MPC MAJOR RESEARCH PAPER

Head in the Clouds:
A Critical Discourse Analysis of American Cloud Computing and State Surveillance in Post-Snowden Press Coverage

Stefan Milosevic

Dr. Matthew Tiessen
Dr. John Shiga

This Major Research Paper is submitted
in partial fulfillment of the requirements for the degree of
Master of Professional Communication

Ryerson University
Toronto, Ontario, Canada
2014

AUTHOR'S DECLARATION FOR ELECTRONIC SUBMISSION OF A MAJOR RESEARCH PAPER

I hereby declare that I am the sole author of this Major Research Paper and the accompanying Research Poster. This is a true copy of the MRP and the research poster, including any required final revisions, as accepted by my examiners.

I authorize Ryerson University to lend this major research paper and/or poster to other institutions or individuals for the purpose of scholarly research.

I further authorize Ryerson University to reproduce this MRP and/or poster by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

I understand that my MRP and/or my MRP research poster may be made electronically available to the public.

Abstract

The National Security Agency (NSA) revelations leaked by Edward Snowden on June 6, 2013 regarding the digital surveillance tactics of the United States government were a series of profoundly disruptive discursive events that signaled an uncomfortably cozy relationship between US technology companies and the US government for the maintenance of US national security. Leaked internal NSA slides revealed a host of domestic and foreign clandestine spying programs, including PRISM and MUSCULAR, which suggested the unscrupulous collection of data from US technology giant Google's cloud servers and private networks, among other technology companies. Google's cloud computing services particularly became implicated in a crisis of global proportions, as the technology giant and US technology industry writ large faced a global loss of confidence and future revenue from cloud computing customers unhappy with the implications the NSA revelations had for the security of their personal and corporate data. This paper conducts a multi-layer critical discourse analysis about the effect the NSA revelations had on US cloud computing with a specific focus on Google's cloud computing services. By focusing on the sociopolitical and economic functions of surveillance as established within surveillance literature, this project examines how the crisis was discursively constructed in order to paint a larger picture about how popular press coverage framed the NSA revelations and the relationship of this rhetoric to the technology companies it implicates.

Acknowledgements

I would like to thank my family and friends for their love, unwavering support, and patience throughout my education and, in many ways, my life.

Thank you to my second reader, Dr. John Shiga, for his encouraging feedback on my work.

Finally, I would like to thank my dedicated supervisor, Dr. Matthew Tiessen, whose friendly flavor of mentorship gave me confidence in my capacities as a young scholar and communications professional.

Table of Contents

List of Figures

Introduction

On the morning of June 6, 2013 influential daily newspapers *The Guardian* and *The Washington Post* quietly published stories with leaked evidence from former U.S. National Security Agency (NSA) contractor Edward Snowden proving that the NSA had been granted secret court orders that gave the agency the ability to unscrupulously collect daily metadata from all domestic Verizon customers. Since the release of these revelations, more and more stories focused on the endless trove of Snowden leaks, which have been popularly referred to as the NSA revelations, have exposed the U.S. government's spying activities on foreign and domestic Internet users. A particularly resonant leak, particularly for the purposes of this study, has revealed that these secret court orders also granted NSA access to the servers of nine leading U.S. cloud computing providers, including Google, Facebook, Apple, and Amazon, among others.

The public outing of the NSA's secret spying program, which is named PRISM, (though there are others), has revealed the sheer magnitude of the NSA's surveillance capacities, allowing for warranted speculation about the broader social effects of this new (as far as the public was concerned) politically-monitored and surveilled Internet environment. As many critical media studies scholars have observed, based on the news that the U.S. government does in fact have the capacity to monitor Internet communication using a clandestine spying program, and by virtue of their self-given position as watcher of the Internet, the U.S. government has positioned the Internet and its users as subjects of its punitive gaze in what has been outed as a data-hungry surveillance state. The U.S. government, in other words, subordinates users through the forced legal strong-arming of U.S. Internet companies as it exercises its ability to monitor, classify, and potentially

discipline users whose online activity it deems threatening to its national security and integrity via secret court orders.

The NSA revelations have contributed to a global conversation about the state of online privacy and the panoptic power of American state-sanctioned online surveillance. The NSA revelations have also meant that our most beloved and routinely visited Internet companies are legally complicit in U.S. government surveillance of our online (and, by extension, offline) activities. Considering that the NSA acts under the U.S. government's Department of Defense, it is significant to note again that the NSA, as a mechanism of surveillance, must be understood as a powerful tool of state-driven social control that exists to maintain social order that benefits U.S. national interests.

The NSA revelations can be regarded as a timely and relevant example with which to ground theoretical notions about surveillance since the revelations have made real the cozy relationship between American technology giants and the U.S. government for the purpose of surveillance and identifying dissidence and risks.

This paper will examine the effects the NSA revelations have had on American cloud computing providers by conducting a critical discourse analysis of popular post-Snowden press coverage of the phenomenon, focusing specifically on coverage of Google's cloud computing services as an exemplar of the industry.

Literature Review

Surveillance as a Discipline, a Punitive Tool, and an Economic Stimulator

As a discipline, surveillance studies is a relatively new field. Queen's University's David Lyon is one of its seminal thinkers and pioneers. That being said, in Lyon's *Surveillance Studies: An Overview* (2007) he does not (nor can he) take credit for creating the field, but rather for beginning to piece it together. Lyon locates surveillance studies historically, outlining its history and purpose in social theory, particularly in the work of theorists like Michel Foucault and Gilles Deleuze (Foucault, 1980; Deleuze, 1992).

Lyon states that surveillance is generally:

> Interested in gathering information about individuals and listing them in categories, a form of inventory. But it does not achieve this in an abstract, objective way. As surveillance categories make people up to fit them, so those thus identified may also assert what they claim are their identities, those ways of thinking about themselves that make sense to them. Surveillance is as old as human history and has always been ambiguous. It starts with anyone watching over others for some purpose. … Surveillance is then the routine and focused attention to personal details for the purposes of influence, protection, management or control. (2006, p. 74-6)

Lyon's definition of surveillance is significant because it reinforces structural privileges that come with watching that allow the watcher to define, keep an inventory of, and control the watched—what Bowker and Star (1999) have referred to as an "act of classification which is moral because each standard or category valorizes one viewpoint and silences another; it can therefore create advantage or suffering" (pg. 5). For Lyon, the fact that surveillance is based on one agent having the power to classify and keep an inventory of another for some subjective purpose is significant because it affects "how each person or his or her activities are classified, which is likely to make a difference to his or her life" (2006, pg. 73).

Identification, categorizing, and monitoring, then, are the pillars and purpose of surveillance; moreover, as Lyon notes, they can also be regarded as the fundamental building blocks of modernity in so far as they deliver "the kinds of information sought and revealed by surveillance practices [throughout history] from the informal and unsystematic supervision of pre-modern times, through the formal, classificatory schemes of modernity, and into the complex and fluctuating world of digital networks that some dub postmodern" (2006, pg. 74). Briefly, pre-modern, or face-to-face, surveillance is bound by space and occurs in real-time in a clear observer / observed relationship. Modern surveillance, on the other hand, is the result of rationalization, standardization, and file-based coordination that encourages on society-wide scales the uniformity and homogeneity that is critical for constructing the bureaucratic structure and hierarchies of modern society. Postmodern surveillance is digitally mediated and based on tracking and modulation using electronic interfaces between the subject and the surveillance system; it conflates previous notions of surveillance and produces new ones that can be oriented around the micro level of the body or the macro level of the entire globe (Lyon, 2006, pg. 75).

These three temporally distinct forms of surveillance—pre-modern (face), modern (file), postmodern (digital)—can and do overlap, existing in various combinations or independently. The three distinctions are critical to beginning to understand the complex spectrum of surveillance as described in surveillance studies literature.

Alongside Orwell's *1984,* Foucault's (1980) work on knowledge, visibility, and power is often cited as the archetypal analytical literature on the immense influence and privilege watching and tracking bodies has in society and the role of surveillance as a tool

for creating and enforcing moral categories (Lyon, 2006; Bowker and Star, 1999). Through his metaphorical appropriation and projection of Bentham's "panopticon," a prison design that made prisoners fully visible to prison guards while not being able to see the guards themselves, Foucault linked visibility and power to the entire mechanism of the modern bureaucratic state, which produces subjects as it acknowledges or performs surveillance on them from an often unobservable distance. Foucault argues that the watcher interpolates the watched into a system of power relations through the surveillance process that the watched internalize and identify with, thereby giving power to it and the watcher (1980).

There is much to be said in contemporary surveillance literature that negotiates with and updates Foucauldian notions of what Haggerty and Ericson (2000) have referred to as the "soul-shaping surveillance" of the panopticon as both metaphor and reality. It is important to acknowledge Foucault's contribution but also to go beyond him to investigate more contemporary forms of surveillance today and societies of control as referenced in, for example, Deleuze (1992) and his work with Guattari (1987) or Haggerty and Ericson's (2000) development of the "the surveillant assemblage" concept which explores the complex factors that come together to produce and reproduce the contemporary surveillance state.

Haggerty and Ericson (2000) point to Foucault's "curious silence" when "engaging in contemporary developments in surveillance technology" and propose the assemblage as a critical metaphor with more contemporary depth and traction than the surveillance theories in the work of Foucault or Orwell (p. 607). The surveillant assemblage is a "multiplicity of heterogeneous objects whose unity comes solely from the fact that these

items function together, that they 'work' together as a functional entity" (p. 608). In other words, while Orwell sees surveillance as a tool of elite control and Foucault sees it as a form of discipline, Haggerty and Ericson, citing Bauman (1992), develop what can be more familiarly referred to as the "intersectionality" of surveillance, which they name the assemblage. Government surveillance becomes entrenched in postmodern society as the market becomes concerned with the production of insightful consumer profiles that arise from the increasingly sought-after "surplus value of surveillance" (p. 616). This pursuit of surplus value implicates the government, the police, and business in the development of the same surveillance activities and mechanisms they all benefit from. This assemblage "standardizes the capture of flesh/information flows of the human body" across social fields, so that "it can be rendered more mobile and comparable" and "information derived from [these flows can be] scrutinized in the hopes of developing strategies of governance, commerce, and control" (p. 613).

Deleuze and Guattari (1987) use the image of the rhizome to describe the control society: it "may be broken, shattered at a given spot, but it will start up again on one of its old lines, or on new lines" (p. 9). The rhizome metaphor can help us illustrate Haggerty and Ericson's notion of the surveillant assemblage. For them, both ideas work together to illustrate three ways in which surveillance has been woven into identity formation, digital economics, and the social fabric: (1) postmodern theorist Mark Poster's (1990) idea of the "data double" is taken to its absolute extreme, making individuals identifiable and punishable through and by their digital trails forever; (2) the surplus value created by individual user behaviour online is constituting a form of commodification of the self as users create value for others while creating themselves online (p. 616); and (3) since

computerization has saturated society, surveillance has ushered in the obliteration of privacy or the "disappearance of disappearance" (p.619). The rhizomatic surveillant assemblage society poses a grand bargain to citizens: participate in culture and be watched alongside your participation, or do not participate and remove yourself from an increasingly inescapable digitized world.

Tiessen (2011) illustrates Deleuze's prediction of imperceptible and dematerialized forms of discipline in the control society by investigating airport body scanners (p. 169). Tiessen uses the airport scanner as a material object through which to glean insights about the surveillance state more generally, several of which are particularly germane to an analysis of the NSA and cloud computing particularly: (1) the notion that "preemptive [politics] and security practices [are] securing the present from pursuing or acting on any subversive or undesirable power-resisting potentials" (p. 174); (2) the idea that this commitment to preemptive political action brings new financial markets into being through "the marketing of insecurity" (p. 175); (3) the observation that "perversely…citizens both pay for the expansion of the surveillance state while also being constituted as its targets," referencing immaterial and digital labour (Lazzarrato, 1996; Scholz, 2012); (4) the idea that individuals "who are subject to the invisible gaze of security find themselves clamoring to expose themselves in order to reveal they are not a threat…complete exposure, then, becomes the only way to reveal innocence" (p. 180); and finally (5) the observation that these practices are to be understood paradoxically in so far as they function both to threaten *and* protect privacy (p.169).

The writers mentioned above acknowledge the multiplicity of motives, meanings, and manifestations of surveillance when it becomes pervasive in the digitized network as a

way of life and moneymaker in government policy and business. Foucauldian panopticism does not account for all of the complex realities advanced control societies mandate. Projecting the panopticon outside of the prison may be a useful entry point into surveillance studies, however panopticism alone doesn't cut it.

It is noteworthy that the above analyses of surveillance draws almost exclusively on top-down, dystopian, and Orwellian imagery, often denying or omitting entirely the agency of individuals implicated in these surveillance systems whose capabilities seem to be dwarfed by that of the surveillance mechanism operating over and above them. Goffman (1961) and Yar (2003) are outliers in the traditional surveillance literature because they acknowledge the power of the individuals who are subject to surveillance. In *Asylums: Essays on the Social Situation of Mental Patents and Other Inmates,* Goffman (1961) probes the classification system which the prison system borrowed from—the asylum's—by referring to the asylum as a "total institution" and as the original surveillance apparatus (1961, p. 4). Despite writing about mid-century asylums, Goffman's comments have particular parallels with the postmodern surveillance state. Lyon (2006) points out a key insight in Goffman's work where Goffman describes the agency of the individual subjected to surveillance, which we can project out of the asylum and onto the web:

> while patients were watched over with the intention of changing them in specific ways … they did not necessarily become … reformed criminals. … The point is this: the surveillance aspect of the "total institution" creates circumstances … not necessarily … intended by the institution. This insight is crucially important in surveillance studies, because there is a frequent assumption that surveillance systems are all powerful. (pg. 83)

Yar (2003) explores the ways surveilled subjects actively negotiate with the systems and interfaces that monitor them, effectively challenging the Foucauldian notion that grants the watcher untestable power by claiming that the negotiation of the power relationship by the watched is "polyvalent and complex," (pg. 5) from avoiding the gaze of security cameras to hacker culture. Lyon, on the other hand, questions "how technically unqualified people are to be engaged in the politics of surveillance today" (pg. 87). Albrechtsund's *Empowering Residents: A Theoretical Framework for Negotiating Surveillance Technologies* (2010) proposes revisits Marx's notion of agency and structure and suggests that designers of digital technologies and interfaces need to understand how and why users negotiate with prescribed uses of online technologies. In *Islands of Privacy,* sociologist Christina Nippert-Eng conducts interviews with people who go to extreme lengths to achieve not only digital but physical privacy in a society where surveillance and watching have been normalized on all fronts. Dwelling on surveillance as a multidimensional practice performed by states and corporations on citizens and customers, respectively, is paramount before examining the technology of cloud computing specifically. The next portion of the literature review will establish the connection between NSA spying and the cloud computing industry considering the assemblage metaphor established above.

Surveillance, the NSA Revelations, and Cloud Computing

Considering the overlapping sociopolitical and economic functions of surveillance in society as described in the literature, the American cloud computing industry could be approached with this multifaceted "assemblage" metaphor in mind. The fact that a cozy relationship between American cloud computing providers and the NSA has been revealed

and confirmed in popular discourse has created an ideal and timely opportunity to ground these abstract theoretical claims. To do so, cloud computing must be understood as a sort of mythic or supernatural technological reality (as far as the public is concerned) that has been co-opted by "power" for the needs of the capitalist surveillant assemblage.

Mosco (2014), for example, has taken it upon himself to do a trans-disciplinary mapping of the enormous economic, social, political, and cultural significance of cloud computing by exploring the "seemingly unchallengeable beliefs that influence not only how we think about cloud computing, but about technology in general and our relationship to it" (p. 5). Mosco's contribution to critical technology and surveillance studies is significant and his widely accepted notion of the digital sublime, "the tendency of technology to take on a transcendent role in the world beyond the banality of its role in everyday life" (2004), is a powerful idea that introduces and acknowledges a mythological element to our engendered understanding of technology. Understanding digital technologies as expressive of an experience of digital sublimity requires a multifaceted – and interdisciplinary – understanding of how digital technologies affect the social fabric by examining the narratives that surround them and are embedded in them, endowing them with almost mystical qualities. For example, as a technology, cloud computing is a convenience, but as a myth, cloud computing:

> Serves as a prism that reflects and refracts every major issue in the field of information technology and society, including the fragile environment, ownership and control, security and privacy, work and labor, the struggles among nations for dominance in the global political economy, and how we make sense of the world in discourse and in cultural expression. (Mosco, 2014, pg. 5)

The mythological dimension of cloud computing is significant to mention for this project because, for Mosco "there is no generally accepted definition of cloud computing… it is a metaphor for the Internet. It's rebranding the Internet… By virtue of being a metaphor, it's open to different interpretations" (2014, p. 16). As a loosely anchored signifier, the term cloud computing itself can have a multiplicity of meanings: popularly, cloud computing "describes a new system for accessing files, software, and computer power over the Internet instead of from a computer's own hard drive or some other portable storage system" (Regaldo 2011). More formally, a widely accepted definition of cloud computing hails from a U.S. government request of the National Institute of Standards and Technology (NIST) to standardize a definition and description of cloud computing when government departments were themselves considering moving to the cloud in 2011. According to NIST, clouding computing is:

> A model for enabling ubiquitous, convenient, on demand network access to shared pool of configurable resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (Mell and Grance 2011)

"It is important," writes Mosco, "that cloud-computing descriptions, however objective in appearance, are typically conflated with promotion. … The goal is to promote the cloud and not just understand it" (2014, pg. 18). For example, along with its definition of cloud computing, NIST itself introduces awe into its definition of cloud computing—even a degree of panic—to stimulate swift adoption of cloud computing by introducing it as an unquestionable and optimistic inevitability, a streamlining necessity the U.S. government simply cannot operate without. After NIST's definition, they add: "The cloud computing model offers the promise of massive cost savings combined with increased IT

agility. It is considered critical that government and industry begin adoption of this technology in response to difficult economic constraints" (NIST 2013).

It is notable that defining cloud computing is often coupled with selling and blindly adopting cloud computing. This builds discursive associations with the term that make the popular narrative disproportionately based on what marketing discourse refers to as value propositions. This is not a surprise considering that cloud computing "is generally viewed as the fastest-growing, or near fastest growing, segment of the IT sector, even though in 2012 it represented only 3 percent of all IT spending" (Mosco, 2014, pg. 17). Marketing is tasked with bringing the cloud to widespread awareness, and several circles of promotion (including commercial advertising, private research and consulting firm reports, worldwide technology forums, and trade shows) have disproportionately hyped up the seemingly sublime myth of cloud computing as a "transcendent force to solve the world's problems" (Mosco, 2009, pg. 9).

The pitch has been convincing enough that the U.S. government has required its agencies to adopt "cloud-first" policies for new IT deployments, a move propelled by the belief that cloud computing must become a central means of meeting its information-technology needs. This promotional campaign has fostered steady business relations and lucrative contracts with large American telecommunications companies, like IBM and Amazon (Mosco, 2009, p. 63). The Department of Defense has seen a strategic opportunity in the creation of a military cloud, which "began with a test case led by the National Security Agency, which gathers, stores, processes, and analyzes huge amounts of data," is "three times the size of the CIA," and "has one-third of total U.S. intelligence spending" (Mosco, 2014, pg. 70); this example proved that cloud computing enabled the

"NSA to meet its goals with greater security and at lower cost, thereby demonstrating the value of moving other government agencies to the cloud" (pg. 71). Of course, the series of NSA leaks published in June 2013 by the *Guardian* and *Washington Post* further revealed that the cloud-literate NSA, in order to meet its goals, had placed a legal stranglehold and gag order on American cloud computing providers' whose foreign and domestic in-house user data it had gained legal access to for national security purposes.

Cloud computing is slowly weaving itself into the social fabric through its widespread adoption by government, corporations, and individuals. Considering the NSA revelations and the function of surveillance, cloud computing can be approached as a fertile object of study to shed light on the complex sociopolitical and economic dimensions of surveillance in contemporary technoculture.

Research Questions

Considering (1) the sociopolitical and economic dimensions of surveillance established in the literature, (2) what the NSA revelations suggest about the actual dynamics of contemporary state surveillance, and (3) what cloud computing symbolizes as a widely adopted technology affected by the NSA revelations, two research questions guide this paper's thematic inquiry into the post-Edward Snowden press coverage of American cloud computing providers (considered after June 6, 2013). A particular focus was placed on Google as an exemplar of the American cloud computing industry:

RQ1: Considering the established sociopolitical and economic functions of surveillance, how does "post-Snowden" popular press coverage of Google's cloud computing services discursively address and construct cloud computing themes?

RQ2: How are these sociopolitical and economic themes positioned alongside other unanticipated themes in post-Snowden popular press coverage of Google's cloud computing services, and how are those themes constructed discursively?

Methodology

Critical Discourse Analysis & The Grounded Theory Approach

To answer adequately RQ1 and RQ2 this paper will engage in a Critical Discourse Analysis (CDA) that explores the naturalization of discursive assumptions and the processes that make particular discursive themes appear self evident and legitimate in popular press coverage of the NSA revelations and their effect on Google cloud computing. Since RQ1 anticipates finding sociopolitical and economic themes in the popular press coverage (considering these are established functions of surveillance), and RQ2 anticipates locating unanticipated themes alongside sociopolitical and economic ones, the CDA coding will be conducted with the aid of a grounded theoretical approach.

The grounded theory approach is highly compatible with CDA because it encourages a process of discovery in which coding categories develop though an ongoing constant-comparative method that allows and accounts for dynamic coding changes when novel or independently unique data alters the coding process and analytic framework. The grounded theory approach further compliments CDA by allowing researchers to produce deeper meanings out of the codes by encouraging integration (acknowledging connections between codes) and dimensionalization (identifying attributes, properties and characteristics of codes) to help theoretically saturate the coding process. Conducting CDA with a grounded theory approach will provide data to answer RQ1 and RQ2 that will also allow for a reasoned, traceable construction of interpretive claims.

Data Sampling

Considering the NSA revelations as a discursive event that began with the first leaks on June 6, 2013, which marks the post-Snowden era of press coverage which is still continuing just over a year later in the summer of 2014 (the time this paper was written), it is important to consider Post-Snowden popular press coverage from a variety of different materials written by different stakeholders. This CDA will be a diachronous, multi-layer discourse analysis across four discourse layers each of which have the "authority" to "speak" on the topic and add up to enough material for analysis for the purposes required by RQ1 and RQ2. The term "discourse layer" refers to the assumption that discourse about a complex event occurs in multiple discursive areas or fields, and these complex discursive phenomena require analysis of multiple textual layers of material culture to understand how different stakeholders construct them (Spitzmuller and Warnke, 2011).

Within each discourse layer, fifteen discourse strands (coding categories) were identified using the grounded theory approach mentioned above. This created a living coding legend through evolutionary coding that iteratively evolved from theoretical considerations into an operational list based on empirical data as the material was coded. For example, a popular discourse stand in this CDA was *Loss of profit for American cloud computing as a result of the NSA revelations.* This discourse strand became a distinct coding category because it hosted an economic, numbers-driven conversation about the material, measurable effects of the NSA revelations on corporate profits. The entire data sample was closely examined several times as codes that appeared later in the coding process affected how earlier material would and could be coded. Full sentences were coded as discourse fragments. Each sentence was highlighted with the respective code

colour to which it belonged, to be tallied and grouped upon coding completion. The discourse layers and the total materials looked at within each layer were:

1. Investigative News (2 sources, 10 articles each)
2. Technology Commentary (6 sources, 10 articles each)
3. Google Public Relations Statements (10 articles each)
4. NSA Public Relations Statements (10 articles each)

Total: 100 articles from 8 sources

1. Investigative News

Sources: *The Guardian, Washington Post*

For the purposes of this CDA, the Investigative News discourse layer considered investigative journalism from traditional daily newspapers that have historically had a function and responsibility to inform the public in order to contribute to healthy discourse in the public sphere in the most Habermasian (1962) sense of that term. The two sources that were chosen from which to sample data were the first two Investigative News sources that published the leaked NSA slides on June 6, 2013 and thereby initiated the discursive event known as the post-Snowden era. This paper and the ongoing global debate the NSA revelations have spurred are indebted to *The Guardian*'s Glenn Greenwald and *Washington Post*'s Barton Gellman and Laura Poitras, all of whom had the courage to meet with Edward Snowden himself in Hong Kong at Snowden's request in the months prior to June 2013 and the bravery to push the limits of journalism (particularly in our corporate-media-dominated era) by publishing these shocking government leaks. The data to be coded in the Investigative News discourse layer was found by entering the search query "nsa google cloud computing" in each source's search engine on their respective websites.

2. Technology Commentary

Sources: *TechCrunch, Wired, InfoWorld, Spider Oak, The Atlantic, Global Post*

Alongside Investigative News, Technology Commentary is considered a genre of popular press discourse that discusses technology and is dedicated not only to delivering timely news about technological innovation, but also takes it upon itself to provide sound social commentary on the social, political, and economic implications of technological innovation. Established news, tech business, and lifestyle publications have contributed thought leadership and influential contemporary technoculture analysis, and their word is generally accepted as emblematic of popular, authoritative knowledge and commentary about the current state and future of technology.

The sources within this discourse layer were found by entering the search query "nsa google cloud computing" into the Google search engine. The top 10 hits that were commentary-focused websites and not Investigative News or self-published statements by Google or the NSA were examined, and within those websites the search query was again inputted to comprise the data sample per source in this Technology News discourse layer. Websites that were top hits after being searched on Google but failed to provide 10 relevant sources (having the search terms embedded in the article itself and not as secondary or commercial content on the periphery of the webpage) were eliminated from the sample and the next Google hit was visited. Considering that Google's Search Engine Optimization (SEO) algorithm is a closely guarded secret with results often changing per day, per search query, per user, and per geographic area, it is important to note the sources that comprise the data sample in this discourse layer were collected in early June of 2014 in Toronto, Ontario while logged in under my personal Gmail account. Six sources were

chosen to comprise 60 articles in order for the grand total of articles to be 100 articles, a manageable and adequate sample for one coder.

3. Google Public Relations Statements

Though Google has made several statements directed to the sources within the Investigative News and Technology Commentary discursive layers, it has also published its own content on its own platforms in order, as a form of crisis communication, to address the discursive event according to their own point of view and in support of their own corporate motives. In fact, the bulk of Google's statements have been responses to journalists within the previously mentioned discourse layers; they have conspicuously published only a handful of pieces on their own publishing platform to address the NSA / cloud computing / Snowden issue directly. Because ten sources could not be found from one Google publishing platform alone, three were visited to comprise this discursive layer:

1. Google Public Policy Blog
2. Google Transparency Report
3. Google Blogspot Blog

Within this discursive layer the same "nsa google cloud computing" search query was used.

4. NSA Public Relations Statements

Like Google, the bulk of the NSA's ongoing statements during the NSA revelations continue for the most part to operate as direct answers to the questions of individual press outlets, with only a handful of useful statements related to the "nsa google cloud computing" search query being found in the NSA press room. Because ten useful sources containing the search terms could not be found from one single NSA publishing platform alone, four NSA digital properties were visited to comprise this discursive layer:

1. NSA's Press Room
2. NSA's Public Information Page
3. Icon The Record (Official Tumblr Blog for the Director of National Intelligence)
4. Department of Justice Press Room

The same "nsa google cloud computing" search query was used within each

Coding Categories

Below are the final fifteen coding categories that resulted from the constant comparative evolutionary coding method adopted throughout the data sample. Each code is accompanied by a brief description to justify its existence as an independent discourse strand and is accompanied by an example of a typical discourse fragment that would comprise the category.

Figure 1: Coding Legend of Discourse Strands

	Coding Categories	Description	Example
1.	Loss of profit **f**or American cloud computing industry as a result of the NSA Revelations	An economic, numbers-driven conversation about the material, measurable effects of the NSA revelations on profit	*"Another report by the Information Technology and Innovation Foundation suggested that the surveillance revelations could cost the U.S. cloud-computing industry $22 to $35 billion in lost revenues over the next three years."*
2.	Loss of consumer confidence and perceived security in the American cloud computing industry as a result of the NSA Revelations	A focus on the reputational, symbolic damage American cloud computing providers must mitigate with existing and potential customers	*"Some US companies said they have already lost business, while UK rivals said that UK and European businesses are increasingly wary of trusting their data to American organisations, which might have to turn it over secretly to the National Security Agency, its government surveillance organisation."*
3.	Confirming or adding credence to the digital sublime and myth around cloud computing	Statements that support marketing value propositions about the inevitability and convenience of cloud	*"At the end of the day, the capabilities and economics around the cloud computing model are so compelling that when you artificially try to not take advantage of them you*

		computing services	*impact your ability to compete, because others will take advantage of them."*
4.	Outright denial or lack of corporate and government transparency about details about their revealed cooperation	Statements that obfuscate or deny the capabilities of the NSA-tech relationship	*"They couldn't fully deny the charges without disclosing certain classified details, and the only affirmative statements they could make had to be cleared with the government first, which ultimately led to all of the companies issuing statements that included curiously similar phrasing, further fuelling paranoia."*
5.	American cloud computing experiencing success despite NSA revelations	Economic statements that engender consumer confidence in cloud computing with proof of the industry's continued resilience and necessity	*"Explosive revelations in the past six months about the U.S. government's massive cyber-spying activities have spooked individuals, rankled politicians and enraged privacy watchdogs, but top IT executives aren't panicking -- yet."*
6.	Confirming that the NSA and technology companies are complicit in a surveillance operation	Statements that without doubt acknowledge the existence of a relationship between the NSA and technology companies for the purpose of surveillance	*"The fact is that Google, Facebook, Yahoo, Amazon, Apple and Microsoft are all integral components of the US cyber-surveillance system. Nothing, but nothing, that is stored in their 'cloud' services can be guaranteed to be safe from surveillance or from illicit downloading by employees of the consultancies employed by the NSA"*
7.	Negative criticism of mass surveillance, the surveillance state and American spying powers	Sociopolitical statements negatively framing the NSA and the clandestine surveillance activities it is complicit in	*"The White House is also battling to respond to growing unrest over surveillance of citizens by the state and the vast caches of data many digital giants are now storing about individual consumers."*
8.	Explicit calls for reform, transparency, accountability to NSA-corporate cooperation	Rallying statements that directly address the need for or provide evidence of reform to NSA spying	*"In a bid to calm growing privacy concerns about the government's spying powers, President Obama outlined a series of steps Friday aimed at ushering in "concrete and substantial" reforms to the National Security Agency."*
9.	Technical details	Statements that explore	*"Section 702 of the Foreign*

	about NSA spying programs, including PRISM, MUSCULAR, Boundless Informant, XkeyscoreNSA under the Foreign Intelligence Surveillance Act (FISA) Court	the mechanics of various internal NSA spying programs	*Intelligence Surveillance Act allows the government to collect information on foreign targets that are, to use its own language, 'reasonably believed to be outside of the U.S. at the time of data collection.' It can't target United States persons by law, and it isn't allowed to reverse-target—picking a foreign target with the hopes of picking up the communications of someone thought to be in the United States."*
10.	The NSA revelations have altered the state of the Internet with social, political, economic consequences	Sociopolitical and economic statements that address the effect the NSA revelations have had on the democratic function of the Internet	*"Decisions made about cybersecurity operations will have massive repercussions not only for our immediate defense interests, but the how we and other countries treat cyberspace."*
11.	The NSA revelations hurt American foreign diplomatic relations	Statements that address the strain the NSA revelations have had on American political power	*"European officials and politicians have reacted furiously, with some saying the revelations may harm efforts that began this month to negotiate a transatlantic free trade zone, a high foreign policy priority for the Obama administration."*
12.	Individual, corporate, and government resistance to NSA spying	Statements that explore how individuals, corporations, and foreign governments have countered NSA spying	*"Since the Guardian's revelations about the scale of state surveillance, Brazil's government has published ambitions plans to promote Brazilian networking technology, encourage regional internet traffic to be routed locally, and is moving to set up a secure national email service."*
13.	Critical, self-reflexive reporting about NSA reporting	Statements that reflect on the NSA narrative itself, condemning popular reporting	*"If there were enough experts with the time, inclination, ability, and independents to write fluently and enjoyably for a general audience, there would be no need for journalists as informational middlemen."*
14.	Justification or minimization of	Statements used to legitimize and assert the	*"The NSA's activities are 'focused and specifically deployed against –*

	NSA spying techniques and capabilities	continuation of NSA spying	*and only against – legitimate foreign intelligence targets in response to requirements that our leaders need for information necessary to protect our nation and its interest."*
15.	Human interest coverage about Edward Snowden	Statements that provide detail about Edward Snowden's experience	*"The New York Times contributed a deep profile of Snowden himself, who continues to provoke strong reactions, especially after he revealed some details about U.S. spying on China and Russia."*

It is important to keep in mind that the manner in which each discursive layer constructs and approaches each discourse strand can be vastly different, and therefore identifying how each discursive layer constructs the established economic and sociopolitical functions of surveillance as discourse strands, central to RQ1 and RQ2, can change with each discursive layer. Though the constant-comparative evolutionary coding method helped to theoretically saturate the data sample by establishing discourse strands as codes with legitimate and isolating thematic boundaries, the discursive fragments that comprise different discourse strands in different discourse layers can tell different—even conflicting—stories about the same theme. For example, Code #7 deals with negative criticism about the surveillance state and American spying powers; it may be constructed much differently by Google's PR Statements, which are operating in a reactionary and reputation-saving capacity and may halt the theme's possible political permutations with simple statements merely condemning NSA surveillance, while Investigative News, which ideally operates in a public interest capacity, may act as a theoretical space intended for the nuanced debate of the pros and cons of surveillance in contemporary society. In other words, in this paper the four discursive layers may paint much different pictures of the discourse strand despite using the same codes.

It is worth repeating that the discourse strands in Figure 1 have in fact been constructed through constant comparison and their existence as codes is mostly prescriptive of the type of conversation happening within the code. The differences between the layers mentioned above act as deviations that will in fact enrich the discussion. Having said that, the layer-specific discussions based on the findings will account for these deviations by acknowledging which codes provide answers to RQ1 and RQ2 while providing the necessary meta-commentary to justify focusing on them.

Coding Method and Analysis Technique

The data sample was coded using Microsoft OneNote, a note-taking software laden with technological affordances that allowed for all the articles within each discourse layer to be coded appropriately and edited retroactively as constant-comparison mandates through color coding. Notably, color-coding the discourse strands also afforded the coder the ability to conduct a high-level examination of the structural thematic features of each article at a glance, since the colors signified which discourse strands had an overwhelming or dominant presence, which discourse strands were conspicuously omitted, and which discourse strands seemed to reappear in complimentary patterns together. Having these preliminary feelers established a deep familiarization with the discourse strands in each layer and prepared the coder well for subsequent analysis.

After the constant-comparative coding process was complete and the data sample had been saturated with distinct and unique codes, each of those codes, within their respective discourse layer, was collected and the sentences were counted. This revealed the percentages of each discourse strand within each discourse layer compared to others,

while also revealing quantifiable macro-features of the data sample. The documents from which these numbers were gleaned—the discourse layer-specific documents with the individual discourse strands grouped together—also proved to be a qualitative resource which was used to investigate how each discourse layer constructed each discourse strand.

These qualitative documents allowed for the discovery of more nuanced meanings to emerge about the findings that were discovered within the quantitative results. A variety of micro-analysis techniques were used to accomplish this deeper analysis, which involved zooming in on individual fragments and identifying the function of cultural references, intertextuality, framing devices, and linguistic and rhetorical mechanisms such as word groupings, metaphors, grammar features, modalities, and common-sense statements. These techniques were used to examine what realities were being discursively legitimized and naturalized through language and rhetoric.

In keeping with the mandates established by RQ1 and RQ2, these techniques were used to identify at the micro-level how sociopolitical and economic themes (RQ1) were constructed alongside other unanticipated themes (RQ2) in Post-Snowden popular press coverage of American cloud computing provider Google, considering the anticipated economic and sociopolitical functions of surveillance established in the literature. Knowledge from the macro structural features and the micro fragments was combined with the broader context established in the literature review. Alongside the literature review, the analysis and discussion portion of this paper has been bolstered by recent commentary on our surveillance society in Glenn Greenwald's *No Place To Hide* (2014) and Vincent Mosco's *To The Cloud: Big Data in a Turbulent World* (2014).

Limitations

CDA is a form of content analysis that cannot claim to make fully transparent what people think or believe as a prescriptive effect of the content it is examining. This paper does not claim to harbour insights as to what public opinion *is* regarding the NSA revelations and their effect on cloud computing. Rather, this paper uses CDA to examine with a certain degree of confidence what kinds of statements certain actors or stakeholders surrounding the discursive event try to establish as self-evident and true, what rhetorical methods they chose to communicate those truths in ways that they thought would be effective, plausible, and even natural, and how their statements and frameworks proliferate through (online) communication (Schneider 2013).

Having said that, it is important to understand that CDA invites and encourages a substantial degree of subjective interpretation by the coder in designing the codes and analyzing them. The chance of full replication of the results and study is therefore understandably low. Despite this, being transparent about the ways the codes and themes were created engenders confidence and external validity to this CDA. The subjectivity of the coder can in fact be regarded as an asset that contributes methodologically grounded empirical research to the discourse while allowing for a degree of subjective interpretation and commentary. It is important to repeat the fact that the discursive event being examined in this study is a product of government secrecy, as such truth claims are avoided in favour of describing the arguments and statements that exist in the discourse itself.

Further, it is important to note the limitations that result from the unique time and place this paper was written. These limitations were alluded to in the data sampling

section, which acknowledged that the articles gathered through Google's search engine were available partly because of this paper's unique location and time interacting with fluctuating search engine optimization (SEO) techniques and Google's own ranking algorithms. More generally, it is important to acknowledge that this paper was written in Canada approximately one year after the Snowden revelations, and novel information relevant to a Canadian audience post July 2014 has not been included in the analysis.

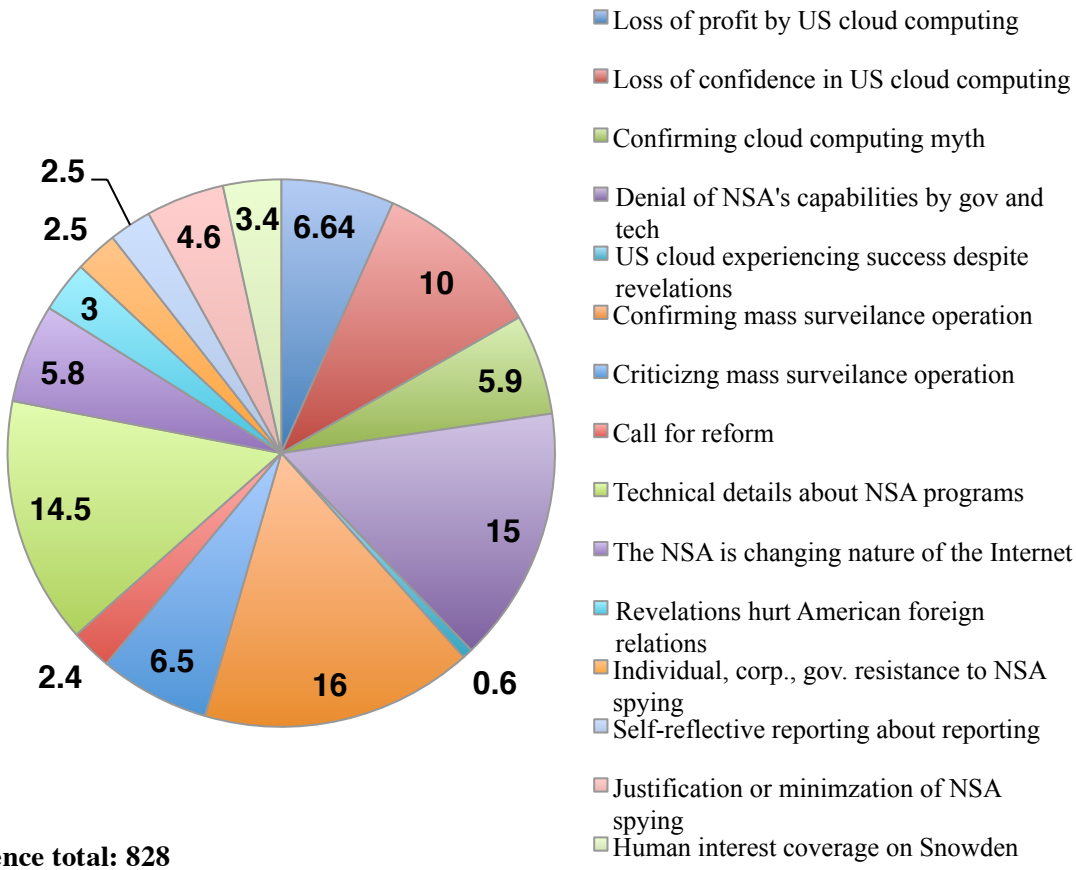
Findings and Discussion

This section will present the findings of the CDA and then discuss the findings within the CDA framework. It will achieve this by visiting the data from each discourse layer in two parts: 1) it will present a pie chart showing each code's presence in the discourse layer as a percentage of the total number of sentences in the layer (specified in the chart itself); and 2) it will discuss the key takeaways in the discourse layer, involving a micro-examination of discursive statements and the discursive truths being made, if necessary. The discussion will be developed in accordance with RQ1 (How are economic and sociopolitical themes constructed discursively in the discourse layer?) and RQ2 (How are unanticipated themes constructed alongside economic and sociopolitical themes in the discourse layer?). The layer-specific discussions will then be harmonized into a final discussion in the following section, all to be informed by the literature review.

For purposes required by data visualization, the detailed codes as described in Figure 1 will be presented in a summarized form in the accompanying legend of each pie chart. If necessary, please refer to Figure 1 for a detailed description of the codes while reading the pie charts.

DISCURSIVE LAYER #1: INVESTIGATIVE NEWS

Figure 2A: Coding Totals for Investigative News (Pie Chart)



Sentence total: 828

Figure 2B: Coding Totals for Investigative News (Table)

1	Loss of profit by US cloud computing	6.64%
2	Loss of confidence in US cloud computing	10%
3	Confirming cloud computing myth	5.9%
4	Denial of NSA's capabilities by gov and tech	15%
5	US cloud experiencing success despite revelations	0.6%
6	Confirming mass surveillance operation	16%
7	Criticizing mass surveillance operation	6.5%
8	Call for reform	2.4%
9	Technical details about NSA programs	14.5%
10	The NSA is changing the nature of the Internet	5.8%
11	Revelations hurt American foreign relations	3%
12	Individual, corp., gov resistance to NSA spying	2.5%
13	Self reflective reporting about reporting	2.5%
14	Justification or minimization of NSA spying	4.6%
15	Human interest coverage on Snowden	3.4%

As a discourse layer, Investigative News is unique because it is constituted by a romanticized legacy of public service. The purpose of Investigative News can be regarded as a utopian one: to contribute to a vibrant and healthy public sphere by stimulating rational and informed debates through objective news reporting. Considering that the literature establishes that understanding the sociopolitical and economic dimensions of surveillance in contemporary society is vital, and that exploring these effects is significant, it was surprising but understandable to find that the majority of the content in this discourse layer did not pay attention to the anticipated themes outlined in RQ1 as much as it focused on the revelations about the NSA and Google by zeroing in on *what* this spying mechanism actually was, *how* it worked, and *who* was involved in it (rather than the broader socio-cultural-economic effects these revelations entail). In short, the major finding of this discursive layer is that sociopolitical and economic conversations that considered the effects of the NSA revelations were present but eclipsed by unanticipated narrative-driven themes in the coverage, which mostly focused on establishing the discursive event from a variety of stakeholder opinions (considered in RQ2). Figure 3 includes a breakdown of which codes dealt overwhelmingly with economic themes and sociopolitical themes (RQ1), and which codes were the result of unanticipated themes that proved to be narrative-driven coverage communicating what the NSA revelations were, how they worked technically, and who was involved (RQ2). This figure will be repeated for each layer:

Figure 3: Thematic Code Summary for Investigative News

	Codes	Total Percentage*
Economic Themes (RQ1)	1, 2, 3, 5, 8, 12	28%
Sociopolitical Themes (RQ1)	7, 10, 11, 14	20%
Unanticipated Themes (RQ2)	4, 6, 9, 13, 15	52%
*Percentages have been rounded up to full decimal point		100%

Anticipated Themes (RQ1)

Codes Hosting Economic Surveillance Conversations

Codes covered*:*

- *1. Loss of profit*
- *2. Loss of consumer confidence*
- *3. Confirming the cloud computing myth*
- *5. US cloud computing experience monetary success despite revelations*
- *8. Call for reform*
- *12. Individual, corporate, government resistance to NSA spying*

Admittedly, the presence of economic framing in the Investigate News discourse layer was smaller (28%) than anticipated, considering the standard search query ("NSA Google cloud computing") in each discourse layer was chosen to isolate news that affected the cloud computing industry specifically. However, despite its relatively small presence, an exploration of the codes that contributed to the economic framing reveal a story that overwhelmingly demonstrates the negative effects the NSA revelations will have on future projected revenues and consumer confidence in the American technology industry more generally. Notably, negative economic framing also makes room for positive economic framing about Google and American cloud computing despite the revelations. Positive economic framing within the layer asserts the power, responsiveness, and inevitability of American cloud computing providers who use the NSA revelations as an opportunity to disassociate from the perceived crisis by positioning themselves as advocates of the people against NSA spying (which other codes suggest they are deeply complicit in).

Although negative economic news has a disproportionately larger percentage within the frame, a spectrum emerges from negative to positive economic framing that is worth examining.

Loss of profit (6.64%) and *loss of consumer confidence* (10%) are negatively economically framed codes that take up the majority of economically-framed content. These codes are laden with references to various consulting firms who project a substantially undermined U.S. cloud computing industry because of international and domestic wariness of U.S. technology companies, which face a projected loss of $21.5B to $35B in cloud computing contracts worldwide over the next three years. A substantial loss of that business will be lost to European rivals, which have experienced a surge in clients who are purchasing based on strict requirements that the geographic location of the cloud computing provider's servers be outside of US legal jurisdiction, according to the most frequently cited study by the Information Technology and Innovation Foundation. The notion that the U.S.-dominated cloud computing industry was shot in the foot by the NSA revelations is an oft repeated observation; in other words, a market set to double in size over the next three years to $200B and considered a massive future revenue generator for the American economy had been jeopardized.

The story within this negative framing is colonized by the logic of public relations and crisis communication and follows the trajectory of the usual mediated corporate crisis: some event has led to a negative paradigm shift in consumers' minds about a product which has in turn put revenue at risk and this negative perception must somehow be changed to save revenue. The problem here becomes how to approach global skepticism about U.S. cloud computing in a way that engenders confidence in them and encourages

them to open their wallets. It is the opinion of this paper that defining the issue within a PR framework is an exercise in purposeful obfuscation which confuses the cause of the issue for its economic effects. The facts are that the NSA has legally subordinated US technology companies to comply with its spying activities by requiring their unbridled cooperation with its own mandates. Further, US national integrity and security cannot be maintained without infiltration of the private data that has been accumulated by, and belongs to, U.S. technology companies—in other words, the NSA seeks to shed light, and in turn extend, the surveillant assemblage (Haggerty and Ericson 2002).

In this light we are better able to understand the codes that positively frame and represent cloud computing despite such harrowing leaks. Two codes in particular, *Confirming the cloud computing myth* and *US experiencing monetary success despite the revelations,* deliver on the economic need to portray cloud computing positively even during a global scandal and crisis. These codes tell a story about the continued value of investment in cloud computing. Op-ed pieces that mention the revelations tout cloud computing's convenience for personal data retrieval, while technology gurus gush about 1) its ability to cut internal energy costs by outsourcing servers offsite, 2) that it is in fact better at storing data than local hard disks, 3) that it is becoming the backbone of the contemporary American workplace, and 4) that it cuts costs related to maintaining internal IT departments. This discourse is invested in portraying Google, Microsoft, and Amazon as experiencing international growth, and cites consulting firms which claim companies will, despite the NSA revelations, see $788 billion in cloud services over the next four years, and that cloud services will have a positive impact of $1.7 trillion to $6.2 trillion a year by 2025. Gillmore's (2013) op-ed exemplifies this opinion that confirms the

usefulness of cloud computing despite the revelations: “I fear, in any case, that we’ve become so accustomed, even addicted, to the easy-to-use convenience of Google and its peers that not enough of us will opt for genuine privacy.”

The codes *Call for reform* and *Individual* and *Corporate, government resistance to NSA spying* were anticipated to be sociopolitical ones, but rather they have been hijacked within the PR framework by the U.S. tech companies to distance themselves from the scandal by using these codes as rallying calls to state their vehement disapproval of and measurable actions against NSA spying, despite evidence of their mandatory participation in that spying. These codes are considered economic because they serve to promote the reputation and image of the tech companies involved to win back consumer confidence, like Google’s decision to beef up encryption of the data moving between its own data centers the NSA was accused of infiltrating and Google, Apple, and Facebook’s public letters calling for substantial reforms, not to mention publicized meetings between technology CEOs and President Obama about program reforms (Eilperin, 2013). The story here is focussed on giving Google and other technology companies the opportunity to define themselves against NSA spying by allowing them to speak about the manner in which they have added security—peace of mind—and value to their own services while omitting how individuals and governments who are subject to this surveillance mechanism can resist politically. This legitimizes a certain kind of politics that bolsters confidence in U.S. cloud computing despite the scandals and “economizes” conversations that have the potential to be about sociopolitical digital resistance.

Codes Hosting Sociopolitical Surveillance Conversations

Codes covered*:*

- *7. Criticizing mass surveillance*
- *10. The NSA is changing the nature of the Internet*
- *11. Revelations hurt American foreign relations*
- *14. Justification or minimization of NSA spying*

It was unanticipated for sociopolitical themes to only comprise 20% of the Investigative News discourse layer, however the content within each code was anticipated considering the sociopolitical function of surveillance as established in the literature. The codes *Criticizing mass surveillance, The NSA is changing the nature of the Internet,* and *Revelations hurt American foreign relations* explicitly deal with the effects of the surveillant assemblage and each harbour conversations that critically assess what empirical effects will be felt in our networked world as a result of the leaks. This body of discourse explores how the NSA revelations have spurred intense negative sentiment to the American government from its own people and citizens worldwide whose daily online interactions with U.S. tech companies could position them as suspicious adversaries of government policies and programs.

The code *The NSA is changing the nature of the Internet* refers to the implication that the NSA revelations will lead to a "balkanization" of the Internet as countries like Brazil and Germany, whom the leaks reveal were targeted by the NSA and who plan to build their own national Internet infrastructures resulting in less global and more localized islands of online information. That is, Internet balkanization could result in information that was once retrievable from anywhere being housed on one country's server's alone, forcing cloud companies to set up individual shops within nations. This threat of Internet balkanization has been a blow to American foreign relations, particularly with Germany

and Brazil, who abhor the profoundly invasive and alienating surveillance practices of the U.S. and who have vocalized their desire to loosen the US's grip on Internet governance, infrastructure, services, and control.

The code *Justification or minimization of NSA spying* counteracts these critical sociopolitical sentiments by recalling tested and ideologically bulletproof 9/11 rhetoric in order to legitimize NSA spying. They are made almost entirely by NSA spokespeople responding to the news outlets directly, and reside on the opposite end of the critical debate that the other codes in the sociopolitical framework construct. In fact, these statements seem to be used to ensure the existence of current power relations by claiming NSA spying saves US lives from a variety of terrorist threats, and that in fact the NSA is a force for good as a tool for identifying and eliminating those with intent to harm the security of Americans. These justifications are bolstered by assertions that the warrants required by the NSA to initiate surveillance are in fact legal and by extension that the entire surveillance operation is legitimized. It is important to note here that this conversation is a reassertion of power and a perpetuation of the existing social order.

Unanticipated Themes (RQ2)

Codes covered:

- *4. Denial of NSA's capabilities by government and technology*
- *6. Confirming mass surveillance operation*
- *9. Technical details about NSA spying programs*
- *13. Self-reflective reporting about NSA reporting*
- *15. Human interest coverage on Snowden*

Sociopolitical and economic conversations that considered the effects of the NSA revelations were present but eclipsed by unanticipated narrative-driven themes in the coverage, which took up 50% of the sample and mostly focused on establishing the

discursive event from a variety of stakeholder opinions (considered in RQ2). This is understandable considering the information within the leaks was a complex and disruptive government leak that needed to be understood by the news outlets themselves before the public was informed and much before a broader analysis could be performed. A significant amount of news coverage had to be devoted to actually describing what the NSA was, what the spying mechanism it was accused of practicing was doing, how NSA spying worked technically, and who was involved. In other words, the news outlets had to establish and reiterate what was going on before having an opportunity to host a meaningful and informed discussion about the broader sociopolitical and economic effects of this discursive event.

Though it is neither within the scope nor the purpose of this paper to describe the NSA revelations nor debate their validity, it is necessary to engage the popular narrative about the revelations as they determine the unanticipated themes mandated by RQ2 in all layers.

The discourse generally agrees that the NSA has several spying programs of which PRISM has been the most controversial and relevant to Google's cloud computing services. Leaked slides about PRISM claim the NSA has direct access to the servers of Google and Yahoo. When asked about PRISM, the NSA states that it makes use of authority granted to it by Congress in 2008 under the Foreign Intelligence Surveillance Act (FISA) under section 702, which forces technology companies to turn over user data as demanded by easily obtainable warrants that can be granted by secret FISA courts. The NSA claims that these warrants are targeted at suspected foreign targets only and are not sweeping dragnets on domestic and international users of American technology companies; however, these claims are challenged by the fact that leaks about the

MUSCULAR program contain information the NSA intercepted from the private clouds or internal networks of Google and Yahoo that are not found on the consumer-facing side of the Internet. They are also challenged by faulty definitions of what constitutes a foreign target, and how easily available FISA warrants are for the NSA. The slides leaked by Snowden, in other words, reveal that the NSA has infiltrated privately owned fiber optic cables that Yahoo and Google use as secure, private highways for professional and user data, cables that are available only to these companies for the purpose of unbridled government spying alongside the legalized formalized structure PRISM exploits.

Further slides show that the NSA has developed Google-specific protocol-handlers or hackers that are dedicated to decrypting Google's encrypted proprietary data traveling between its international data centers to capture internal server-to-server communication (Gellman, Soltani, & Peterson, 2013). This upstream data collection falls under the spying program named MUSCULAR, and is particularly threatening to Google's cloud computing services because it demonstrates that essentially all of the data that Google houses and moves internally is susceptible to surreptitious, warrantless NSA spying. This information is particularly unsettling considering Google and Yahoo's cloud network services often transmit entire data archives from one data center to another. Alongside PRISM, MUSCULAR has been a problematic leak because the program exploits links between technology companies' international data centers and therefore operates outside of American law in a legal (or extra-legal) no man's land. Together, MUSCULAR and PRISM have affected Google and the cloud computing industry specifically because the leaks describe in detail the total back-and-front door infiltration by the NSA into the company's servers and the digital technology industry writ large.

The narrative established in the anticipated sociopolitical and economic codes within this discourse layer contradicts with the layer's unanticipated, narrative-driven codes by technology companies and the U.S. government. Both companies and government vehemently deny the capabilities of the clandestine spying program and their involvement in it despite the story Snowden's leaks suggest. In statements within the layer, technology companies initially deny ever having heard of PRISM and then later admit to a forced cooperation they condemn and from which they seek to disassociate. MUSCULAR, on the other hand, is always met with fierce denial by Internet companies. These statements are best typified by Google's own statements and will be examined in the Google Public Relations Statements discourse layer

In the NSA's statements the agency repeatedly denies it has the capabilities that the slides suggest it does, while insisting on the morality and legality of the programs, which they say have been gravely misunderstood by the news outlets reporting on them. The NSA also uses these press opportunities to further mystify the leaks and assert its power by two repeated strategies meant to ensure discursive closure: first, they claim that they cannot in fact clear up the narrative they assert is misinformed because it will question the effectiveness of those programs, and second, and by extension, that these programs are a response to the tragedy of 9/11 and should therefore not be questioned or fully explained in the press since they preemptively protect the American people from tragedies like 9/11 from ever happening again. The rhetorical strategies herein shall be examined further in the NSA Public Relations Statements discourse layer.

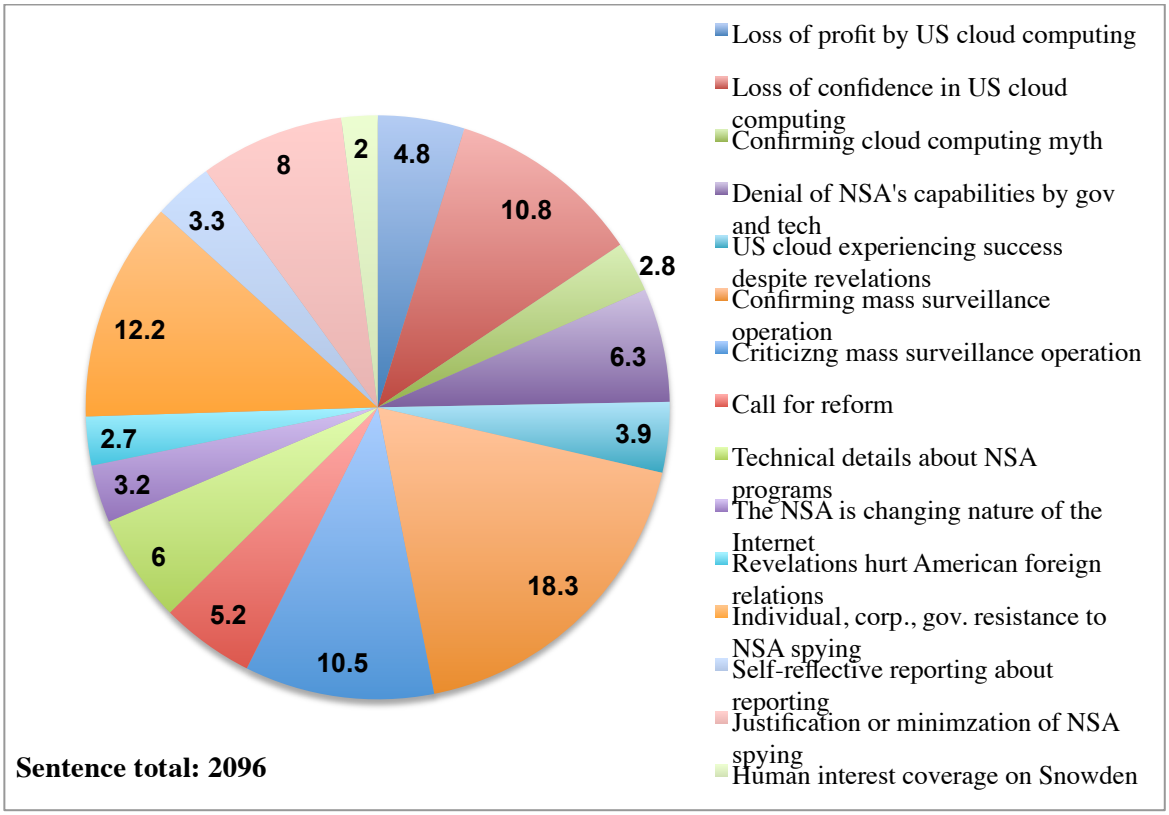
It is notable to observe in unanticipated themes, which do not discuss the sociopolitical and economic role of surveillance, that they comprise the fundamental building blocks of

these necessarily broader, effect-driven discussions that must occur after those blocks have been set. A discursive event of this magnitude shakes the foundation of an ostensibly democratic and law-abiding society invested in the Internet and computer mediated communication; however, how that discursive event is constructed in popular discourse, which this paper tries to summarize, is necessary to examine because it prescribes the future conversations about its broader effects by naturalizing certain narratives and interests with which that event will later be discussed.

Companies like Google have woven themselves into the very fabric of everyday life in the networked world and they utterly rely on their ability to store massive amounts of data and sell that data to advertisers. When news about the misuse of that data is revealed, whole social and cultural practices, economies, ways of sharing and creating information, and modes of political engagement, can be fundamentally altered, and the degree of these alterations needs to be acknowledged in popular press coverage to enrich popular understanding and inform the public. Though themes that comprise RQ2 eclipsed more specific themes sought out by RQ1, the sizeable presence of anticipated themes found by RQ1 within the Investigative News discourse layer suggests that nuanced, effect-driven conversations about the NSA revelations do in fact matter to the Investigative News discourse layer; however, these conversations could not be hosted within the Investigative News discourse layer until the discursive event had been fully established.

DISCURSIVE LAYER #2: TECHNOLOGY COMMENTARY

Figure 4A: Coding Totals for Technology Commentary (Pie Chart)



Sentence total: 2096

Figure 4B: Coding Totals for Technology Commentary (Table)

1	Loss of profit by US cloud computing	4.8%
2	Loss of confidence in US cloud computing	10.8%
3	Confirming cloud computing myth	2.8%
4	Denial of NSA's capabilities by gov. and tech.	6.3%
5	US cloud experiencing success despite revelations	3.9%
6	Confirming mass surveillance operation	18.3%
7	Criticizing mass surveillance operation	10.5%
8	Call for reform	5.2%
9	Technical details about NSA programs	6%
10	The NSA is changing the nature of the Internet	3.2%
11	Revelations hurt American foreign relations	2.7%
12	Individual, corp., gov resistance to NSA spying	12.2%
13	Self reflective reporting about NSA reporting	3.3%
14	Justification or minimization of NSA spying	8%
15	Human interest coverage on Snowden	2%

Figure 5: Thematic Code Summary for Technology Commentary

	Codes	Total Percentage*
Economic Themes (RQ1)	1, 2, 3, 5, 8, 12	40%
Sociopolitical Themes (RQ1)	7, 10, 11, 14	24%
Unanticipated Themes (RQ2)	4, 6, 9, 13, 15	36%
*Percentages have been rounded up to full decimal point		100

Anticipated Themes (RQ1)

Codes Hosting Economic Surveillance Conversations

Themes covered:

- *1. Loss of profit by US cloud computing*
- *2. Loss of confidence in US cloud computing*
- *3. Confirming the cloud computing myth*
- *5. US cloud experiencing success despite revelations*
- *8. Call for or evidence of reform*
- *12. Individuals, corporate, government resistance to NSA spying*

It is not a surprise that this discourse layer had the majority of its coverage be about the economic effects of the NSA revelations on the cloud computing industry and Google. Though this discourse layer is a hub of thought leadership on the state of technology and covers technology from many aspects, as an industry-based news source its focus on the NSA revelations as a discursive event is revealed in the substantial presence of economic framing within the discourse layer Economic conversations here stayed largely within the boundary of monetary loss and reputational risk from domestic and international consumers of American cloud computing providers. Economic conversations also included debates that assert the resilience, inevitability, and utility of American cloud computing; these positively framed economic conversations praised how cloud computing has "fought back" against NSA spying and engendered lost consumer confidence with value-added encryption features. Interestingly, the code that hosted these positively framed economic conversations (*Corporate, individual, and governments resistance to*

NSA spying) has within it the capacity to be a space for sociopolitical action and solidarity against NSA spying. In the Technology Commentary discourse layer, political interpretations of resistance were hijacked by economic interpretations of resistance that confirmed US cloud computing power, signaling how deeply embedded the success of the US technology economy is into the fabric and security of the US.

The narrative in these codes is as follows: the NSA revelations have created a fallout in the US cloud computing industry among domestic and international customers who are turning to non-US providers. As a result US providers must alter their cloud pitch to these customers in order to rekindle their confidence and refill pocketbooks while still dealing with the uncomfortable truth that the NSA still continues to have access to their data. The NSA's repeated statement that it only targets foreigners serves to further undermines US technology companies because these companies are oriented internationally and the majority of their customers are not US citizens. The fear is reinforced by grim predictions by consultants and private research firms about the potential loss of cloud computing revenue to overseas companies as a result of the leaks, ranging from $22 billion through 2016 to $35 billion, with some predictions as high as $180 billion (Staten, 2013).

As a result of these developments, once comparatively tiny search engines like DuckDuckGo and Ixquick that do not collect data from users have experienced a surge in usage, with DuckDuckGo searches rising from 1.8 million searches per day to 3 million searches per day the week of the NSA revelations, and Ixquick rising from 2.8 million searches/day to more than 4 million. Ixquick has notably launched an email service with accounts so secure the company itself cannot get into them without permission from the user. The provider charges a premium fee for these account which reflects users'

willingness to pay for more or less guaranteed privacy. This "privacy premium" foreshadows the ongoing commodification of privacy as it becomes an essential market differentiator, luxury item, and prized value proposition by cloud providers worldwide—particularly US ones.

Despite Technology Commentary's foreboding predictions for future cloud computing revenue, it is imperative to note how Technology News also uses economic framing to justify a positive economic future for cloud computing as it responds to the threats the revelations pose. Economic framing in this discourse layer asserts the power and ingenuity of US cloud computing as something businesses simply couldn't live without, extending value-laden language into the elevated realm of the mythical and the digital sublime. Though small in presence, positive economic conversations within the Technology Commentary discourse layers works to bolster the impression that the US cloud computing industry is experiencing success and seek to perpetuate the message that the cloud computing industry is an unstoppable force in technology, one that even a public relations blow like the NSA revelations cannot slow down.

American hegemony within the global technology industry is asserted implicitly according to a narrative in the Technology Commentary discourse layer that contradicts the grim prediction of codes which host negative economic effects of the revelations on US cloud computing, particularly with the repeated mentions of new cloud business in China alongside the growing market share of global cloud services within IT every year. Positive economic framing about US cloud computing despite the revelations compliments consistent positive statements about Google that asserts how the company has been particularly difficult to infiltrate by the NSA. As a global computing power that

largely subsists on advertising revenue and therefore troves of consumer data it sells to advertisers, the Technology Commentary discourse layers argues that it is in Google's best interest to protect cloud user privacy from government snooping and to maintain cutting-edge security. Failing to engender consumer confidence in their services will hurt Google's ability to sell their data to their primary spies and customers: their advertisers. As corporate transparency grows, Google will likely respond to the NSA revelations with descriptions of value added encryption services to win back lost confidence and advertising dollars.

Alongside positive economic framing touting marketing successes, it is important to acknowledge the confidence this layer has in cloud computing and the way its rhetoric elevates cloud computing to a sublime-like level. A valid rhetorical trap has been made in cloud computing marketing communications that claims that the move to the cloud has hugely compelling benefits to companies who by moving their data to the cloud can avoid the costs that come with running servers on their own premises. These benefits and capabilities of cloud computing are so appealing that avoiding adoption of the cloud while competitors reap its benefits will – the logic goes – impact a business' ability to compete. The NSA revelations, and security, merely become factors in a risk / reward assessment matrix that Chief Information Officers are forced to weigh. If the numbers signal a rise in profit by moving to the cloud, short-minded corporate logic uses that conclusion to trump fear of government snooping—a truth that has given innovative US cloud computing providers leverage despite the Snowden leaks and made cloud computing ongoing momentum. The promise of economic benefits supersedes concerns regarding spying, making cloud computing the ideal technology to propel the surveillant assemblage into the

future as a critical backbone of US economy and security. The myth of cloud computing suggests a mutually beneficial technology for business and government, which sprouts and shoots like a rhizome over the economic, political, and social field.

Codes Hosting Sociopolitical Surveillance Conversations

Themes covered*:*

- *7. Criticizing mass surveillance operation*
- *10. The NSA is changing the nature of the Internet*
- *11. Revelations hurt American foreign relations*
- *14. Justification or minimization of NSA spying*

Despite its relatively small presence in this layer, sociopolitical themes critical of NSA spying were powerful in the Technology Commentary discourse layer. With of course the exception of the *Justification or minimization of NSA spying* code, which serves only to reify and reproduce pre-existing realities that benefit the NSA, the sociopolitical codes critical of NSA power were acknowledging the broader political, social, diplomatic ramifications of the NSA's actions and the US government's oversight in allowing such abuses of power to continue unchecked. The conversation within codes that hosted sociopolitical surveillance conversations condemned the extreme social cost of the NSA's strong hold on corporate actors, the extreme concentration of power in the US, the very significant reality that Google is cooperating with the federal government to blackmail and arrest any ideological dissidents in and outside US borders, how whistleblowers are treated in a supposedly democratic state, the financial interests of organizations like Booz Hamilton which benefit from the expansion of the surveillance state, the negative effects of Foucauldian panoptic surveillance, and the blurred distinctions between liberty and security in American society. Compared to the Investigative News layer, the Technology

Commentary layer accomplished significantly more in terms of contributing sociopolitical criticism to the body of popular discourse about the NSA revelations.

The criticism within the codes that host sociopolitical surveillance conversations even claims that the technology companies' publicized crusade against NSA spying is a well-orchestrated PR move to disassociate the companies from government spying because, in the opinion of civil liberties advocates, Google and US tech companies, who make profit off the commodification of their users, want to be the exclusive spying source for consumer data. News of the NSA sharing in that spying, albeit for different purposes, negatively affects the successful primary purpose of that commercial spying. Again, it is interesting to note how companies routinely become flag bearers of sociopolitical criticism of NSA spying when they themselves are in fact hijacking those themes under economic motivations and pretenses.

Economic motivations for the discussion of sociopolitical themes continue as the Technology Commentary discourse layer discusses how the Internet has changed as a result of the revelations. Like the Investigative News layer, the Technology Commentary layer focuses the conversation on how the repercussions of the NSA revelations have altered the state of the Internet as a communication medium into a conversation about its balkanization by countries who wish to break away from what has been revealed to be an American-run Internet. Theoretical debates about the use of the Internet as a communication medium for citizens are acknowledged, but framed in such way where the topic of the Internet being split into isolated, country-specific islands hurts US economic interests and therefore its global political power. Sociopolitical interests are consumed by and become the fuel for economic interests as non-US countries threaten to engage in data

hoarding, posing a disruption to the current distribution networks of major US tech players.

Individual users may pay the price in future hypothetical situations where they are in a foreign nation and are denied access to their data because it is not housed where they are—the antithesis of what the Internet and the cloud mean today. Countries are exerting pressure on international companies like Google to set up servers for their countries within their borders out of anger, with significant leverage over their large, networked populations. These sentiments are shared particularly among Germany and Brazil, and even the United Nations, who the NSA has spied on for diplomatic and economic purposes.

Unanticipated Themes (RQ2)

Codes covered*:*

- *4. Denial of NSA's capabilities by gov. and tech.*
- *6. Confirming mass surveillance operation*
- *9. Technical details about NSA programs*
- *13. Self reflective reporting about NSA reporting*
- *15. Human interest coverage on Snowden*

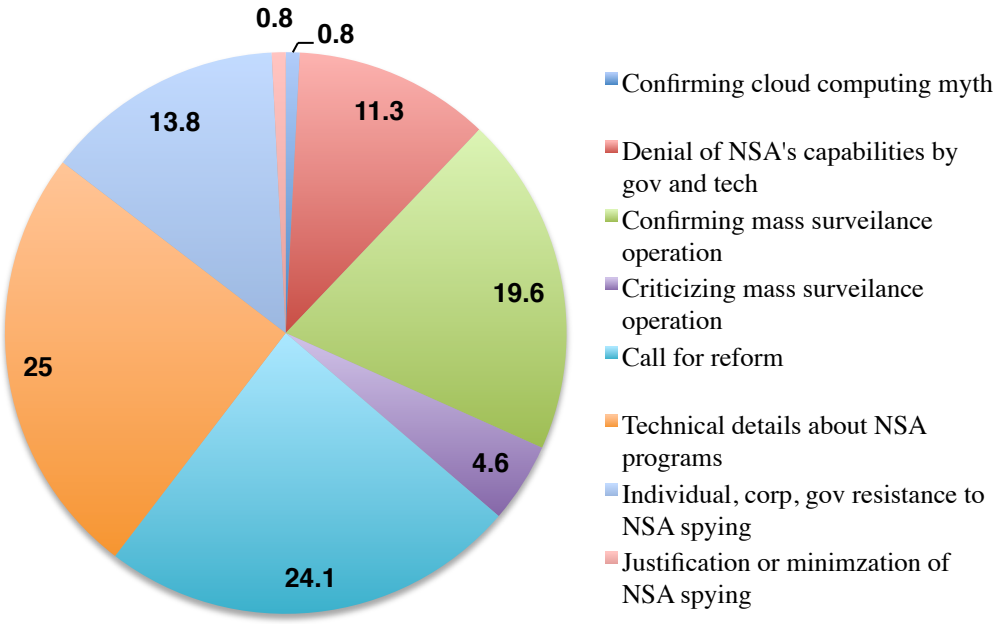
Like the Investigative News layer, unanticipated themes as sought for in RQ2 were focused on establishing the discursive event in the same way: outlining the problem, its technical details, and the stakeholders responsible. Differences in the construction of the narrative were found to be negligible, since the majority of the narrative was explicitly cited from the Investigative News discourse layer that established it.

Perhaps most notably, these themes were only covered in 36% of the Technology News discourse layer compared to 52% in the previous Investigative News discourse layer. This number adds credence to the quality of the major findings about the anticipated

themes in Technology News (RQ1), since it is not necessarily the job of technology news to publish breaking government leaks despite their intimate relationship to and knowledge of the contents of those leaks. As the discourse layer shows, the creation of that narrative occurred within traditional news outlets, and discursive layers like Technology News were afforded the privilege of time to digest the narrative traditional news outlets established in order to begin publishing broader effect-driven conversations about those narratives.

DISCURSIVE LAYER #3: GOOGLE PUBLIC RELATIONS STATEMENTS

Figure 6A: Coding Totals for Google Public Relations Statements (Pie Chart)



Sentence total: 240

Figure 6B: Coding Totals for Google Public Relations Statements (Table)

1	Loss of profit by US cloud computing	0
2	Loss of confidence in US cloud computing	0
3	Confirming cloud computing myth	0.8%
4	Denial of NSA's capabilities by gov. and tech.	11.3%
5	US cloud experiencing success despite revelations	0
6	Confirming mass surveillance operation	19.6%
7	Criticizing mass surveillance operation	4.6%
8	Call for reform	24.1%
9	Technical details about NSA programs	25%
10	The NSA is changing the nature of the Internet	0
11	Revelations hurt American foreign relations	0
12	Individual, corp., gov resistance to NSA spying	13.8%
13	Self reflective reporting about NSA reporting	0
14	Justification or minimization of NSA spying	0.8%
15	Human interest coverage on Snowden	0

Figure 7: Thematic Code Summary for Google Public Relations Statements

	Codes	Total Percentage*
Economic Themes (RQ1)	3, 8, 12	36%
Sociopolitical Themes (RQ1)	7, 14	5%
Unanticipated Themes (RQ2)	4, 6, 9	56%
*Percentages have been rounded up to full decimal point		100

Discussion

Anticipated Themes (RQ1)

Codes Hosting Economic Surveillance Conversations

Codes covered*:*

- *3. Confirming the cloud computing myth*
- *8. Call for reform*
- *12. Individual, corporate, government resistance to NSA spying*

The NSA revelations posed a significant risk to Google's reputation and revenue. Its legal complicity in the US government's spying efforts made it a primary stakeholder in the crisis among other major US technology firms in the leaked Snowden slides. As the discussion for RQ2 in the Investigative News discourse layer revealed, programs like PRISM and MUSCULAR affected Google's cloud computing services in particular because, as reported, those programs together claimed to have unbridled access to Google's servers which their cloud computing services live on. Google had been aware of PRISM through years of FISA warrants, but MUSCULAR had signified the NSA had infiltrated Google's servers unscrupulously for indiscriminate data collection.

As a result, Google's statements entered into crisis mode as they began to disassociate themselves from the crisis to compensate for a perceived loss of confidence and potential lost revenue in its cloud services. Interestingly, however, Google produced few statements on its own platforms about the topic, with the majority of their statements being individual responses to news outlets. Since mitigating reputational damage is considered to have

economic motivations, economic framing in this discourse layer almost exclusively focused on codes that distance Google from the crisis at the expense of other economic codes in the data sample. The codes in question that were most popular in the Google Public Relations Statements discourse layer were *Call for reform* and *Corporate resistance to government spying.* Within these two codes is a similar conversation that speaks to the lengths to which Google went to insist upon its negative feelings towards NSA spying, and what they have done to battle the NSA on behalf of their users. Through strategic use of collective pronouns and the second person, the Google Public Relations Statements discourse layer requires the audience to assume Google is on their side as Google leverages its power as a stakeholder in the crisis to become an advocate for the public within that crisis. The rhetorical shift allows for a pivot in Google's positioning within the crisis. This is critical for image rehabilitation and is grounded in the need to create an overall perception that Google is fighting to keep its user data from the prying eyes of the government—but not advertisers.

Google accomplishes this on its own platforms largely by describing the lawsuit it filed demanding the ability to disclose the number of FISA requests it received, including how many users and accounts those requests included. Google in fact won the lawsuit which, in turn, enabled Google to begin publishing the Google's Transparency Report (a document that remains subject to indefinite publishing delays imposed by the Department of Justice). Google further distances itself from the NSA by describing the continued and deliberate obfuscation by the government regarding the manner in which it can report numbers of NSA data requests and users affected, which bans Google from revealing how

many accounts were in fact impacted by a surveillance request in favor of how many requests occurred.

Google describes and forms opinions about a host of legal documents and reforms, such as: 1) the USA Freedom Act, which would make in depth transparency reports much more accessible to users from all companies whose data is used for US national security demands; and 2) the Electronic Communications Privacy Act (ECPA) of 1986, which Google criticizes as an outdated piece of legislation that fails to reflect how the Internet is used today and that provides the major loopholes government agencies use to begin legal processes that compel companies to disclose information. Google also describes working with civil liberties advocacy groups, like the Digital Due Process Coalition lobby, to petition for the reform of the ECPA to ensure for these reforms. The company even vocalizes its disapproval of the existence of FISA, and advocates for the abolition of secret courts altogether in a democratic society.

Google claims to resist government requests for data through their ability to narrow the scope of the requests they receive by objecting to subpoenas and warrants presented to it by citing its internal policies. For example, the company repeatedly boasts that in 2006 they were the only major search company to refuse a US government request to hand over two months worth of user search queries. The company also claims to add transparency to these requests when they do happen by notifying the targets through their Gmail accounts, unless they have been legally prohibited to do so, alongside mandatory HTTPS encryption on all e-mail messages, which the audience is led to believe is somehow beyond the NSA's hacking capabilities. It is not difficult to see Google's claims to resistance are

haphazard and unconvincing. In fact, these claims can be read as confirmations of the US government's absolute power and control over the company's data.

Codes Hosting Sociopolitical Surveillance Conversations

Codes covered:

- *7. Criticizing mass surveillance operation*
- *14. Justification or minimization of NSA spying capabilities*

It is important to note that sociopolitical themes in this discourse layer were eclipsed by or omitted in favor of economic themes because Google has an economic interest in this crisis and a significant portion of its communication about this crisis was done as an exercise in disassociation and image rehabilitation. Since the crisis itself involved government spying for the purposes of national security, it is also important to note that traditionally sociopolitical themes, such as calls for reform of FISA courts and condemnations of larger breaches of legal power, were hijacked by economic framing and used as evidence by Google to prove its disassociation from the crisis through its technical abilities and moral judgment of the crisis.

Having said that, Google hosts a conversation about the challenges the NSA revelations have posed for surveillance and secrecy, by presenting the dangers surveillance poses for societies that rely on transparent and informed public debate. They iterate a quite noble position, that "the levels of secrecy that have been built up around national security requests undermine the basic freedoms that are the heart of a democratic society" (Page, 2014), alongside an unwavering belief in the need for transparency and public understanding about how surveillance laws work to benefit the public. However, alongside challenging NSA power, Google also confirms it when they claim that "national security and transparency for the public are not in competition" while somehow also claiming that

they "hope governments around the world will follow the lead of the US government and be more transparent about the national security demands they serve on service providers" (Page, 2014). These statements are incompatible with their more critical statements and signal that Google's dual audience for these statements, the government and its own users, have competing and seemingly incompatible interests.

Unanticipated Themes (RQ2)

Codes covered*:*

- *4. Denial of NSA's capabilities by gov and tech*
- *6. Confirming mass surveillance operation*
- *9. Technical details about NSA programs*

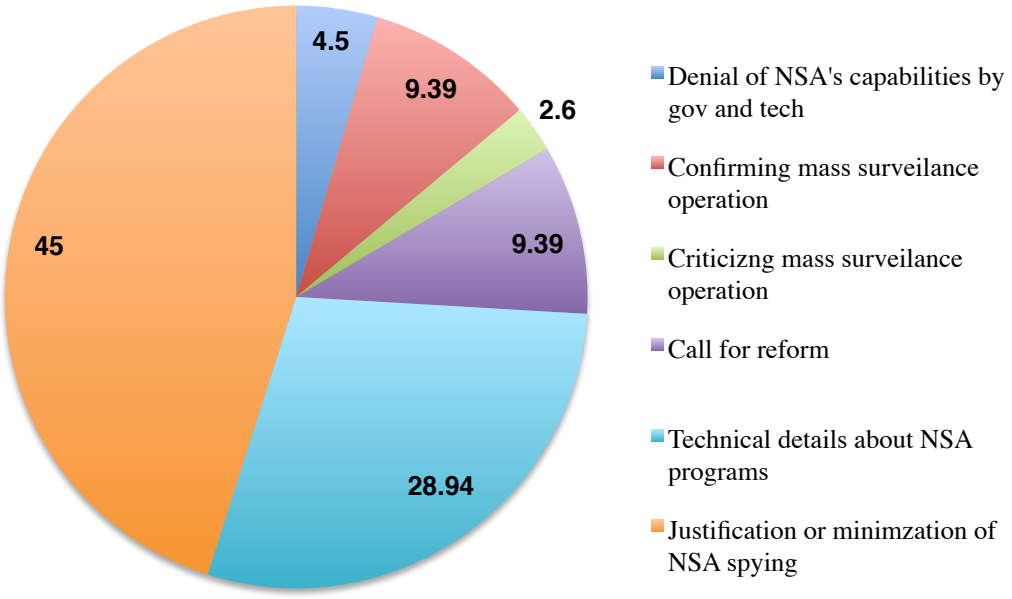
Since Google was positioned as a stakeholder in the crisis, it is unsurprising that the majority (56%) of this discursive layer's content had to do with unanticipated, narrative-driven themes in which Google constructed the discursive event it was deeply implicated in on its own terms. Google's confirmation of the mass surveillance operations is largely identical to the story told by the other discursive layers, despite the fact that Google's storyline focuses on a description of PRISM, which it claims to had never heard of by name. Google's story is that it provides user data to the government through legal FISA court orders, which it is unhappy with but legally compelled to do, and Google has done all it can to seem as transparent about those requests as possible despite the gag orders government nondisclosure agreements demand.

Google's denial of the NSA's capabilities is perhaps the most interesting conversation hosted within the Google Public Relations Statements since it has been accused of granting or standing idly by the NSA's back door access to its servers. Google categorically and vehemently denies this sort of back door access, saying that it is simply

not true, period. Interestingly, no mention is ever made of other insidious programs that have led the press to speculate about back door access, particularly MUSCULAR, which is conspicuously absent from Google's narrative and which, as reported in other layers, is entirely disruptive and incompatible with Google's official narrative about the NSA revelations.

DISCURSIVE LAYER #4: NSA PUBLIC RELATIONS STATEMENTS

Figure 8A: Coding Totals for NSA Public Relations Statements (Pie Chart)



Sentence Totals: 266

Figure 8B: Coding Totals for NSA Public Relations Statements (Table)

1	Loss of profit by US cloud computing	0
2	Loss of confidence in US cloud computing	0
3	Confirming cloud computing myth	0
4	Denial of NSA's capabilities by gov. and tech.	4.5%
5	US cloud experiencing success despite revelations	0
6	Confirming mass surveillance operation	9.39%
7	Criticizing mass surveillance operation	2.6%
8	Call for reform	9.39%
9	Technical details about NSA programs	28.9%
10	The NSA is changing the nature of the Internet	0
11	Revelations hurt American foreign relations	0
12	Individual, corp., gov resistance to NSA spying	0
13	Self reflective reporting about NSA reporting	0
14	Justification or minimization of NSA spying	45%
15	Human interest coverage on Snowden	0

Figure 9: Thematic Code Summary for NSA Public Relations Statements

	Codes	Total Percentage*
Economic Themes (RQ1)		0
Sociopolitical Themes (RQ1)	6, 7, 8, 9, 14	86%
Unanticipated Themes (RQ2)	4	14%
*Percentages have been rounded up to full decimal point		100

Anticipated Themes (RQ1)

Codes Hosting Sociopolitical Surveillance Conversations

Themes covered*:*

- *6. Confirming mass surveillance operation*
- *7. Negative criticism of mass surveillance*
- *8. Call for reform*
- *9. Technical details about NSA spying programs*
- *14. Justification or minimization of NSA spying powers*

It is important to note that this discourse layer housed no economic framing as an anticipated function and theme of surveillance coverage established in the literature. As a government agency whose purpose it is to defend the nation's safety through intelligence gathering, it is expected that the NSA met the crisis with its own framing of the discursive event in terms of political necessity and sociopolitical benefit. Sociopolitical framing's overwhelming percentage in the discourse was comprised of a denial of the capabilities the NSA had been accused of, a minimization of the danger of the spying mechanisms it was in fact capable of, and the majority of the NSA rhetoric justified the NSA's existence and role as a spying agency.

Interestingly, the codes *Call for reform* and *Negative criticism of mass surveillance,* codes that were used by the Technology Commentary and Google's Public Relations Statements to deeply criticize and disassociate themselves from the crisis, were also

present in the NSA's statements as responses to the negative criticism existing in these other layers, but are used to dissolve and erase those criticisms by appealing to issues of national security. *Confirming the mass surveillance operation* and *Technical details about NSA spying programs,* codes that appeared as unanticipated themes for the sole purpose of creating the discursive event in other layers, was in this layer considered to be framed socio-politically because the NSA's confirmation and explanations of its spying activities were inseparable from those activities' sociopolitical purpose: "The NSA's activities are focused and specifically deployed against – and only against – legitimate foreign intelligence targets in response to requirements that our leaders need for information necessary to protect our nation and its interests" (NSA Press Room, 2014).

Citing the fear of terrorist threats and therefore their ability to intercept and prevent them, the NSA becomes rhetorically bulletproof in a string of logic that preys on and rekindles fears of 9/11 to justify its surveillance activities and ideology. The NSA, in other words, creates a discursive world in which its ideological interests are valid and its existence seems necessary. The fact that popular press coverage has widely debated whether the NSA's pursuit of national security interests has become mutually exclusive with civil liberties has been profoundly disruptive to the NSA, which reconciles this disruption through asserting confidence in the checks and balances of American governance. The Office of the Director of National Intelligence's Tumblr page, which aims to provide the public with direct access to lawful foreign surveillance activities carried out by the US, made this statement about the NSA's impetus and behaviour:

> The NSA's challenge in an increasingly interconnected world–a world where our adversaries make use of the same communications systems and services as Americans and our allies–is to find and report on the

> communications of foreign intelligence value while respecting privacy and civil liberties. We do not need to sacrifice civil liberties for the sake of national security – both are integral to who we are as Americans. NSA can and will continue to conduct its operations in a manner that respects both. We strive to achieve this through a system that is carefully designed to be consistent with Authorities and Controls and enabled by capabilities that allow us to Collect, Analyze, and Report intelligence needed to protect national security. (icontherecord.tumblr.com, 2014)

The NSA and the US government attempt to instil further confidence in their spying programs by siding with their most critical voices and confirming that there should be a call for more accountability. Notably, on May 23, 2013 President Obama addressed the nation calling for the immense need for reform and transparency in the intelligence agency in the wake of the revelations, despite the NSA's repeated statements that transparency of its programs would dissolve their efficacy to maintain national security and therefore could never be realized. The major reform that resulted from President Obama's reform speech was the end of the NSA housing data from the Section 215 Bulk Telephony Data Program—the first NSA program that *The Guardian* and *Washington Post* revealed on June 6, 2013. Rather than housing telephony data themselves, the NSA now allows the telecommunications providers to hold that data while ensuring "a mechanism that preserves capabilities we need without the government holding this bulk data" (icontherecord.tumblr.com, 2014). By claiming the NSA has ensured a mechanism that preserves the capabilities it needs to get what it wants from telecommunication providers, it takes the audience little effort to understand that this act of reform is anything but. Ironically, this reform, which is supposed to check NSA power, in fact extends that power because it mystifies these news mechanisms that ensure the NSA can access that data it wants. Now that the companies hold the data, it is implied that the NSA can access that data however it wishes—an uncomfortable change considering the known capabilities

of programs like MUSCULAR. Like Technology Commentary and Google's PR Statements, NSA PR Statements seem to hijack the theme of reform and transparency for self-serving purposes and self-legitimization in a manner that asserts and even extends their own power.

Unsurprisingly, the codes *Justification or minimization of NSA spying* (45%) and *Technical details about NSA programs* (28.94%) together made up almost three-quarters of the total discourse in this layer. As the NSA became implicated in a crisis that exposed intimate details about its secretive operations, the agency took time to lock down the narrative that it claims has misrepresented the agency's programs and motivations. By citing that the US government's intelligence agencies had failed to connect the dots to prevent the attacks of 9/11 because of a lack of surveillance tools, the NSA justifies its existence and technical prowess as described in the leaks as an appropriate response to 9/11, which makes taboo morally questioning the activities of the US government. The NSA cites its collection arsenal as the most important tool for the "detection, identification, and disruption of terrorist threats to the US and around the world," like the 2009 capture of Colorado-based Najibullah Zazi as he travelled across the US to meet co-conspirators to conduct a terrorist attack on the NYC subway system (icontherecord.tumblr.com, 2013).

Though these justifications grossly contradict prior statements by the NSA that claim its spying activities occur wholly outside the US, the NSA assumes its audience would not connect the dots about this slip in favour of the wave of relief they will feel knowing the NSA has the capacities to thwart a would-be terrorist attack. The implication

here is that foreign intelligence requirements for the purpose of national security require very fluid definitions of foreignness, and counterterrorism measures occupy a moral high ground so untouchable that all activities done in their name are lawful. As such, the NSA seeks to dissolve prior criticisms of its surveillance goals being contradictory to the goals of civil liberties by conflating them: through the pursuit of national security via surveillance, the NSA in fact allows for the existence of liberty – it does not squash it! This rhetorical slight of hand is absolutely necessary to legitimize the NSA; it is a reframing that requires the unquestionable defense of the physical security of the nation to supersede and overshadow, even redefine, all other facets of life that goal seems to impinge upon.

Unanticipated Themes (RQ2)

Codes covered:

- *4. Denial of NSA capabilities*

As mentioned above, the previous layers housed unanticipated codes that established what the discursive event was, what its technical details were, and who was involved. In the NSA Public Relations Statements discursive layer, the NSA framed its story largely socio-politically, citing national security in an attempt to establish a grand, official narrative of the NSA revelations.. Having said that, *Denial of NSA capabilities* took up a small portion of the unanticipated, narrative-building themes in this discursive layer because the code consisted of sentences acknowledging and denying the verity of the claims made by the press about the NSA's programs as simply not true, inaccurate, or misinformed. These statements do nothing to establish the narrative, but rather deny the

truthfulness of the stories told in other discursive layers. In the discussion above, it is shown how the NSA absorbs narrative-building codes into anticipated socio-political framing.

Conclusion

Langdon Winner argued that artefacts have politics (1980). To him, human created technologies do not exist in a value-neutral vacuum, but are inscribed with the social values of the period that created them. Moreover, human values enter the social fabric as embodiments of those values, confirming and reproducing them. It can be difficult to see technologies as being laden with ideological values, as being legitimizations of very politicized ways of life, because our technologies are laden with values that have become naturalized and taken for granted. It often takes a disruptive event to uncover these ideological assumptions and even more interrogation to lay them bare. The NSA revelations were a profoundly disruptive discursive event that allowed for the widespread interrogation of several interconnected facets of the networked world. Lifting a curtain on a clandestine US surveillance operation that implicated US technology companies and the entire Internet, the NSA revelations and Snowden leaks necessitated the investigation of the power relationships between the US government and cloud computing companies. The particularly strong presence of American technological superpower Google's cloud computing services within those leaks proved to be a valid object of study that allowed this researcher to begin to uncover the ideological assumptions inscribed in cloud computing technology by examining the surveillance context of the NSA revelations in popular press coverage.

This paper conducted a multi-layer critical discourse analysis (CDA) to interrogate which conversations were present about Google's cloud computing services as a result of the NSA revelations, considering the anticipated economic and socio-political functions of

surveillance as established in the literature (RQ1). Alongside those anticipated themes, this paper also accounted for unanticipated themes that did not explicitly deal with the anticipated socio-political and economic functions of surveillance, and were instead narrative-building themes devoted to establishing the NSA revelations as discursive events, describing their technical details, and identifying major stakeholders and their responsibilities within the discursive event (RQ2). A grounded theory approach that involved a constant-comparative evolutionary coding method afforded fluidity between codes to travel from RQ1 to RQ2 and across each discourse layer depending on how the discursive layer constructed each code.

As a profoundly disruptive discursive event, the ongoing NSA revelations have reverberated and continue to reverberate in several areas or layers of public discourse. The discussions for the four discursive layers investigated in this CDA (Investigative News, Technology Commentary, Google Public Relations Statements, NSA Public Relations Statements) reveal how different stakeholders in the discursive event define the NSA revelations and describe their nuanced implications in accordance with their institutional motivations and perceived rhetorical ownership over the issue.

The Investigative News discourse layer broke the story about the NSA revelations and within that layer, unanticipated, themes serving to establish the narrative eclipsed more nuanced, socio-political and economic conversations about surveillance. Having said that, the layer did host a variety of critical economic conversations about the damages to the reputation and profit of US cloud computing as a result of the leaks. Alongside these negative economic conversations, the Investigative News discourse layer gave the

technology companies involved in the NSA revelations the opportunity to speak and disassociate themselves from the crisis to mitigate their own reputational damage. These economic conversations eclipsed socio-political conversations in the discourse layer, which prioritized economic and narrative-driven themes to establish the event and its tangible, economic implications before offering theoretical conversations about the NSA revelations' democratic or socio-political consequences.

The discourse layer I describe as Technology Commentary, as a hub of thought leadership in the technology industry, built on the narrative established in the Investigative News discourse layer and hosted more effects-driven conversations about the socio-political and economic implications of the NSA revelations. Generally, this layer disproportionately focused its effects-driven themes on economic conversations about mitigating the damage to the reputation and profit of cloud computing providers as a PR issue. Economic conversations showcased how cloud computing providers and Google were battling NSA spying by giving technology companies a platform to speak about value-adding encryption services. These conversations effectively hijacked conversations about the NSA revelations to showcase the new features cloud computing companies provided. Socio-political conversations about the balkanization of the Internet were also framed as threats to US technological hegemony. Commentary further focused on bolstering the mythological dimension of cloud computing: first, by asserting explicitly that the promise of profit via corporate adoption of cloud computing trumps the fear of privacy, and second, by implying that cloud computing is a growing backbone of the US economy and US national interests.

Naturally, Google's PR Statements almost exclusively focused on economic framing, taking the opportunity to define the crisis while compensating for the perceived loss of confidence and revenue in all of its services as a result. Google also took the opportunity to associate itself with negative criticism of the NSA as a strategic move to disassociate from the crisis and associate with critics of it, even positioning itself as an advocate for its users against NSA power. On the other hand, the NSA housed no economic framing and framed all of its communication about the revelations by citing their absolute necessity for the maintenance of national security. Interestingly, the NSA even acknowledged the topic of reform and transparency in its services, but did so in a haphazard way that reinforced its own powers, ideological interests, and necessity for the maintenance of US integrity.

Notably, within each discourse layer, truly critical socio-political conversations as anticipated by the literature were generally omitted, underrepresented, poorly explored, or hijacked by economic framing. The strong presence of economic framing in the data sample signals the economic significance the NSA revelations have had on the US cloud computing industry. It also demonstrates how important it was for popular press coverage within the US to acknowledge the crisis and to begin addressing it symbolically based on economic motivation to maintain US technological dominance. The general omission of socio-political themes also signifies that this dimension of cloud computing is not as significant to popular press coverage as economic effect-driven conversations.

Despite the different amounts of coverage for both socio-political and economic themes in each discourse layer, the substantial presence of both socio-political and

economic framing alongside unanticipated, narrative-building themes among the data sample about the NSA revelations and cloud computing points to the complex, symbiotic relationship socio-political and economic conversations have when discussing US national security, ideological interests, and economic integrity. It also signifies the complicit role telecommunications companies play in the pursuit of national, ideological, and economic security in so far as they serve as the data troves on which this security depends.

References

Albrechtslund, A., & Glud, L. N. (2010). Empowering Residents: A Theoretical Framework for Negotiating Surveillance Technologies. *Surveillance & Society*,*8*(2).

Bauman, Z. (1991). *Intimations of postmodernity*. Routledge.

Bowker, G. C., & Star, S. L. (2000). *Sorting things out: Classification and its consequences*. The MIT Press.

Cohen, S. (1985). *Visions of social control: Crime, punishment and classification* (p. 10). Cambridge: Polity Press.

Dandeker, C. (1990). *Surveillance, power and modernity: Bureaucracy and discipline from 1700 to the present day* (pp. 117-18). Cambridge: Polity.

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

Deleuze, G., & Guattari, F. (1987). A Tousand Plateaus. *Trans. BRIAN MASSUMI. Minneapolis: Te University of Minnesota Press*.

Foucault, M. (1980). *Power/knowledge: Selected interviews and other writings, 1972-1977*. Random House Digital, Inc.

Gellman, B., Soltani, A., & Peterson, A. (2013, November 4). How we know the NSA had access to internal Google and Yahoo cloud data. Retrieved August 25, 2014, from http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/

Goffman, E., & Helmreich, W. B. (1961). *Asylums: Essays on the social situation of mental patients and other inmates* (Vol. 277). New York: Anchor Books.

Galloway, A. R. (2004). *Protocol: how control exists after decentralization*. the MIT press.

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

Lazzarato, M. (1996). Immaterial labour. *Radical thought in Italy: A potential politics*, 133-147.

Lyon, D. (2007). *Surveillance studies: An overview*. Polity.

Marx, G. T. (1989). *Undercover: police surveillance in America*. University of California Pr.

Nippert-Eng, C. E. (2010). *Islands of privacy*. University of Chicago Press.
Poster, M. (1990). *The mode of information: Poststructuralism and social context*. University of Chicago Press.

Scholz, T. (Ed.). (2012). *Digital labor: The Internet as playground and factory*. Routledge.

Staten, J. (2013, August 14). The Cost of PRISM Will Be Larger Than ITIF Projects. Retrieved August 25, 2014, from http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects

Tiessen, M. (2011). Being Watched Watching Watchers Watch: Determining the Digitized Future While Profitably Modulating Preemption (at the Airport).*Surveillance & Society*, *9*.

Winner, L. (1980). Do artifacts have politics? *Daedalus*, 121-136.

Yar, M. (2002). Panoptic Power and the Pathologisation of Vision: Critical Reflections on the Foucauldian Thesis. *Surveillance & Society*, *1*(3), 254-271.

Appendices

Appendix 1: Investigative News Sources

The Guardian				
	Author	**Title**	**Date Published**	**URL**
1	Arthur, Charles	Fears over NSA surveillance endanger US cloud computing industry: Companies say they could lose billions as customers become way about their data being turned over to US authorities	June 20, 2013	http://www.theguardian.com/world/2013/aug/08/nsa-revelations-fears-cloud-computing
2	Naughton, John	After Edward Snowden's revelations, why trust US cloud providers? The NSA's activities are a massive blow for US computer businesses.	Sept. 15, 2013	http://www.theguardian.com/technology/2013/sep/15/edward-snowden-nsa-cloud-computing
3	Garside, Juliette	Apple, Google and AT&T meet Obama to discuss NSA surveillance concerns: Silicon Valley companies concerned at effect on business as revelations over US government spying spread more widely	Aug. 9, 2013	http://www.theguardian.com/technology/2013/aug/09/nsa-surveillance-apple-google-obama
4	Rushe, Dominic	Apple, Facebook and Google call for 'substantial' reform of NSA surveillance: Firms call for 'substantial enhancements to privacy protections' and 'appropriate oversight' in letter to Senate committee	Oct. 13, 2013	http://www.theguardian.com/technology/2013/oct/31/apple-facebook-google-nsa-surveillance-reform
5	Taylor, Matthew	NSA revelations 'change how businesses store sensitive data': Survey suggests many firms choosing more secure forms of store over 'cloud computing' in light of Snowden's disclosures	March 31, 2014	http://www.theguardian.com/technology/2014/mar/31/data-storage-nsa-revelations-businesses-snowden
6	Gillmore, Dan	Embrace the cloud computing revolution--with caution: Google's Chromebook Pixel is the latest device pushing cloud data storage, but I'm not convinced it's safe enough	March 5, 2014	http://www.theguardian.com/commentisfree/2013/mar/05/cloud-data-revolution-google-chromebook-pixel
7	Gillmore, Dan	Google, Yahoo et al. have the power (and money) to fight back against the NSA: The tech billionaires should create the anti-surveillance, pro-security equivalent of the NRA	Nov. 1, 2013	http://www.theguardian.com/commentisfree/2013/nov/01/google-yahoo-nsa-surveillance-reform
8	Naughton,	Edward Snowden's not the story,	July 28, 2013	http://www.theguardian.com/t

	John	the fate of the Internet is: The press has lost the plot over the Snowden revelations. The fact is that the net is finished as a global network and that US firms' cloud services cannot be trusted		echnology/2013/jul/28/edward-snowden-death-of-internet
9	Greenwald, Glen and MacAskill, Ewan	NSA Prism program taps in to user data of Apple, Google and others: Top secret Prism program claims direct access top servers of firms including Google, Apple and Facebook. Companies deny any knowledge of program in operation since 2007	June 7, 2013	http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
10	Taylor, Matthew and Hopkins, Nick and Kiss, Jemina	NSA surveillance may cause breakup of internet, warn experts: Internet specialists highlight moved by Brazil, Germany and India towards creating separate networks to avoid spying	Nov. 1, 2013	http://www.theguardian.com/world/2013/nov/01/nsa-surveillance-cause-internet-breakup-edward-snowden

Appendix 2: Technology Commentary Sources

Washington Post				
	Author	**Title**	**Date Published**	**URL**
1	Peterson, Andrea	NSA snooping is hurting U.S. tech companies' bottom line	July 25, 2013	http://www.washingtonpost.com/blogs/wonkblog/wp/2013/07/25/nsa-snooping-is-hurting-u-s-tech-companies-bottom-line/
2	Peterson, Andrea	The NSA seems to really enjoy exploiting high profile tech companies	Dec. 30, 2013	http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/30/the-nsa-seems-to-really-enjoy-exploiting-high-profile-tech-companies/
3	Kollipara, Puneet	One year after Snowden, surveillance reform has stalled	June 6, 2014	http://www.washingtonpost.com/blogs/wonkblog/wp/2014/06/06/wonkbook-one-year-after-snowden-surveillance-reform-has-stalled/

4	Gellman, Barton and Soltani, Ashkan	NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say	Oct. 20, 2013	http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html
5	Peterson, Andrea	How we know the NSA had access to internal Google and Yahoo cloud data	Nov. 4, 2013	http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/
6	Skok, Michael	Five myths about the cloud	Jan. 3, 2013	http://www.washingtonpost.com/opinions/five-myths-about-the-cloud/2014/01/03/dd826052-7191-11e3-8b3f-b1666705ca3b_story.html
7	Cohen, Richard	NSA is doing what Google does	June 10, 2013	http://www.washingtonpost.com/opinions/richard-cohen-nsa-is-doing-what-google-does/2013/06/10/fe969612-d1f7-11e2-8cbe-1bcbee06f8f8_story.html
8	Gellman, Barton and Poitras, Laura	U.S., British intelligence mining data from nine U.S. Internet Companies in Broad Secret Program	June 7, 2013	http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html
9	Nakamura, David and Deyoung, Karen	Obama defends U.S. intelligence-gathering tactics	July 1, 2013	http://www.washingtonpost.com/world/europe/kerry-in-brunei-faces-european-anger-of-snowdens-nsa-disclosures/2013/07/01/b223aeb8-e247-11e2-a11e-c2ea876a8f30_story.html
10	Neumeister, Larry	Tech giants seek to halts overseas snooping by US	June 16, 2013	http://www.washingtonpost.com/business/technology/tech-giants-seek-to-halt-overseas-snooping-by-us/2014/06/16/8ea8daae-f587-11e3-930d-ca5db8eb8323_story.html

Appendix 2: Technology Commentary Sources

The Atlantic				
	Author	**Title**	**Date Published**	**URL**
1	Scaturro, Michael	The Quest to Build an NSA-Proof Cloud: European leaders want to go head to head with Amazon and Google, but some tech executives are pushing against the plan	Nov. 21, 2013	http://www.theatlantic.com/international/archive/2013/11/the-quest-to-build-an-nsa-proof-cloud/281704/
2	Friedman, Allan	Why Wasn't the NSA Prepared? Contingency planning is critical to covert operations, and the NSA's failure to anticipate or effectively mitigate its recent leak is inexcusable.	Aug. 2, 2013	http://www.theatlantic.com/national/archive/2013/08/why-wasnt-the-nsa-prepared/278310/
3	Madrigal, Alexis C.	NSA Leak Catch-Up: The Latest on the Edward Snowden Fallout	June 17, 2013	http://www.theatlantic.com/technology/archive/2013/06/nsa-leak-catch-up-the-latest-on-the-edward-snowden-fallout/276926/
4	Fridersdorf, Conor	How Surveillance-State Insiders Try to Discredit NSA Critics	Dec. 3, 2013	http://www.theatlantic.com/politics/archive/2013/12/how-surveillance-state-insiders-try-to-discredit-nsa-critics/281941/
5	Fridersdorf, Conor	The NSA wants America's Most powerful Corporations to be Dependent on It: General Keith B. Alexander, its leaer, sought unprecedented access to financial-industry computers. He hasn't gotten it yet.	July 16, 2013	http://www.theatlantic.com/politics/archive/2013/07/the-nsa-wants-americas-most-powerful-corporations-to-be-dependent-on-it/277822/
6	Mims, Christopher	2013: A terrible, horrible, no good very bad year for the tech industry	Dec. 26, 2013	http://www.theatlantic.com/technology/archive/2013/12/2013-a-terrible-horrible-no-good-very-bad-year-for-the-tech-industry/282656/
7	Madrigal, Alexis C.	Bombshell Repoert: NSA and FBI 'Tapping Directly' into Tech Copmanies' Servers: Microsoft Yahoo, Google, Facebook, AOL, Skype, YouTube, and Apple are all implicated	June 6, 2013	http://www.theatlantic.com/technology/archive/2013/06/bombshell-report-nsa-and-fbi-tapping-directly-into-tech-companies-servers/276633/
8	National Journal	Here is Obama's Plan to Reform NSA Surveillance: The biggest news is that the president plans to shift bulk collection of phone data from the government to the private sector	Jan 17, 2014	http://www.theatlantic.com/politics/archive/2014/01/here-is-obamas-plan-to-reform-nsa-surveillance/283166/
9	Schneier, Bruce	Don't Listen to Google and Facebook: The Public-Private	March 25, 2014	http://www.theatlantic.com/technology/archive/2014/03/don-

		Surveillance Partnership Is Still Going Strong		t-listen-to-google-and-facebook-the-public-private-surveillance-partnership-is-still-going-strong/284612/
10	Indiviglio, David	Google Partners with the NSA to fight Cyberattacks	Feb. 4, 2010	http://www.theatlantic.com/business/archive/2010/02/google-partners-with-the-nsa-to-fight-cyberattacks/35359/

Global Post				
	Author	**Title**	**Date Published**	**URL**
1	Trifunov, David	NSA broke into Google, Yahoo clouds through project MUSCULAR: Washington Post: The National Security Agency's Project MUSCULAR infiltrated the links of Google and Yahoo data centers, The Washington Post reported	Oct. 20, 2013	http://www.globalpost.com/dispatch/news/regions/americas/united-states/131030/nsa-hacked-google-yahoo-clouds-project-muscular-snowden
2	Overdorf, Jason	US may finally grasp the NSA scandal's seriousness: As the controversy threatens relations, Obama plans to ban spyin on allies' leaders	Oct. 29, 2013	http://www.globalpost.com/dispatch/news/regions/europe/germany/131029/germany-us-nsa-scandal-seriousness
3	West, Angust	16 Disturbing things Snowden has taught us (so far)	July 9, 2013	http://www.globalpost.com/dispatch/news/politics/130703/edward-snowden-leaks
4	The Canadian Press	NSA Spying revelations prompt some ordinary citizens to rethink computing habits	July 22, 2013	http://www.globalpost.com/dispatch/news/the-canadian-press/130722/nsa-spying-revelations-prompt-some-ordinary-citizens-rethink
5	Purtill, Colin	Building walls in the cloud: In the wake of NSA revelations, countries want to bring data back within their borders	Dec. 6, 2013	http://www.globalpost.com/dispatch/news/regions/europe/united-kingdom/131205/building-walls-the-cloud
6	The Canadian Press	Technology powerhouses try to protect financial interests as they fight U.S. government spying	Dec. 10, 2013	http://www.globalpost.com/dispatch/news/the-canadian-press/131210/technology-powerhouses-try-protect-financial-interests-they-
7	Miller, Matthew	In China, U.S. tech firms weigh "Snowden Effect"	Jan. 21, 2014	http://www.globalpost.com/dispatch/news/thomson-reuters/140121/china-us-tech-firms-weigh-snowden-effect
8	Menn, Joseph	Snowden's former provider launches open effort for secure email	Oct. 30, 2013	http://www.globalpost.com/dispatch/news/thomson-reuters/131030/snowdens-former-provider-launches-open-effort-secure-email

9	The Canadian Press	Encryption arms race escalates. But can it stop government snoops?	Nov. 29, 2013	http://www.globalpost.com/dispatch/news/the-canadian-press/131129/encryption-arms-race-escalates-can-it-stop-government-snoops
10	France-Presse, Agence	US Tech sector feels pain from NSA's prism	Aug. 26, 2013	http://www.globalpost.com/dispatch/news/afp/130826/us-tech-sector-pain-prism-cloud-computing

InfoWorld				
	Author	**Title**	**Date Published**	**URL**
1	Snyder, Bill	The NSA's spying has in fact hurt U.S. cloud providers: Although worrying, the loss of business is not as great as analysts feared	March 27, 2013	http://www.infoworld.com/d/the-industry-standard/the-nsas-spying-has-in-fact-hurt-us-cloud-providers-239168
2	Linthicum, David	Serious Action is needed to undo NSA's damage to U.S. cloud providers: As U.S. cloud providers face customer backlash, the feds treat the electronic controversey as merely a PR problem	Aug. 16, 2013	http://www.infoworld.com/d/cloud-computing/serious-action-needed-undo-nsas-damage-us-cloud-providers-224667
3	Linthicum, David	Thanks, NSA, you're killing the cloud. The current NSA scandal raises a ton of questions - and gives enterprises another excuse to resist the cloud.	June 11, 2013	http://www.infoworld.com/d/cloud-computing/thanks-nsa-youre-killing-the-cloud-220434
4	Perez, Juan Carlos	Why IT execs stick with cloud computing despite NSA snooping scandal: The benefits of cloud computing are a powerful draw, and IT execs are taking steps to mitigate their risk	Dec. 6, 2013	http://www.infoworld.com/d/cloud-computing/why-it-execs-stick-cloud-computing-despite-nsa-snooping-scandal-232208
5	Linthicum, David	Google's cloud encryption is good for PR -- and users, too: Google's addition of default encryption in its cloud storage plays on NSA-induced fears, but it's not a bad strategy	Aug. 20, 2013	http://www.infoworld.com/d/cloud-computing/googles-cloud-encryption-good-pr-and-users-too-225179
6	Linthicum, David	Serious action is needed to undo NSA's damage to U.S. cloud providers: As user providers face backlash, the feds treat the electronic spying controversy as merely a PR problem	August 16, 2013	http://www.infoworld.com/d/cloud-computing/serious-action-needed-undo-nsas-damage-us-cloud-providers-224667
7	Linthicum, David	Cloud adoption suffers in the wake of NSA snooping: Due to PRISM, non-U.S. firms are	July 30, 2014	http://www.infoworld.com/d/cloud-computing/cloud-adoption-suffers-in-the-wake-

		avoiding Stateside cloud providers, but governmnet access to cloud data can't be stopped		of-nsa-snooping-223606
8	Linthicum, David	Let the NSA spy on us -- we're still moving to the cloud. A survey shows that IT leaders are still moving to the cloud, despite NSA spying -- after all, they really don't have a choice	Dec. 20, 2013	http://www.infoworld.com/d/cloud-computing/let-the-nsa-spy-us-were-still-moving-the-cloud-232314
9	Linthicum, David	Google to NSA: You'll have to take our data the hard way. The cloud industry is turning its focus away from blocking criminal hackers to blocking systematic government snooping.	Sept. 10, 2013	http://www.infoworld.com/d/cloud-computing/google-nsa-youll-have-take-our-data-the-hard-way-226407
10	Craig, Caroline	Amazon, Cisco, Google crowd the cloud-- no thanks to NSA or IT: The march to the cloud will not be deterred, not even by the chilling effects of NSA surveillance	March 28, 2014	http://www.infoworld.com/t/cloud-computing/amazon-cisco-google-crowd-the-cloud-no-thanks-nsa-or-it-239250

SpiderOak				
	Author	**Title**	**Date Published**	**URL**
1	M., Kalyani	NSA Surveillance Taking a Toll on U.S. Cloud Computing Companies	Feb. 20, 2014	https://spideroak.com/privacypost/cloud-security/nsa-surveillance-taking-a-toll-on-us-cloud-computing-companies/
2	M., Kalyani	Impact of Surveillance on U.S. Cloud Industries	Oct. 24, 2013	https://spideroak.com/privacypost/cloud-security/impact-of-nsa-surveillance-on-u-s-based-cloud-industries/
3	M., Kalyani	NSA Surveillance Spurred Tech Firms to Tighten Security-Examining the EFF Survey Report	May 22, 2014	https://spideroak.com/privacypost/online-privacy/nsa-surveillance-spurred-tech-firms-to-tighten-security-examining-eff-survey-report/
4	M., Kalyani	Tech companies call for more restrains on NSA surveillance	Nov. 11, 2013	https://spideroak.com/privacypost/cloud-security/tech-companies-call-for-more-restraints-on-nsa-surveillance/
5	M., Kalyani	US Government Denies Tech Companies' Request for NSA Transparency	Oct. 7, 2013	https://spideroak.com/privacypost/cloud-security/us-government-denies-technology-companies-request-for-nsa-transparency/
6	M., Kalyani	Shielding yourself from PRISM	July 2, 2013	https://spideroak.com/privacyp

				ost/online-privacy/prism-user-privacy/
7	M., Kalyani	Calming the biggest cloud fears	Sept. 27, 2013	https://spideroak.com/privacypost/business-the-cloud/calming-the-biggest-cloud-fears/
8	M., Kalyani	NSA Plans on Building Quantum Computers to Break Encryption	Jan. 6, 2014	https://spideroak.com/privacypost/cloud-security/nsa-plans-on-building-quantum-computers-to-break-encryption/
9	M., Kalyani	The Importance of Encryption for Companies in the Cloud	Dec. 24, 2013	https://spideroak.com/privacypost/business-the-cloud/the-importance-of-encryption-for-companies-in-the-cloud/
10	M., Kalyani	Threats from Within: Dealing with Insider Attacks in Cloud Computing	May 1, 2013	https://spideroak.com/privacypost/cloud-security/dealing-with-insider-attacks-in-cloud-computing/

TechCrunch				
	Author	**Title**	**Date Published**	**URL**
1	Wilhelm, Alex	Apple, Google, Microsoft And Others Call On The Senate To Strengthen NSA Reform	June 4, 2014	http://techcrunch.com/2014/06/04/apple-google-microsoft-and-others-call-on-the-senate-to-strengthen-nsa-reform/
2	Wilhelm, Alex	FBI, CIA Join NSA in "Backdoor" searches on Americans	June 30, 2013	http://techcrunch.com/2014/06/30/fbi-cia-join-nsa-in-backdoor-searches-on-americans/
3	Wilhelm, Alex	The White House Throws Its Weight Behind Weakened NSA Reform Bill	May 21, 2014	http://techcrunch.com/2014/05/21/the-white-house-throws-its-weight-behind-weakened-nsa-reform-bill/
4	Wilhelm, Alex	Gmail Traffic Between Google Servers Now Encrypted To Thwart NSA Snooping	March 20, 2014	http://techcrunch.com/2014/03/20/gmail-traffic-between-google-servers-now-encrypted-to-thwart-nsa-snooping/
5	Wilhelm, Alex	NSA Allegedly Intercepts Shipments of Servers to Install Spying Backdoors	May 12, 2014	http://techcrunch.com/2014/05/12/nsa-allegedly-intercepts-shipments-of-servers-to-install-spying-backdoors/
6	Etherington, Darrell	NSA Reportedly Intercepts And Alters Routers And Servers	May 13, 2013	http://techcrunch.com/2014/

		Exported From U.S. To Facilitate Surveillance		05/13/nsa-reportedly-intercepts-and-alters-routers-and-servers-exported-from-u-s-to-facilitate-surveillance/
7	Lomas, Natasha	Zuckerberg: Snowden NSA Revelations Have Brought The Tech Industry Closer	Feb. 24, 2014	http://techcrunch.com/2014/02/24/zuck-on-snowden/
8	Ferenstein, Gregory	Those NSA Transparency Reports from Google Aren't So Transparent	Feb. 3, 2014	http://techcrunch.com/2014/02/03/those-nsa-transparency-reports-from-google-arent-so-transparent/
9	Ferenstein, Gregroy	Snowden Answers Our Burning Data Collection Question: What's the word that could happen?	Jan. 23, 2014	http://techcrunch.com/2014/01/23/snowden-answers-our-burning-data-collection-question-whats-the-worst-that-could-happen/
10	Wilhelm, Alex	US Gov Releases First NSA Transparency Report	Jun 27, 2014	http://techcrunch.com/2014/06/27/us-gov-releases-first-nsa-transparency-report/

Wired				
	Author	**Title**	**Date Published**	**URL**
1	Metz, Cade	The world is weary of American cloud computing. But it always was.	Dec. 30, 2013	http://www.wired.com/2013/12/cloud-us/
2	Kravets, David	Feds Refuse to release public comments on NSA reform -- citing privacy	Feb. 27, 2014	http://www.wired.com/2014/02/metadata-reform/
3	Poulsen, Kevin	What's in the rest of the top-secret NSA powerpoint deck?	June 10, 2013	http://www.wired.com/2013/06/snowden-powerpoint/?viewall=true
4	Zetter, Kim	Intel Director sets record straight on PRISM, sort of	June 8, 2013	http://www.wired.com/2013/06/prism-faq/
5	Poulsen, Kevin	Zuckerberg, Page: NSA Has No 'Direct Access' to Facebook or Google Servers	June 7, 2013	http://www.wired.com/2013/06/prism-google-facebook/
6	Finley, Klint	The Google Clones that Power NSA Surveillance	Dec. 12, 2013	http://www.wired.com/2013/12/opensource_nsa/
7	Levy, Steven	How the NSA Almost Killed the Internet	Jan. 7, 014	http://www.wired.com/2014/01/how-the-us-almost-killed-the-internet/all/
8	Finley, Klint	Tech Companies and Activists Unite to Protest the NSA	Feb. 11, 2014	http://www.wired.com/2014/02/fight-back/
9	Metz, Cade	Google's Bold Plan to Overthrow Amazon as King of	March 24, 2014	http://www.wired.com/2014/03/urs-google-story/

		the Cloud		
10	Mor, Yaniv	Big Data and Law Enforcement: Was 'Minority Report' Right?	March 15, 2014	http://www.wired.com/2014/03/big-data-law-enforcement-minority-report-right/

Appendix 3: Google Public Relations Statements Sources

Washington Post				
	Author	**Title**	**Date Published**	**URL**
1	Page, Larry and Drummond, David	What the…?	June 7, 2013	http://googleblog.blogspot.ca/2013/06/what.html
2	Salgado, Richmond	Government requests for user information double over three years	Nov. 14, 2013	http://googleblog.blogspot.ca/2013/11/government-requests-for-user.html
3	Salgado, Richard	Shedding some light on Foreign intelligence Surveillance Act (FISA) requests	Feb. 3, 2014	http://googleblog.blogspot.ca/2014/02/shedding-some-light-on-foreign.html
4	Lidzborski, Nicolas	Staying at the forefront of email security and reliability: HTTPS-only and 99.978 percent availability	March 20, 2014	http://googleblog.blogspot.ca/2014/03/staying-at-forefront-of-email-security.html
5	Drummond, David	Asking the U.S. Government to allow google to publish more national security request data	June 11, 2013	http://googleblog.blogspot.ca/2013/06/asking-us-government-to-allow-google-to.html
6	Salgado, Richard	A step toward government transparency	June 27, 2014	http://googlepublicpolicy.blogspot.ca/2014/06/a-step-toward-government-transparency.html
7	Google	Transparency Report: Legal Process	July 1, 2014	http://www.google.com/transparencyreport/userdatarequests/legalprocess/
8	Google	Transparency Report: FAQ	July 1, 2014	http://www.google.com/transparencyreport/userdatarequests/faq/
9	Google	Transparency Report: Overview	July 1, 2014	http://www.google.com/transparencyreport/userdatarequests/
10	Chavez, Pablo and Salgado, Richard	A petition for transparency	Sept. 9, 2013	http://googlepublicpolicy.blogspot.ca/2013/09/a-petition-for-greater-transparency.html

Appendix 4: NSA Public Relations Statements Sources

Washington Post				
	Author	**Title**	**Date Published**	**URL**
1	Director of National Intelligence, NSA	Joint Statement of the Office of the Director of National Intelligence and the National Security Agency	Aug. 21, 2013	http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_21_Joint_Statement_ODNI_NSA.pdf
2	NSA	Press statement on July 20 2013	July 30, 2013	http://www.nsa.gov/public_info/press_room/2013/30_July_2013.shtml
3	NSA	NSA Press Allegations Statement	March 13, 2014	http://www.nsa.gov/public_info/_files/speeches_testimonies/2014_03_14_press_allegations_response.pdf
4	Office of Public Affairs, Department of Justice	Joint Statement by Attorney General Eric Holder and Director of National Intelligence James Clapper on New Reporting Methods for National Security Orders	Jan. 27, 2014	http://www.justice.gov/opa/pr/2014/January/14-ag-081.html
5	NSA	The National Security Agency: Missions, Authorities, Oversight and Partnerships	Aug. 9, 2013	http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf
6	NSA	Joint Statement by Attorney General Eric Holder and Director of National Intelligence James Clapper on the Declassification of Renewal of Collection Under Section 215 of the USA PATRIOT Act (50 U.S.C. Sec. 1861)	March 28, 2014	http://www.justice.gov/opa/pr/2014/March/14-ag-319.html
7	NSA	Statement from DNI Clapper on Ending the Section 215 Bulk Telephony Metadata Program	March 27, 2014	http://www.dni.gov/index.php/newsroom/ic-in-the-news/206-ic-n-the-news-2014/1033-statement-from-dni-clapper-on-ending-the-section-215-bulk-telephony-metadata-program
8	NSA	Statement to the NSA/CSS Workforce	June 25, 2013	http://www.nsa.gov/public_info/speeches_testimonies/25jun13_dir.shtml
9	NSA	Press Statement on 30 July 2013	July 30, 2013	http://www.nsa.gov/public_info/press_room/2013/30_July_2013.shtml
10	Office of the Director of National Intelligence	List of Permissible Uses of Signals Intelligence Collected in Bulk	Feb. 10, 2014	http://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/1014-list-of-permissible-uses-of-signals-intelligence-collected-in-bulk