clearly that he would veto any bill that attempts to codify mass telephone metadata surveillance, but we felt this was good enough to merit a point.

7. Reject the third party doctrine.
Score: 0
The third party doctrine is an outdated and deeply problematic legal theory that wipes out many of the privacy protections we could otherwise enjoy. It's the shaky foundation on which some of the most invasive programs by the NSA and other law enforcement agencies rest. Obama should have said that we have a reasonable expectation of privacy in data even though we've trusted third party service providers with it—instead, he was silent on the issue.

8. Provide a full public accounting of our surveillance apparatus.
Score: .5
In our criteria, we asked that Obama "appoint an independent committee to give a full public accounting of surveillance programs that impact non-suspects around the world" and that this committee "directly engage whistleblowers like Thomas Drake, William Binney, Edward Snowden and others, and include independent technological experts." For this category, we awarded Obama with a half point because he did appoint his counsel, John Podesta, to lead "a comprehensive review of big data and privacy." However, it remains to be seen whether this committee will actually provide a full public accounting or engage with the whistleblowers who have much to contribute.

9. Embrace meaningful transparency reform.
Score: 0

Fundamental to all of the problems surrounding NSA spying is the fact that the government's notorious secrecy shields it from any sort of meaningful oversight or accountability. This appears, among other places, in the overclassification of documents that should not actually be secret, in the executive branch's ruthless campaign against whistleblowers, and in its continued abuse of the "state secrets" privilege in the courtroom. Obama could have announced changes to these secrecy standards, embracing transparency as a default, and making some good on his now laughable election promise to be "the most transparent administration in history." Instead we got nothing.

10. Reform the FISA court.
Score: 1
We gave Obama a full point for these reforms, since he embraced both independent advocates for the FISA court and an annual process of review of FISC decisions for declassification. While we would like the review to be more current, and there is much to be done to ensure that the independent advocacy panel has a real, unfettered role, Obama's announcement indicated a good direction on both.

11. Protect national security whistleblowers.
Score: 0
Obama was clear: "One thing I'm certain of, this debate will make us stronger." And there is little question that this debate would not have happened without the evidence brought to light by Snowden and other whistleblowers. It might seem that Obama would have some recognition that, but for these individuals, we would not be having this important debate.
Sadly, Obama's speech today gave no indication of a change in strategy in his administration's war on whistleblowers. If Obama welcomes this debate, he should stop his attack on the people who have risked so much to help make it happen.

12. Give criminal defendants all surveillance evidence.
Score: 0
It's a cornerstone of our justice system that the accused have the right to see all the evidence against them. That made it very alarming when we learned that the NSA was collecting intelligence and then laundering it into criminal investigations by the Drug Enforcement Agency and other law enforcement groups. This practice conflicts with the protections enshrined in the Fifth and Sixth amendments, and should be stopped immediately. While Attorney General Holder has promised to review the cases, the Administration has not promised to ensure that everyone whose information was shared with law enforcement agencies by the NSA ultimately gets notice. Obama didn't mention this necessary measure in his speech, and gets no points.

Appendix K: SPSS Output

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	3,135[a]	1	,077		
Continuity Correction[b]	2,006	1	,157		
Likelihood Ratio	3,225	1	,073		
Fisher's Exact Test				,155	,078
Linear-by-Linear Association	3,056	1	,080		
N of Valid Cases	40				

a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 5,50.

b. Computed only for a 2x2 table

Stance of corporate sector regarding mass surveillance

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	14,250[a]	3	,003
Likelihood Ratio	18,783	3	,000
Linear-by-Linear Association	10,168	1	,001
N of Valid Cases	30		

a. 6 cells (75,0%) have expected count less than 5. The minimum expected count is ,33.

Stance of citizen group sector regarding mass surveillance

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	1,111[a]	2	,574
Likelihood Ratio	1,158	2	,561
Linear-by-Linear Association	,389	1	,533
N of Valid Cases	50		

a. 3 cells (50,0%) have expected count less than 5. The minimum expected count is 1,00.

Mentioning of corporate sector data collection

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	3,125[a]	2	,210
Likelihood Ratio	3,791	2	,150
Linear-by-Linear Association	2,333	1	,127
N of Valid Cases	50		

a. 3 cells (50,0%) have expected count less than 5. The minimum expected count is ,40.

Mentioning of corporate sector data monetization