Spring 5-15-2015

Technology and Big Data Meet the Risk of Terrorism in an Era of Predictive Policing and Blanket Surveillance

Alexandra C. Patti
University of New Orleans, cpatti@uno.edu

Technology and Big Data Meet the Risk of Terrorism in an Era of Predictive Policing and Blanket Surveillance

A Thesis

Submitted to the Graduate Faculty of the
University of New Orleans
in partial fulfillment of the
requirements for the degree of

Master of Arts
in
Sociology

by

Alexandra Camille Patti

B.S. Boston University, 2007

May, 2015

Dedication

For Edward Snowden, whose courage inspired this research.

Acknowledgements

Without the work of Glenn Greenwald and Laura Poitras, this thesis would not have been possible. Greenwald's book, *No Place to Hide*, was an invaluable starting point, and his website, *The Intercept*, provided the NSA documents analyzed in this study.

Thank you as well to the invaluable contributions of my thesis committee, Vern Baxter, Pam Jenkins and Salmon Shomade. They provided the support, enthusiasm, advice, knowledge, and encouragement necessary to complete this project.

Finally, my sincere thanks to my friends and family, who help me maintain my sanity, throughout the writing of this thesis but at all other times, as well.

Table of Contents

List of Figures

Nomenclature and Abbreviations

AURORAGOLD: NSA program that monitors company communications to identify, exploit, and introduce vulnerabilities in cellular networks.

Big Data: Extremely large data sets, not analyzable by traditional data processing applications.

DNI: Digital Network Intelligence

DNR: Digital Number Recognition

Fairview: NSA program that collects bulk phone, internet and e-mail data

FOXACID: NSA program that defines potential surveillance targets' vulnerabilities.

Metadata: Information about the content of data, which makes it easier to analyze large quantities of data.

NSA: National Security Administration

PRISM: Planning Tool for Resource Integration Synchronization and Management. Begun in 2007, PRISM collects stored Internet communications from Internet companies.

SIGNIT: NSA program designed to break encrypted systems and introduce flaws into these systems.

Abstract

Surveillance studies suffer from a near-total lack of empirical data, partially due to the highly secretive nature of surveillance programs. However, documents leaked by Edward Snowden in June of 2013 provided unprecedented proof of top-secret American data mining initiatives that covertly monitor electronic communications, collect, and store previously unfathomable quantities of data. These documents presented an ideal opportunity for testing theory against data to better understand contemporary surveillance. This qualitative content analysis compared themes of technology, privacy, national security, and legality in the NSA documents to those found in sets of publicly available government reports, laws, and guidelines, finding inconsistencies in the portrayal of governmental commitments to privacy, transparency, and civil liberties. These inconsistencies are best explained by the risk society theoretical model, which predicts that surveillance is an attempt to prevent risk in globalized and complex contemporary societies.

Surveillance, Dataveillance, Data Mining, 9/11, Qualitative Content Analysis

> *"Nothing in our past compares to the efforts at distributed mass-surveillance that are now underway, which combine the long-standing police impulse to expand private-sector information sources with awesome new technological capabilities for vacuuming up, storing and keeping track of vast oceans of information" (Stanley 2004:3).*

> *"The greatest military power in history shields itself with an anti-missile defense system costing billions of dollars. Is it not also a bitter irony that this power should be struck to the heart of its security and self-confidence by an action that was utterly improbable according to every logic of risk, when suicide terrorists succeeded in turning commercial passenger aircraft into rockets, which destroyed symbols of American world power? The irony of risk here is that rationality, that is, the experience of the past, encourages anticipation of the wrong kind of risk, the one we believe we can calculate and control, whereas the disaster arises from what we do not know and cannot calculate" (Beck 2006:330).*

Introduction: The NSA Surveillance Programs and Surveillance Literature

On June 6, 2013, *The Guardian* published the first of numerous documents demonstrating the breadth of the American National Security Administration's (NSA) previously top-secret mass data mining programs. These documents, made available by former NSA contractor Edward Snowden and publicized by journalists Glenn Greenwald and Laura Poitras, demonstrate the existence of secret electronic surveillance data mining initiatives that use the cooperation of major Internet companies to gather information on previously encrypted Internet communications, tap into vulnerable domestic and international networks, and exploit technological innovations to collect and store previously unfathomable amounts of information, all without traditional legal checks and balances. The NSA's programs were implemented in the wake of the September 11 terrorist attacks and were ostensibly designed to prevent further terrorist plots. Revelations about the programs have revivified debates about surveillance and privacy in the modern age and provided the opportunity to empirically analyze contemporary surveillance. This study used qualitative content analysis to compare themes within a sample of NSA documents to those found in sets of laws, reports, and guidelines in order to test several hypotheses about digital surveillance that were suggested by the literature. The literature review also revealed a distinct lack of empirical data in contemporary surveillance literature, and this study attempts to at least partially rectify that limitation.

Despite their lack of data, some common themes do emerge from surveillance studies. They generally abound with theory, and they also tend to agree that surveillance changed after the 9/11 terrorist attacks. Prior to those attacks, surveillance law in the United States had remained relatively stable for decades (Henderson 2002). During those same decades, technology proliferated, facilitating the transfer of information and making communications exponentially more traceable. In the commercial sector, this meant that the model for making money shifted as businesses moved online. In this new model, the traceability of data is invaluable for marketers because the use of big data tracking technology enables marketers to construct intricate profiles of consumers and precisely target their messages to exactly the people that are most receptive to hearing it. Contemporary government surveillance programs use big data in the same way as marketers, constructing profiles of targets using data collected through their routine use of technology.

Although technological advances made mass data collection possible, changes to the legal system made by the PATRIOT Act enabled the NSA's data mining programs. The Act, drafted in 1995 but passed following the September 11 attacks, loosened restrictions on surveillance of suspected terrorists. At the time it passed, scholars argued that it had the potential to usher in an unrestricted executive surveillance power (Henderson 2002, Stanley 2004). While the Act does contain provisions to protect privacy and in most instances merely updated existing law, it has several controversial sections, Sections 203, 206, and 215 in particular. These sections, which amended the Foreign Intelligence Surveillance Act (FISA), established in 1978 in order to limit "the ability of the executive branch to conduct electronic surveillance for national security purposes" (Henderson 2002:190), were all controversial at the time Act was passed because of the threat they posed to individual privacy. The FISA Act established the FISA Court as way of subjecting federal officers investigating secret and potentially sensitive targets to judicial supervision. Originally, applications requesting electronic surveillance had to establish probable cause "that the target was either a foreign power or the agent of a foreign power" (Henderson 2002:191) and that the locations of surveillance were used or were about to be used by the target of surveillance. Judicial precedent also established that FISA evidence was only admissible as criminal evidence if its collection was incidental to intelligence gathering: "Information obtained pursuant to FISA could be used in criminal proceedings provided that intelligence gathering was the 'primary purpose' of the surveillance" (Henderson 2002:195). All other evidence was subject to more stringent requirements laid out in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III). Title III requires probable cause for governmental interception of wire communications and also mandates that "surveillance target[s] have, prior to the introduction of any damaging evidence in a criminal proceeding, the opportunity to challenge both the existence of probable cause and the conduct of the surveillance" (Henderson 2002:183). However, the PATRIOT Act changed the protocols for conducting surveillance enough that it created loopholes that enabled the government to collect data virtually unchecked.

The most controversial sections of the PATRIOT Act were set to expire 5 years after passage of the Act, but have been renewed ever since. Section 203 enables government agencies to share "foreign intelligence information" but "the definition of foreign intelligence information is sufficiently broad that it encompasses virtually anything that could be construed as a threat to national security, regardless of whether a U.S. person is involved" (Henderson 2002:205). Section 206 gives the government power to engage in roving surveillance without an obligation to prove that the target of surveillance even uses the device, enables data mining programs,. Section 215, provides "library records permission," which allows government access to materials potentially relevant to terrorist investigations. These sections continue to be controversial because of their apparently limitless scope. They also, by relaxing restrictions on surveillance, increase the likelihood of monitoring innocent and untargeted individuals.

While many of actions taken following the 9/11 terrorist attack, including detainment of prisoners in Guantanamo Bay, the invasion of Iraq, and the abuse of prisoners of war were well-documented areas of public debate, there was scant evidence of governmental surveillance. Certainly there was nothing like the comprehensive archive of documents disclosed by Edward Snowden. While the exact number of leaked documents is difficult to pinpoint, the NSA estimates that Snowden released 200,000 to 1.7 million classified documents (Kelley 2013) to Poitras and Greenwald. Because of the secret nature of the program, there had been no prior evidence of its size or scope. Now, a significant number of the documents are readily available online, primarily through Glenn Greenwald's website *The Intercept*, but on other news sites as well.

The leaked NSA documents present the opportunity to empirically explore post-9/11 surveillance in America. Most scholars agree that there was a shift in the nature of surveillance following the attacks, but there has never been such an abundance of documentation of that shift until now. Previously top secret, the NSA program has now been so extensively documented—and the leaked documents made so readily available—that it can serve as a benchmark to test theory against reality and more completely understand contemporary surveillance. To that end, this study employs a comparative qualitative content analysis to evaluate the NSA documents and better understand post-9/11 surveillance in America within a sociological framework. Several hypotheses were formed based on theoretical arguments found in surveillance studies, and themes within a sample of the top-secret NSA documents were tested against themes found in sets of publicly available laws, guidelines, and reports as a method of understanding post-9/11 surveillance in America.

Theory

The literature did suggest several themes, and surveillance literature repeatedly addresses key aspects of contemporary surveillance. One key aspect is the role that technology plays in surveillance. The effect of technology on surveillance in contemporary society has been of interest to surveillance scholars for some time, and visible changes in monitoring—the increasing number of recording devices, unprecedented reliance on personally identifiable data for verification, and corporate uses of surveillance—have been used to form theories of surveillance. In the literature, technology is consistently presented as an essential part of modern surveillance that makes surveillance almost unbelievably easy, cheap, unobtrusive, and ubiquitous (Marx and Muschert 2007:380). Modern technology has also allowed more flexible surveillance. Kevin D. Haggerty and Richard V. Ericson conceptualize modern surveillance as a "surveillant assemblage," that uses imagery that may be more appropriate for modern surveillance than even Foucault's Panopticon. The surveillant assemblage results from the convergence of previously discrete surveillance systems that reduces individuals to a set of representative data that are then analyzed (Haggerty and Ericson 2000:606). While this trend of networking is one of the hallmarks of modern surveillance, information legitimately collected in one arena may violate civil rights in another: "Practices that may in some respects be acceptable in one [type of application] (say, marketing) may erode rights and deny human dignity in another (say, anti-terrorism)" (Lyon 2014:2).

Most surveillance studies adhere to a postmodernist paradigm, and

As understood by postmodernists, power is not a top-down, structural entity, possessed and wielded exclusively by elites. Rather, it comes from everywhere, even below, and is exercised rather than owned (Foucault 1989:177). The majority of surveillance work also owes a debt to Michel Foucault. In *Discipline and Punish*, Foucault addresses the processes that create power, principally discourse and knowledge, also discussing how both power and discipline are exercised through a variety of techniques, including surveillance (Foucault 1989:27). Technology is suspicious because it not only aids this surveillance, but also because it is a tool of power with the potential to oppress and control, a theme that also frequently appears in surveillance literature (Haggerty and Ericson 2000; Lyon 2004, 2007, 2014; Mann 2012; Willcocks 2006). Foucault's metaphor of the Panopticon also has implications for many areas of interest to surveillance scholars, including those of dominance, control, and power.

Foucault's Panopticon metaphor demonstrates the necessity of surveillance in disciplinary society: "Hierarchized, continuous and functional surveillance may not be one of the great technical 'inventions' of the eighteenth century, but its insidious extension owed its importance to the mechanisms of power that it brought with it" (Foucault 1989:176). The brilliance of the Panopticon, a 19th century model prison, as a metaphor is the structure's efficient consolidation of power and control. The Panopticon's raised central tower presented the constant threat of surveillance by unseeable guards. The prison population internalized the surveillance they were subjected to and effectively policed themselves, internalizing external methods of control regardless of whether a guard was actually present. This, Foucault says, is why surveillance is so effective, not only in prisons but in schools, factories, and even society at large. Calling it a "multiple, automatic, and anonymous power," Foucault outlines its efficiency: "Its functioning is that of a network of relations from top to bottom but also to a certain extent from bottom to top and laterally...The power in the hierarchized surveillance of the disciplines is not possessed as a thing, or transferred as a property; it functions like a piece of machinery" (Foucault 1989:176-177).

Modern surveillance does mimic the Panopticon in several ways. As in the Panopticon, contemporary individuals/consumers willingly facilitate their own surveillance. Willcocks (2006) emphasizes that those under surveillance in modern Information/control society submit to the disciplinary power exercised through technological surveillance and internalize its control over them. Furthermore, a relatively small portion of the population enacts this surveillance; the rest of the population lacks the means to see reciprocally into the workings of the institutions that monitor their activities. Privacy laws increasingly distinguish between data collected on a person and personal identity (Lyon 2004), information is a commodity (as in Foucault's writing people became objects) and consumers are increasingly willing to leverage their data for perceived rewards (Campbell and Carlson 2002). Just as prisoners in the Panopticon began to believe discipline was good for them, modern consumers accept that they are justly compensated for the sacrifice of their personal information (Lyon 2004, Campbell and Carlson 2002), which is accomplished, as Foucault predicted, by coercion so subtle it is not even felt: "The contemporary Panopticon…is a consumer Panopticon based on positive benefits where the worst sanction is exclusion" (Campbell and Carlson 2002:592). People accept new technology as so essential to their own happiness and self-identity that they willingly submit to surveillance.

Despite the appeal of the disciplinary model, most contemporary surveillance scholars point to its shortcomings and have expanded and altered Foucault's original theory to better tailor it to current surveillance. The risk society and control society models, for instance, are both rooted in postmodernist theory but are distinct and more contemporary sociological frameworks that explain many aspects of present-day society, including increasing carceral rates, class inequality, and social monitoring that disproportionately affects lower classes, particularly in Western societies that boast relatively high levels of security and stability. Foucault's disciplinary model predicted that these social ills would dissipate in the face of more subtle and internalized civility, and more recent theoretical models all seek to explain what actually happened.

Benoit Dupont argues that there are, “Several architectural incompatibilities between nineteenth century prisons and twenty-first century computer networks…The distributed structure of the Internet and the availability of observation technologies has blurred the distinction between those who watch and those who are being watched” (Dupont 2008:259). Dupont identifies two principle trends frequently minimized or neglected by surveillance scholars that deserve more scrutiny: the “democratization of surveillance” and the “resistance strategies” Internet users have and are adopting to thwart this surveillance (Dupont 2008:261). Unlike the Panopticon, which by definition utilizes a central hub to enact its surveillance, the Internet was designed to be amorphous and decentralized, in order to make it resilient. This design creates an openness paradox: “while the technical protocols that underpin the Internet are public and standardized, therefore making surveillance relatively easy to carry out, the very same openness empowers application writers (programmers), who are free to design and distribute new tools of surveillance and resistance” (Dupont 2008:261). In addition, cheap surveillance software and hardware is marketed to individuals; the combination of this accessible surveillance technology with the proliferation of affordable and free tools for blocking surveillance and masking Internet activity has the potential to create unprecedented possibilities for citizen rebellion (Dupont 2008). However, the existence of resistance strategies does not equate to their widespread use, and their complexity often makes them difficult for average users (Greenwald 2014:7-33).

The study tests two prevailing models of modern surveillance society suggested in the literature: the control society model and the risk society model. Control societies operate much like modern surveillance society, using technology and the availability of data rather than prison to exert control over populations: “Control societies no longer operate, by for example, physically confining people but through continuous control and instant communication enabled by developments in material technology (Willcocks 2006:4). A crucial difference between disciplinary and control societies is that surveillance has moved from observation of specific populations to almost haphazard collection of data in the quest for relevant information (Lyon 2014:2). Because of the volume of data collection, in control societies physical confinement is no longer necessary to control society, since the threat of surveillance is felt through the perception of ubiquitous data collection (Deleuze 1992:7). Still, the control society model evolved from the disciplinary model, and the two are similar. For instance, both caution against understanding power (in this case exercised through surveillance) as a top-down, hierarchical venture: "Understanding surveillance in the 21st century also entails an analytic move beyond the conventional loci of power—the state or the corporation—to discover ways in which all sorts of processes, procedures, strategies and tactics help to shape relations and enable or constrain activities touched by globalized flows of personal data, from international to local community levels" (Lyon 2004:146). In control societies, factories have been replaced by corporations, and competition between individuals and corporations is presented as healthy and natural, thereby keeping these entities focused on each other, rather than mechanisms of control (Deleuze 1992:5). Control societies are also distinguished from disciplinary societies by the use of codes; disciplinary societies use numbers or signatures to de-individuate people (Deleuze 1992:5). While several aspects of the control society model preliminarily appeared to be relevant to contemporary dataveillance, there also appear to be discrepancies between that model and contemporary society.

Loic Wacquant proposes that incarceration rates are actually indicative of another kind of control in this country. While the disciplinary and control society models both predict that surveillance will minimize the need for physical incarceration, Wacquant calls incarceration a method of "punitive containment," not an inexplicable accident, but rather a deliberate attempt to contain the increasing number of people marginalized by neoliberal policies. He factors modern surveillance and data collection into his argument, and agrees with the control society model that both are used to control the increasing number of marginalized citizens in neoliberal societies. He points out a seeming contradiction: In an increasingly stratified and globalized society, the privileged minority of citizens enjoy increased laxity—deregulated financial systems and low rates of prosecution for white collar crimes---while impoverished populations are subjected to escalating police surveillance and incarceration in place of social assistance programs that were eliminated in the neoliberal era (Wacquant 2010). Wacquant therefore repudiates the disciplinary model. Contemporary prisons, he says, serve only to contain undesirable populations: "Hierarchical classification, elaborate time schedules, nonidleness, close-up examination and the regimentation of the body: these techniques of penal 'normalization' have been rendered wholly impracticable by the demographic chaos spawned by overpopulation, bureaucratic rigidity, resource depletion, and the studious indifference if not hostility of penal authorities toward rehabilitation" (Wacquant 20120:205).

The risk society model portrays different motives for modern surveillance than both Wacquant and control society theorists, and states that data collection is not an attempt to control society but rather prevent future disasters. They even question the possibility of control in contemporary society, given the pace of technology, globalization, and inequality: "World risk society theory does not plead for or encourage (as some assume) a return to a logic of control in an age of risk and manufactured uncertainties—that was the solution of the first and simple modernity. On the contrary, in the world risk society the logic of control is questioned fundamentally, not only from a sociological point of view but by ongoing modernization itself" (Beck 2000:218). Beck (2000; 2006) argues that risk in contemporary society has become inescapable. Data mining programs, which use actuarial models to predict risk, reflect larger societal trends, "combin[ing] a neoliberal disappointment in welfare-state objectives of totalizing transformations with an optimistic belief in the ability of information and technology to produce a risk-free society" (Amoore and De Goede 2005:150). While the disciplinary model targets individuals for reform, thereby creating an individuated and normalized society, risk management individuates characteristics within individuals, turning people into what Lyon calls "data doubles" and what Amoore and De Goede refer to as "a set of measurable risk factors" (Amoore and De Goede 2005:150). In risk societies, science only confirms peoples' feeling that risk is everywhere and danger is imminent, while denials of both risk and responsibility for risk only exacerbate danger, as when both climate change and responsibility for climate change are denied. Founded on an impossibility—the ability to predict the future—risk societies are full of ironies like this one.

The emphasis on prediction in risk society constitutes a break from the type of policing that has traditionally taken place in the United States and other democracies: "Big data reverses prior policing or intelligence activities…Now bulk data are obtained and data are aggregated from different sources *before* determining the full range of their actual and potential uses and mobilizing algorithms and analytics not only to understand a past sequence of events but also to predict and intervene *before* behaviors, events, and processes are set in train" (Lyon 2014:4). This shift in criminal justice has major implications for individual citizens, particularly when they are unable to contribute to the process. (Lyon 2014:4). Predictive policing is also inconsistent, and statistics demonstrate the ineffectiveness of attempting to predict crimes: “Criminological research showing that no method of prediction achieved more than a 50 per cent success rate in predicting dangerousness” (Zedner 2005:512). Meanwhile, the sacrifice of civil liberties for security fundamentally alters the country that is being protected (Beck 2006:330).

In both risk and control societies, surveillance is a fundamental part of society, a necessity for rational government and modern nation states: “Surveillance is a condition of modernity, integral to the development of disciplinary power and new forms of governance. It has been essential to the development of the nation state, to global capitalism and to the decentered forms of disciplinary power and ‘governmentalities’ inherent within modern societies” (Bennett 2012:485). Tokens like passwords and pin numbers that are used to establish trust and navigate the modern individuated and virtual world all create trails and establish searchable databases that enable digital surveillance, and the technology that facilitates surveillance is increasingly inescapable (Lyon 2002, 2004, 2007; Marx and Muschert 2007).

One potential problem with its ubiquity is the effect that surveillance has on social structures. Wacquant addresses this in his discussion of disparate surveillance tactics for rich and poor populations. Lyon, too, points to the potential new forms of surveillance have for stratifying society. Discussing the increase of state surveillance following the 9/11 terrorist attacks, he states, “The quality of social existence in a globalizing world is affected directly by the automated identification and social sorting systems that proliferate both at territorial borders and within the routines of everyday life” (Lyon 2002:162). While he primarily deals with airport screening measures enacted following 9/11, he also makes it clear that the potential for social sorting applies to all forms of modern surveillance dependent on automated identification, risk management and categorization: “New electronic infrastructures for risk management, deployed in the cause of security, often reflect particular priorities and long-term social, economic, and cultural divisions…Within these, categories of suspected terrorist and illegal worker, resident and claimant loom large" (Lyon 2002:163). Different social classes are also subjected to different types of surveillance, the effects of which are not equally felt. Thin surveillance "monitors movement and transactions (e.g., as with cell phones or credit cards) generally without constraining mobility, whereas [thick surveillance] refers to confinement delineated and frequently fortified spaces" (Marx and Muschert 2007:380). These types of surveillance are generally directed at different social groups, exacerbating patterns of inequity: "While poor individuals may be in regular contact with the surveillance systems associated with social assistance or criminal justice, the middle and upper classes are increasingly subject to their own forms of routine observation, documentation and analysis" (Haggerty and Ericson, 2000:618). Although thin surveillance tends to affect more affluent people with access to credit cards and technology, thin surveillance tends to be more superficial and less invasive than thick surveillance (Torpey 2007:116).

Preliminary data also indicates the potential for social stratification as a result of modern surveillance. Conducting telephone interviews of 2,400 randomly selected, non-institutionalized adults, Best and Kreuger studied perceptions of online surveillance and the perceived sensitivity of certain search terms mentioning key political figures. While they found that a majority of the public felt that they were subject to surveillance. The participants also thought that violent as well as merely oppositional political activity increased the likelihood of surveillance, political and demographic characteristics were predictors for online surveillance perceptions. Individuals with lower income and lower education levels were the most likely to perceive monitoring. They suggest that perceptions of online surveillance affect online political activity. Therefore, two of the most politically underrepresented groups may be most affected by online surveillance (Best and Kreuger 2008:205).

Data on more traditional forms of surveillance indicates that it has the potential to suppress even legal dissent and political activity. Conducting 20 individual and group interviews in each of five different geographical regions, Fernandez et al. found that surveillance suppressed and modified political dissent, discouraging people from participating in even legal protests (Fernandez et al. 2006:11). However, there is conflicting evidence about the impact of perceived government surveillance on political participation. In an earlier study in which he used, "an ordered probit model of the online participation scale using perceived government Internet surveillance and support for the war in Iraq and an interaction term of these two variables" (Kreuger 2005:443), Kreuger found that people who were strongly opposed to the Iraq War and most confident that the government monitors Internet activity were also the most likely to be politically active online (Kreuger 2005:446). However, he also cautioned against confusing cause with effect, as people predisposed to being more politically active may also be more aware of surveillance attempts, stressing that awareness of surveillance is only one in a number of predictors of political participation.

Its other noteworthy traits aside, contemporary surveillance is, first and foremost, unprecedented. The events of the early 2000s coincided perfectly to enable modern American surveillance: 9/11 happened as technology evolved, and the PATRIOT Act was passed to allow the government to capitalize on the ability of new technology to capture previously unimagined amounts of data. The several theories that explain contemporary surveillance have very little data to support them. Although the discipline of surveillance studies is developing rapidly, and the existence of post-9/11 surveillance is often discussed, there is still a lack of empirical data. Precisely because of this dearth of concrete information, modern surveillance studies themselves are an example of the risk model. There is abundant discussion of risks and what they could mean but scant empirical research that actually confirms or disproves this research. In the absence of data, all theory is equal, and modern surveillance is yet another incalculable risk. The NSA Program therefore provides an opportunity to test theory against reality, and to discard hypothetical theorizing in favor of what can more nearly be called facts.

Questions

This study addressed the lack of empirical data in surveillance studies. The top-secret NSA surveillance documents provided an opportunity to compare those documents to publicly available government materials, divided into sets of reports, laws and guidelines. This study investigated six hypotheses:

Hypothesis 1: The NSA documents will display different themes than the reports, laws, and guidelines.

Hypothesis 2: The reports and guidelines will be thematically consistent.

Hypothesis 3: The laws will be thematically consistent with the reports and guidelines.

Hypothesis 4: The control society theoretical model predicts that data collection will be haphazard, corporations and competition will play a prominent role in surveillance, codes will be used to de-individuate targets of surveillance, and the intent of surveillance is to control populations.

The risk society theoretical model predicts that data collection will be actuarial and precise, based on risk models and focused on risk prevention.

The risk society theoretical model is the best theoretical explanation of post-9/11 surveillance, as represented by the NSA's surveillance program.

Research Design

This study used a qualitative research design. Creswell defines qualitative research as "an approach for exploring and understanding the meaning individuals or groups ascribe to a social or human problem. The process of research involves emerging questions and procedures, data typically collected in the participant's setting, data analysis inductively building from particulars to general themes, and the researcher making interpretations of the meaning of the data" (Creswell 2014:4). More than quantitative research, qualitative research is interested in understanding and interpreting intent and meaning (Morgan 2014:49). It often focuses on a specific event, situation, or set of people and "relies on a holistic approach that examines as many of the relevant elements as possible (Morgan 2014:50). The specific situation studied in this study is the NSA's surveillance program in order to understand the intent and meaning of that program within existing surveillance literature.

Methods

To qualitatively understand the intent and meaning of the NSA's surveillance program, this study analyzed sets of documents using a comparative content analysis. Content analysis developed in the early twentieth century and is used across a range of disciplines for systematic analysis of communicative material (Flick et al. 2004:265). While this study looked only at texts, content analysis can analyze any documented communication. Although content analyses can also be quantitative, qualitative content analyses deal with the meaning, rather than simply the technical attributes, of documents. Qualitative content analysis involves several steps in which codes are used to establish meaning in documents and establish themes: "This sort of qualitative data analysis is a series of alternating inductive and deductive steps, whereby data-drive inductive hypothesis generation is followed by deductive hypothesis examination, for the purposes of verification" (Punch 2009:173) Codes label pieces of data within documents to attach meaning to pieces of data, thereby abstracting the large amounts of data that often characterize qualitative studies to sets of themes that can be compared to each other (Punch 2009:176). In a content analysis, deductive codes are suggested by the literature review, and inductive, or emergent codes, emerge from preliminary analysis of the data with the deductive codes.

To understand which surveillance theory best explains the surveillance exhibited in the NSA documents, this study also used a grounded theory analysis: “The ultimate idea in discovering a grounded theory is to find a core category, at a high level of abstraction but grounded in the data, which accounts for what is central in the data “ (Punch 2009:183). Grounded theory analysis was appropriate because, although three existing theoretical models were considered, none was rooted in empirical data, and so this study was, in a sense, grounding existing theory. To create grounded theory, conceptual categories in the data are identified, relationships between these categories are established, and these relationships are conceptualized and accounted for at an even higher level of abstraction (Punch 2009:183).

Data

The data in this study consist of 9 public, official privacy documents (3 laws, 4 reports and 2 guidelines) and a convenience sample of 63 NSA documents. The public documents were selected to provide an overview of changes in surveillance from the 1974 Privacy Act to the 2014 report prepared at the direction of President Obama following the Snowden leaks. These documents were specifically referred to in the literature, or referred to by other documents already included in the study. The OECD guidelines were included to represent international standards for privacy, and the other documents were written for a specifically American audience. Due to the volume of the Snowden leaks, those documents were selected based on apparent relevance to the research questions as well as their representativeness of the larger leak.

- **The Privacy Act of 1974, Title 5**: This act established a code of Fair Information Practice that governs federal agencies' use of and access to personal records (HHS 2014). Title 5 mandated the creation of the Privacy Commission and contains these Fair Information Principles.
- **Privacy Commission Report, 1977**: Established in Section 5 of the 1974 Privacy Act, the Privacy Commission was created to make recommendations for the implementation of the Privacy Act. The report made 162 recommendations, none of which were passed by Congress.
- **Electronic Communications Privacy Act of 1986**: Revising federal wiretapping and electronic eavesdropping laws, the ECPA expanded protections for citizens' phone conversations. The act also includes the Wiretap Act, the Stored Communications Act, and the Pen-Register Act. The Stored Communications Act regulates access to stored information sites and is usually applied to electronic communications.
- **OECD Privacy Guidelines, 1981**: The Organization for Economic Cooperation and Development (OECD) recommended guidelines for member nations to "harmonize" privacy legislation (OECD 2013).
- **The PATRIOT Act, 2001**: Following the September 11, 2001 terrorist attacks, the Bush Administration introduced the USA PATRIOT Act, which stands for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism." The act has been criticized for its scope and lack of checks and balances. Sections 203 and 901 in particular enable mass data mining and storage. (ACLU 2011).
- **"Safeguarding Privacy" in the Fight Against Terrorism: Report of the Technology and Privacy Advisory Committee. Executive Summary, 2004**: This is a report on one of NSA's predecessors, the Terrorist Information Awareness

program (TIA) ordered by then-Secretary of Defense Donald Rumsfeld to address concerns about legality and privacy protection.

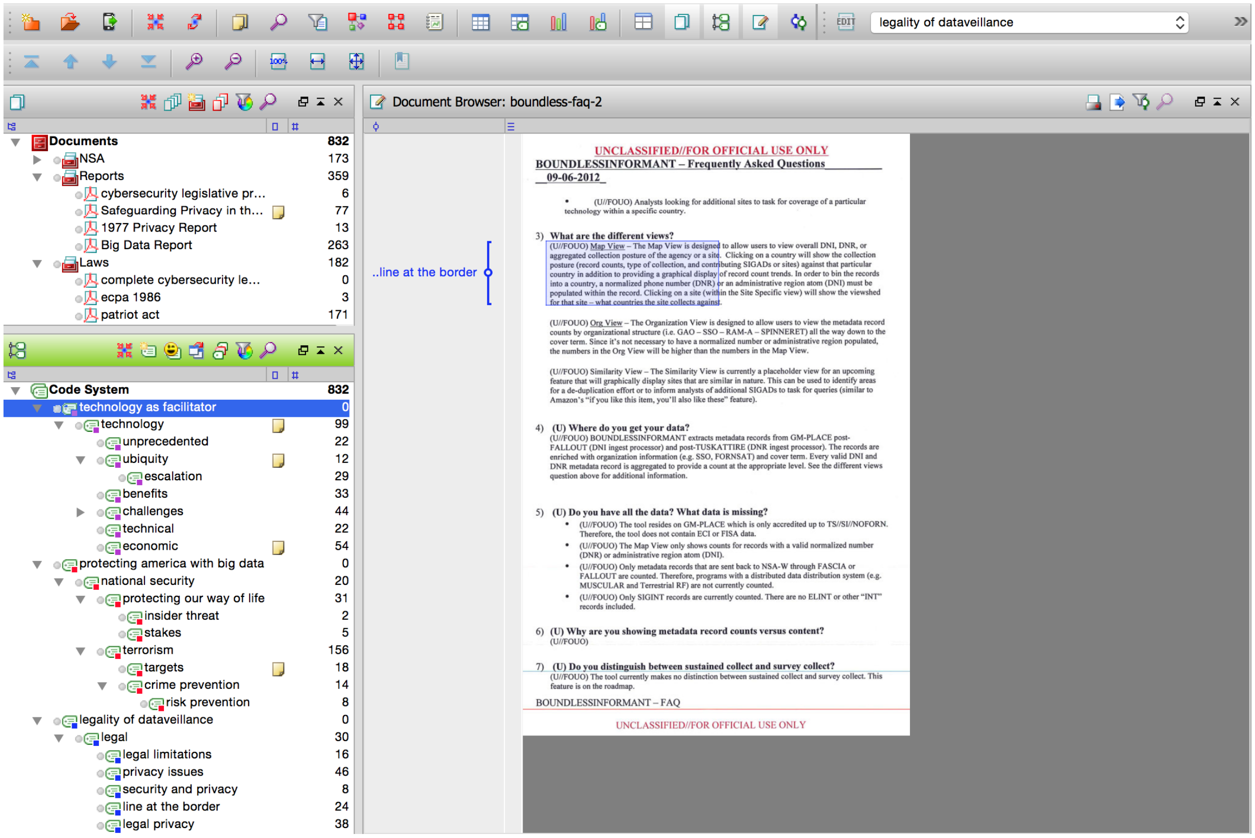
- **NSA documents, 2007-2013**: These documents, demonstrating both the existence and scope of the National Security Administration's previously top-secret data mining programs, were leaked by whistleblower Edward Snowden in 2013. The exact size of the leak is difficult to pinpoint, with the NSA offering estimates that range from 200,000 to 1.7 million classified documents (Kelley 2013). This study analyzed a convenience sample of 63 internal documents from a range of different surveillance programs.
- **Cybersecurity legislative proposal fact sheet, 2009**: "The latest achievement in the steady stream of progress we are making in securing cyberspace," this legislation was introduced by the Obama administration to protect American cyber-security (The Whitehouse, 2009). This fact sheet reports the Administration's motives for the proposal, which amend laws related to cybersecurity.
- **Consumer Data Privacy in a Networked World: A framework for protecting privacy and promoting innovation in the global digital economy, 2012**: This consumer privacy Bill of Rights was issued by President Obama.
- **Big Data: Seizing Opportunities, Preserving Values, 2014:** Following the Snowden leaks in 2013, President Obama ordered a comprehensive review of Big Data surveillance and processing, the findings of which this report documents.

Analysis

The documents were coded using MAXQDAPlus, professional software for qualitative and mixed data analysis. The program helps organize documents and media and provides a variety of ways to code documents for key phrases, concepts, and ideas. Inductive codes, suggested by the research, included "surveillance," "legal," "privacy," "terrorism," "technology," "big data," and "national security." Deductive codes resulting from document review and preliminary analysis included “protecting our way of life,” “accountability,” “transparency,” “oversight,” “challenges,” and “cooperation and standardization.” These codes were applied to segments of text that were analyzed for meaning and compared to other similarly coded segments.

The documents were coded in steps. The laws, reports, and guidelines were all coded as individual sets, using the deductive codes to build themes. They were then coded again with inductive codes, and the preliminary themes—“technology,” “national security,” “protecting privacy,” “legal,” and “economic” were compared across these sets of public documents. The NSA documents were then coded as their own set, using deductive coding and then inductive coding, to identify emergent themes. Finally, the secret NSA documents were compared to the public documents to compare themes of the public laws, reports, and guidelines to the internal, secret NSA documents. Based on this analysis, four final themes emerged: “Technology as Facilitator,” “Protecting America with Big Data,” “The Legality of Dataveillance,” and “Protecting Privacy.” These themes were then compared across document categories. Validity and reliability was established using a number of safeguards, including several rounds of coding by the researcher and external review by scholars familiar with surveillance to establish face validity.

There were several advantages to using MAXQDAPlus for this type of comparative content analysis. It allowed the documents to be organized into sets, and its document browser made it easy to switch between documents. In addition, it organized the codes within a code system. Names of codes and themes could be changed easily, and allowed the researcher to see which codes appeared in which documents at a glance. It color-coded thematic groups, and highlighted the codes with these same colors within the documents. However, while MAXQDA facilitated the analysis, it did not actually perform the analysis.



Documents	832
NSA	173
Reports	359
cybersecurity legislative pr…	6
Safeguarding Privacy in th…	77
1977 Privacy Report	13
Big Data Report	263
Laws	182
complete cybersecurity le…	0
ecpa 1986	3
patriot act	171

Code System	832
technology as facilitator	0
technology	99
unprecedented	22
ubiquity	12
escalation	29
benefits	33
challenges	44
technical	22
economic	54
protecting america with big data	0
national security	20
protecting our way of life	31
insider threat	2
stakes	5
terrorism	156
targets	18
crime prevention	14
risk prevention	8
legality of dataveillance	0
legal	30
legal limitations	16
privacy issues	46
security and privacy	8
line at the border	24
legal privacy	38

UNCLASSIFIED//FOR OFFICIAL USE ONLY

BOUNDLESSINFORMANT – Frequently Asked Questions

09-06-2012

- (U//FOUO) Analysts looking for additional sites to task for coverage of a particular technology within a specific country.

3) **What are the different views?**
(U//FOUO) Map View – The Map View is designed to allow users to view overall DNI, DNR, or aggregated collection posture of the agency or a site. Clicking on a country will show the collection posture (record counts, type of collection, and contributing SIGADs or sites) against that particular country in addition to providing a graphical display of record count trends. In order to bin the records into a country, a normalized phone number (DNR) or an administrative region atom (DNI) must be populated within the record. Clicking on a site (within the Site Specific view) will show the viewshed for that site – what countries the site collects against.

(U//FOUO) Org View – The Organization View is designed to allow users to view the metadata record counts by organizational structure (i.e. GAO – SSO – RAM-A – SPINNERET) all the way down to the cover term. Since it's not necessary to have a normalized number or administrative region populated, the numbers in the Org View will be higher than the numbers in the Map View.

(U//FOUO) Similarity View – The Similarity View is currently a placeholder view for an upcoming feature that will graphically display sites that are similar in nature. This can be used to identify areas for a de-duplication effort or to inform analysts of additional SIGADs to task for queries (similar to Amazon's "if you like this item, you'll also like these" feature).

4) **(U) Where do you get your data?**
(U//FOUO) BOUNDLESSINFORMANT extracts metadata records from GM-PLACE post-FALLOUT (DNI ingest processor) and post-TUSKATTIRE (DNR ingest processor). The records are enriched with organization information (e.g. SSO, FORNSAT) and cover term. Every valid DNI and DNR metadata record is aggregated to provide a count at the appropriate level. See the different views question above for additional information.

5) **(U) Do you have all the data? What data is missing?**
- (U//FOUO) The tool resides on GM-PLACE which is only accredited up to TS//SI//NOFORN. Therefore, the tool does not contain ECI or FISA data.
- (U//FOUO) The Map View only shows counts for records with a valid normalized number (DNR) or administrative region atom (DNI).
- (U//FOUO) Only metadata records that are sent back to NSA-W through FASCIA or FALLOUT are counted. Therefore, programs with a distributed data distribution system (e.g. MUSCULAR and Terrestrial RF) are not currently counted.
- (U//FOUO) Only SIGINT records are currently counted. There are no ELINT or other "INT" records included.

6) **(U) Why are you showing metadata record counts versus content?**
(U//FOUO)

7) **(U) Do you distinguish between sustained collect and survey collect?**
(U//FOUO) The tool currently makes no distinction between sustained collect and survey collect. This feature is on the roadmap.

BOUNDLESSINFORMANT – FAQ

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Fig 1. MAXQDA window, showing the document browser in the right large frame, with a section of coded text highlighted. The top left frame shows the documents, separated into sets of laws, guidelines, reports, and NSA documents. The bottom left frame shows the code system, separated into color-coded themes ("technology as facilitator," "protecting america with big data," and "legality of dataveillance" are shown.)

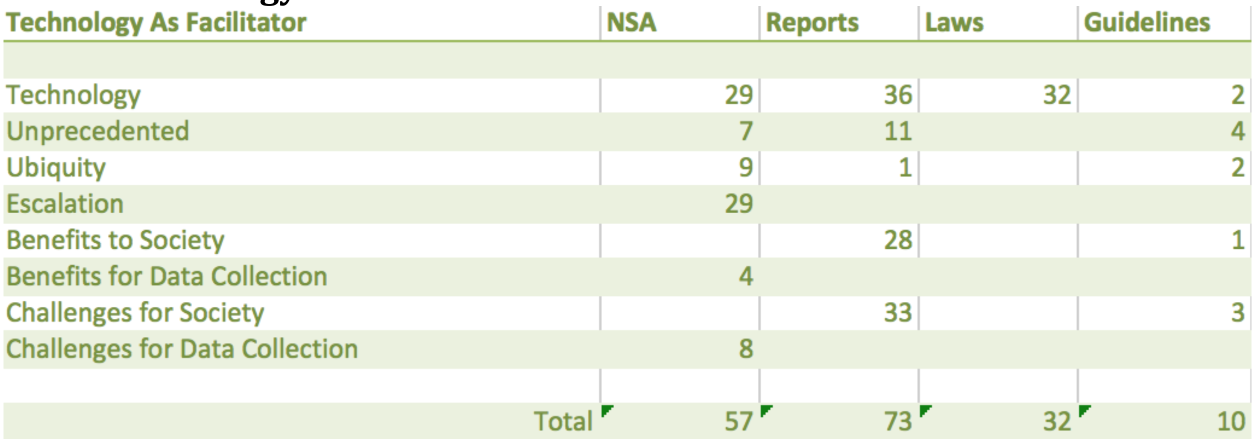
Results

The analysis demonstrated inconsistencies between the reports, laws, and guidelines and the NSA documents categories. While all of the documents indicated that a confluence of technological advances and desire for protection led to the creation of the NSA's data mining surveillance programs, intent was inconsistently portrayed across the document categories. While the NSA documents demonstrated an interest in legality, they also revealed an opaque wing of government not subject to traditional oversights that views any collection limitation as a shortcoming to be overcome through the use of evolving technology. Meanwhile, the reports and guidelines, and to a lesser extent the laws, emphasized the importance of protecting individual data privacy, limiting data collection, and preserving government transparency. The reports and guidelines also tempered their discussions of technology and data collection with conversations about the importance of protecting privacy and constitutional freedoms, presenting data and new technology as tools to help the government carry out its job. Those same documents also weighed the potential benefits of data collection against the risks they pose to these liberties. National security was presented as a motivation for data collection, but it was only one of a number of motives, and the reports and guidelines also listed a number of other ways that big data could be used to protect the American way of life, discussing ways to protect privacy in the face of evolving and escalating technological capabilities.

The NSA documents also demonstrated a number of motives for data collection, but not all of these were consistent with the motivations presented in the reports, laws, and guidelines. The NSA documents portrayed use and collection limitations as obstacles to be overcome rather than fundamental privacy protections and the invasive nature of the surveillance programs was specifically targeted to circumvent user control and overcome privacy protections like encryption. While the public documents emphasized the importance of transparency, the NSA technicians reported only to superiors within the department, there was no evidence of external oversight. Additionally, while terrorists were indeed targets of investigation, other countries and NGO's were also targeted for data collection for economic and political reasons. Furthermore, although the reports and guidelines advocated removing the legal "line at the border," which treats foreign nationals differently from U.S. citizens, the NSA documents demonstrate their programs' continued use of such distinctions. Finally, contrary to the public documents, discussions in the NSA documents of benefits and challenges related to technology only pertained to collection limitations, and not potential infringement of individual liberties.

The changes the PATRIOT Act made to the legal system, coupled with technological advancement, demonstrably allowed the creation of the NSA surveillance programs, and terrorist threats were used as the justification for those changes. Terrorism, contrary to expectation, was only mentioned in two of the public documents, an absence made more conspicuous by the frequency with which it was mentioned in those two documents, "Safeguarding Privacy," and the PATRIOT Act. The PATRIOT Act invoked terrorists and terrorism 237 times in the course of amending privacy and surveillance law, in itself an unprecedented justification for changing in legal doctrine. As a whole, the documents analyzed in this study demonstrated that technological advances, coupled with a tenuous social situation that allowed unprecedented changes to the legal system, allowed the creation of the NSA's surveillance programs, which operate in a manner inconsistent with public portrayals of American government.

Technology as Facilitator



Technology As Facilitator	NSA	Reports	Laws	Guidelines
Technology	29	36	32	2
Unprecedented	7	11		4
Ubiquity	9	1		2
Escalation	29			
Benefits to Society		28		1
Benefits for Data Collection	4			
Challenges for Society		33		3
Challenges for Data Collection	8			
Total	57	73	32	10

Fig. 2: The theme of technology as a facilitator of mass data mining programs across the document categories used in this study. Discussions of the characteristics of technology were consistently represented across the document categories, but discussions of benefits and challenges in the NSA documents were technical in the NSA documents and focused on social repercussions in the reports and guidelines.

Discussions of technology were ubiquitous across the document categories, emphasizing the unprecedented nature of modern technology, its ubiquity in contemporary life, and the rapid pace at which it evolves. Technology was an inductive code, but several deductive codes were generated by the data, including those that spoke to the characteristics of contemporary technology, like "unprecedented," "ubiquity," and "escalation." Discussions of the social effects of technology were also prevalent, and led to the creation of the "benefits" and "challenges" codes. The NSA documents contained the most technical information, while the other three document categories discussed the characteristics of modern technology and the legal, social, and economic impacts of these technologies. However, only two reports, "Safeguarding Privacy" in the Digital Age, and the Big Data Report, explicitly referenced the properties of technology. The Cybersecurity Legislative proposal pertained to issues resulting from new technology, but discussed economic and national security issues and took the presence of technology as a fact (The White House 2011). The Privacy Protection Study Commission Report, meanwhile, predated modern technological issues. The remaining reports, guidelines, and to a much lesser extent laws, primarily dealt with the characteristics, uses and challenges of "Big Data." Altogether, discussions of technology throughout the documents led to the creation of the first theme, that of Technology as a Facilitator of post-9/11 surveillance.

While technology facilitated the creation of the controversial NSA surveillance programs, appropriate governmental uses of technology were frequently discussed in the laws, reports, and guidelines. The Privacy Act stated that, "All agencies should use modern technology to inform citizens about what is known and done by their Government," adding that, "Disclosure should be timely." (Privacy Act 1974:44) The PATRIOT Act also referred to the governments' use of technology. However, rather than using technology to extend privacy and government transparency, the PATRIOT Act described technologies that should be created in order to properly execute the law (USAPATRIOT 2001:73). The Big Data Report, on the other hand, pointed to many governmental, corporate, and individual uses of modern technology. A frequent theme in that document was Obama Administration's use of data. That use is referred to as a "harnessing" of technology. This is something the Obama Administration has evidently made a priority: "Since the earliest days of President Obama's first term, this Administration has called on both the public and private sector to harness the power of data in ways that boost productivity, improve lives, and serve communities." (Executive Office of the President 2014:9) While the report discussed ways in which the administration has used technology to extend transparency, it also touched on the potential drawbacks of modern technology, an issue also discussed in other reports and guidelines, but entirely neglected in the NSA documents.

One reason the NSA programs are so unique is that technology itself evolves so rapidly and outpaces the legal system's efforts to check it. The laws, guidelines, and reports all stressed the unprecedented qualities of contemporary technology, and the potential problems these qualities create; the "unprecedented" code explained changing privacy norms, regulations, and shortcomings. The ECPA, Privacy Act, and the PATRIOT Act were all prompted at least in part by advances in technology that necessitated updates to existing legal frameworks. The OECD guidelines also focused on the use of technology as unprecedented: "Over the last three decades, personal data have come to play an increasingly important role in our economies, societies and everyday lives. Innovations, particularly in information and communication technologies, have impacted business operation, government administration, and the personal activities of individuals" (OECD 2013:19).

The reports referred to these same qualities, and the increasing importance of technology in contemporary society. The Big Data report repeatedly referred to the "transformative" and rapidity of developing technologies while also pointing to the ubiquity of new technology and the data it generates: "The information age has fundamentally reconfigured how data affects individual lives and the broader economy. More than 6,000 data centers dot the globe. International data flows are continuous and multidirectional. To a greater degree than ever before, this data is being harnessed by businesses, governments, and entrepreneurs to improve the services they deliver and enhance how people live and work" (Executive Office of the President 2014:48). In addition to the reports and laws, the guidelines also indicated that the nature of new technology is unprecedented. The Consumer Privacy guidelines referred to the ways in which modern data is easily shared and moved: "Large corporations and government agencies collecting information for relatively static databases are no longer typical of personal data collectors and processors" (The White House 2012:9).

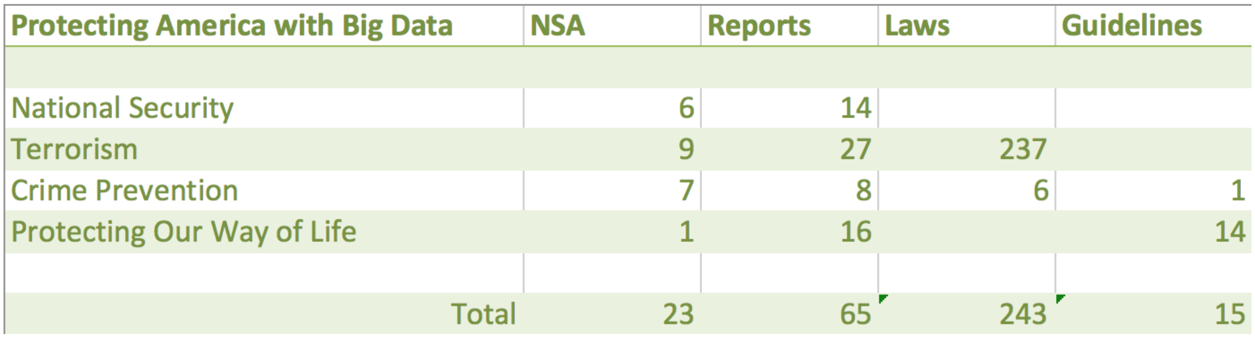
Another characteristic of modern technology exhibited in the reports and guidelines was the "rapid action" that it facilitates and, in turn, necessitates. While the speed of technology was often presented as an advantage for law enforcement, it also creates challenges for the legal system, designed to be slow and deliberative, and creates lags that allow programs like the NSA's. The Big Data report, for example, discussed how this "rapid action" helps law enforcement: "[T]he use of advanced surveillance technology by federal, state, and local law enforcement can mean a faster and more effective response to criminal activity" (Executive Office of the President 2014:31). Meanwhile, in "Safeguarding Privacy," rapid action was presented as a necessary response to keep pace with the scale and speed of modern data mining programs: "We believe rapid action is necessary to address the host of government programs that involve data mining concerning U.S. persons and to provide clear direction to the people responsible for developing, procuring, implementing, and overseeing those programs" (Department of Defense (DOD) 2004:12). Later, the report recommended steps to protect individual privacy in the face of rapidly evolving technology, and other documents also discussed the need to create alternatives to the legal system to protect these individual freedoms. The Consumer Privacy guidelines, for instance, spoke of the necessity of rapid action to keep pace with the speed of technology and maintain individual privacy protection, advocating "multistakeholder processes" as a more timely alternative to regulatory processes and treaty-based organizations: "These groups frequently function on the basis of consensus and are amenable to the participation of individuals and groups with limited resources. These characteristics lend legitimacy to the groups and their findings, which in turn can encourage rapid and effective implementation." While the legal system has been used to regulate privacy, the "unprecedented" pace of technological development is presented in these reports and guidelines as necessitating supplementary and alternative regulations. However, despite presenting issues created by the pace of technology, the shortcomings and relative enforceability of the suggested alternatives was not discussed at any length in the documents, indicating that these alternatives are in the nascent, hypothetical stages.

Still, discussions of the lag between the legal system and rapidly advancing technology were only one example of the challenges of technology that were discussed in the reports and guidelines. The challenges of mass data mining, almost always with regard to upholding privacy laws and standards, were a frequent topic in both the guidelines and reports, and the use of the word challenge was consistent across the reports and guidelines, framing the more negative aspects of data management as something to be overcome rather than immutable drawbacks. The OECD guidelines described challenges related to the value of personal data that result from the open and connected environment that modern technology allows (OECD 2013:12). The Big Data Report also identified new challenges for data privacy protection that result from advancing technology: "The advent of more powerful analytics, which can discern quite a bit from even small and disconnected pieces of data, raises the possibility that data gathered and held by third parties can be amalgamated and analyzed in ways that reveal even more information about individuals" (Executive Office of the President 2014:34). The reports and guidelines explained that the rapid development of technology has made previously effective privacy protections obsolete. Anonymized data, for example, can now be re-identified with increasing ease. Additionally, while sensor technologies that are increasingly prevalent in phones, homes, offices, and public utilities automatically collect information, technologies that promote transparency and privacy choices are developing more slowly and not being widely utilized (Executive Office of the President 2014:42, 58). The report discussed other challenges associated with big data, like uneven regulation and access to data by individuals, corporations, and the government, and filterable characteristics that create the potential for discrimination (Executive Office of the President 2014:48). The "challenges" of Big Data represented in the NSA documents, however, only reflected areas of limited access (NSA 27), and social challenges like discrimination were not discussed at all. Other challenges were issued internally to increase technical and technological data mining capabilities (NSA 32). Solutions for overcoming these challenges were usually based in technological developments (NSA 30).

Similarly, the NSA documents discussed the benefits of technology in a manner that was inconsistent with its portrayal in the reports and guidelines. Although in the public documents the challenges of Big Data were primarily addressed in the Big Data Report, the OECD Guidelines and the Consumer Privacy Bill of Rights, the "benefits" of Big Data were extolled at length in those same documents, and also "Safeguarding Privacy." One listed benefit of Big Data was its potential to actually protect privacy; while the Big Data report presented the re-identification of data as a challenge, it also stated that big data *can* be used to "enhance accountability and to engineer systems that are inherently more respectful of privacy and civil rights" (Executive Office of the President 2014:22). The Big Data report also presented multiple other social and economic benefits of using data to increase productivity: "Big data applications create social and economic value on a scale that, collectively, is of strategic importance for the nation. Technological innovation is the animating force of the American economy. In the years to come, big data will foster significant productivity gains in industry and manufacturing, further accelerating the integration of the industrial and information economies" (Executive Office of the President 2014:48). While the reports and guidelines discussed the social benefits of technology, the NSA documents treated the benefits of technology the same way they discussed challenges; while collection limitation was presented as a challenge of technology, collection facilitation was a benefit, and social repercussions were not discussed.

There were further disparities in the discussions of technology in the NSA documents versus those in the reports, laws, and guidelines. The NSA documents were overwhelmingly technical, and a majority of them referenced technology. As discussed, the presentation of potential social benefits and challenges of these technologies was entirely absent, and technological advances were instead only celebrated for their unprecedented ability to increase access to targets' data (NSA 10, NSA 29) and their efficiency (NSA 30), but other aspects of technology were also discussed. For example, the increasing capabilities of evolving technology were also frequently discussed (NSA 36, NSA 29, NSA 30), as were the perceived threat of foreign nations' increasing technological capabilities (NSA 31). In addition, the training-based nature of many of the documents spoke to the novelty of the access provided by technology, and the escalating ubiquity of data collection was reflected through slides that demonstrated drastically escalating data collection (NSA 19, NSA 22, NSA, NSA 30, NSA 30, NSA 34, NSA 43). Technological discussions in the NSA documents also included the vulnerabilities of particular types of technology, websites, and email providers (NSA 32, NSA, NSA 10, NSA 11, NSA 16A, NSA 16D), further suggesting that the intent of the program was to maximize the potential of technology, not consider its social repercussions. As in the reports and guidelines, more rapid action was presented as one of the benefits of technological advances (NSA 15, NSA 7, NSA 30 2), but, partly owing to their technical nature, the NSA documents were much less reflexive than the public documents, and, while they demonstrated the properties of technology that were discussed in the reports and guidelines, there was no debate about the merits of the conducted surveillance. Still, the NSA documents corroborate the theme of technology as facilitator, providing evidence that the qualities of technology discussed in the reports, laws, and guidelines facilitated the creation and expansion of the surveillance programs.

Protecting America with Big Data



Protecting America with Big Data	NSA	Reports	Laws	Guidelines
National Security	6	14		
Terrorism	9	27	237	
Crime Prevention	7	8	6	1
Protecting Our Way of Life	1	16		14
Total	23	65	243	15

Fig. 3: The theme of Protecting America with Big Data included references to national security and crime prevention as well as discussions of the importance of protecting American ideals and freedoms. These discussions were principally limited to the reports and guidelines. The invocation of terrorists and terrorism as justifications for data collection was similarly limited, appearing 237 times in the PATRIOT Act, 26 times in “Safeguarding Privacy,” and virtually nowhere else in the reports, laws, and guidelines.

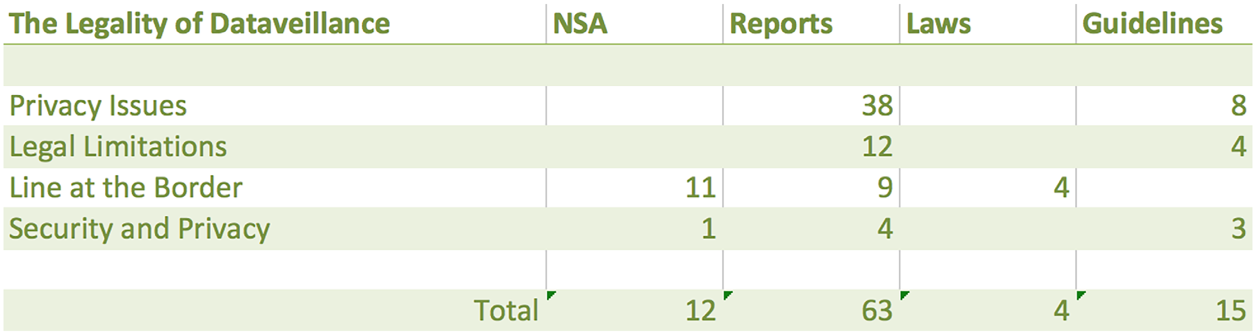
The second theme, “Protecting America with Big Data,” encompassed recurring representations of the national government as a protector. While technological advances made the NSA programs technically feasible, the documents demonstrated that a desire for protection and security was equally responsible for their creation. “Protecting America with Big Data,” not only spoke to the roles that national security and efforts to thwart terrorism play in dataveillance, but also the ways in which data collection both protects and threatens fundamental American rights and freedoms. Data collection was presented as a way of protecting American citizens across the laws, reports, guidelines, and NSA documents. While “terrorism,” “national security,” and “crime prevention” were inductive codes, “protecting our way of life” emerged as a deductive code as a result of the emphasis that the reports and guidelines placed on the importance of protecting American liberties and freedoms.

As expected, national security was presented as an important user and driver of dataveillance in the reports, laws, guidelines, and NSA documents. Both "Safeguarding Privacy" and the Big Data report addressed this benefit, and the Cybersecurity Legislative Proposal recommended updating cybersecurity law "to better protect America against cyber threats (The White House 2011:1). "Safeguarding Privacy", which was created specifically to evaluate government data mining programs, dealt almost exclusively with this benefit to national security (DOD 2004). The PATRIOT Act, meanwhile, specifically amended surveillance law in order to protect against terrorist threats, and the NSA documents indicated targeting potential terrorists in order to prevent future attacks. The invocation of terrorists and terrorism across the documents was itself noteworthy. The documents that predated the 2001 terrorist attacks were, except where amended, wholly silent on the subject, but the PATRIOT Act, used the words terrorist and terrorism 237 times, or an average of 1.8 times per page (USAPATRIOT 2001). "Safeguarding Privacy" repeated the words 26 times over 18 pages, an average of 1.4 times per page (DOD 2004). By contrast, the Big Data report used the word terrorist only once in 85 pages, and none of the other reports, laws, or guidelines mentioned either terrorists or terrorism. While national security continued to be a relevant justification for data collection across the reports, guidelines, and laws, terrorism itself was used as a justification only in the two documents that were written closest to the 9/11 attacks, indicating that it lost its salience as the attacks became less immediate.

However, national security was not the only way government was portrayed as a protector in the documents. The code "protecting our way of life" was an inductive code, created for discussions in the reports, laws, and guidelines about protecting privacy rights and constitutional freedoms. The theme of government as protector, both of its citizens and freedom, appeared across all four document groups, with the reports and guidelines speaking most frequently of the obligation the government has to "protect its citizens when exercising power and authority for the public good" (Executive Office of the President 2014:22). In reports that discussed the dangers posed to privacy by Big Data, "protecting our way of life" asserted the government's commitment to upholding law and privacy, even as, "big data could be a tool that substantially expands government power over citizens" (Executive Office of the President 2014:22). As expressed in the Consumer Privacy Bill of Rights, this government commitment to "protecting our way of life" extended to the private sector; the report stated that the "United States has both the responsibility and incentive to help establish forward-looking privacy policy models that foster innovation and preserve basic privacy rights" (The White House 2012:7). That paper suggested the access and accuracy principle to facilitate consumer access to data that is collected about them, "interpreted with full respect for First Amendment values, especially for non-commercial speakers and individuals exercising freedom of the press" (The White House 2012:20). In addition, while "Safeguarding Privacy" dedicated much discussion to terrorist threats and the pressing need to defend against these threats, it also stated that Secretary of Defense Donald Rumsfeld, "charged the committee with developing safeguards to ensure that the application of this or any like technology developed within the DOD is carried out in accordance with U.S. law and American values related to privacy" (DOD 2004:1). "Protecting our way of life," therefore, emphasized the government's purported commitment to protecting its citizens from external, as well as internal threats.

The NSA documents did not display the same commitment to protecting individual liberties that was evident in the reports, laws, and guidelines, and only demonstrated an interest in national security. The NSA documents contained several references to protecting national security and promoting law enforcement efforts, and some of these explicitly referred to protecting America's cyberspace through data mining initiatives (NSA 38 2, 4). Other references were to counterterrorism, preventing and investigating international crime and narcotics, and other international security issues (NSA 22). Two documents explicitly referred to threat management as a goal (NSA 10, NSA 30 7), and the DTI Report in particular contained references to terrorism and preventing terrorist threats (NSA 30). Targets of surveillance included but were not limited to suspected terrorists; other targets included foreign governments (NSA 10). Furthermore, while discussions of national security in the NSA documents omitted discussions of "protecting our way of life," national security was not the only justification used for surveillance, and other cases of surveillance were economically and politically motivated (NSA 24). Although the NSA documents emphasized national security over the protection of civil liberties, and were in that sense inconsistent with the laws, reports, and guidelines, they did corroborate the overall theme of protection being both a justification for and a use of dataveillance. Furthermore, the overwhelming use of the word terrorist and terrorism as justifications for changes in surveillance law following the 9/11 attacks indicates a shift in the social climate and escalation of fears following those attacks, leading to a social environment that was more supportive of government surveillance programs.

The Legality of Dataveillance



The Legality of Dataveillance	NSA	Reports	Laws	Guidelines
Privacy Issues		38		8
Legal Limitations		12		4
Line at the Border	11	9	4	
Security and Privacy	1	4		3
Total	12	63	4	15

Fig. 4: The Legality of Dataveillance. The legal system, slow and deliberate by design, was portrayed in the reports and guidelines as too slow to keep up with the pace of technological change, creating legal loopholes that allow mass data collection programs. The NSA documents demonstrated an interest in legality, adhering to a legal "line at the border" that treats foreign nationals differently than American citizens. This approach was codified in the PATRIOT Act but discredited in the reports and guidelines, which advocated extending privacy protections to everyone.

While the PATRIOT Act used the instability and fear surrounding the 9/11 terrorist attacks to justify changing the surveillance requirements for suspected terrorists, the other documents used in this study discussed additional legal issues, related to technological advances, that potentially threaten privacy. The "Legality of Dataveillance" theme included discussions of the legality and morality of dataveillance; "privacy" and "legal" were deductive codes, but "line at the border" and "security and privacy" both arose from discussions in the documents that related to the two deductive codes. The reports and guidelines both discussed how the advance of technology and the slow pace of the legal system create loopholes that take years to close, allowing programs like the NSA's to employ collection techniques that have been discredited in the reports and guidelines. The PATRIOT Act actually codified an example of this: a legal line at the border that excludes foreign nationals from the privacy protection afforded to American citizens (USAPATRIOT 2001:11, 15). Traditionally, information collected outside of the United States is exempt from the legal requirements of information collected inside the country, but because of technological advances, data no longer stops at political borders, and a substantial amount of collected information flows through American as well as foreign data networks (NSA 4, NSA 5, NSA 7). Indeed, the NSA documents present this as a benefit to be used when data gathering (NSA 4). The major distinction governing surveillance now is not where the information is collected, but on whom it is collected. Importantly, the reports and guidelines used in this study discredited this approach, and advocated extending American privacy protections to all individuals, but the suggestions made in those documents have not been followed. This raises questions about the best way to protect privacy given rapidly advancing technological capabilities, a slow legal system, and unenforceable suggestions made in official reports and guidelines.

Perhaps because of the confusion surrounding the issue, the "Legality of Dataveillance" theme was the least consistent of the four that emerged from this study. Within the laws, the PATRIOT Act was discordant with the ECPA and the Privacy Act. Those earlier documents both extended individual rights to data protection and government transparency where the PATRIOT Act limited them. Sometimes, as when the Big Data report called the existing consumer data privacy framework "strong" in its introduction (The White House 2012:i) but then detailed limitations of the existing legal system in the body (The White House 2012:6), documents even contradicted themselves.

Of all the document categories, the reports and guidelines presented the most concerns about individual legal privacy protections. In the reports and guidelines, privacy was presented as a fundamental and cherished, as well as constitutionally protected, American right. The reports and guidelines, while stressing the government's commitment to maintaining these rights even as Big Data fundamentally changes the way government functions, also discussed the importance of creating trust with the American public. The reports and guidelines enumerated a number of specific threats Big Data presents for privacy: "Big data analytics have the potential to eclipse longstanding civil rights protections in how personal information is used in housing, credit, employment, health, education, and the marketplace" (Executive Office of the President 2014:iiv). The Big Data report frequently discussed the potential for discrimination; 9 of the 10 coded segments in this category came from that report. The other came from the OECD guidelines, which made ensuring there is no discrimination against data subjects one of its provisions under "National Implementation" (OECD 2013:17). Because digitized data is easily searchable and filterable—something that makes it particularly useful for marketers as well as surveillance technicians—it presents the possibility of what the Big Data report called "digital redlining." That report listed instances of different prices offered to individuals based on the area in which they live. In its recommendations, it exhorted companies and the government to take policy measures necessary to prevent these instances of discrimination. These privacy issues were presented as an inherent "challenge" resulting from big data, and the government was presented as both respectful of privacy and committed to upholding the law.

The legal limitations code was used in the Big Data Report, the OECD guidelines, the Consumer Privacy, and "Safeguarding Privacy" guidelines. While the laws all dealt with privacy issues—The ECPA and the Privacy Act were both created to address threats to privacy arising from new technology and governmental collection and storage of data on individuals and the PATRIOT Act maintained concern with constitutionally protected rights of citizens even as it extended governmental data collection powers—the laws themselves did not explicitly address the legal limitations that led to their creation. The reports and guidelines, however, generally presented legal limitations as a significant obstacle to protecting privacy. Legal privacy protections were called disjointed, out of date, and too narrowly defined (Executive Office of the President 2014; DOD 2004). "Safeguarding Privacy" presented an alternate view of legal limitations, discussing them in reference to the fight against terrorism: "Existing legal requirements applicable to the government's many data mining programs are numerous, but disjointed and often outdated, and as a result may compromise the protection of privacy, public confidence, and the nation's ability to craft effective and lawful responses to terrorism" (DOD 2004:5).

The Big Data Report and the Consumer Privacy Guidelines both framed their discussion of legal limitations with regard to individual privacy protections. The Big Data Report discussed how privacy law became disjointed and narrowly defined, making it more difficult to broadly protect individual privacy: "In the United States during the 1970s and 80s, narrowly defined sectoral privacy laws began to supplement the tort-based body of common law. These sector-specific laws create privacy safeguards that apply only to specific types of entities and data. With a few exceptions, individual states and the federal government have predominantly enacted privacy laws on a sectoral basis" (Executive Office of the President 2014:18). In addition, The Consumer Privacy bill also cited the legal limitations of Internet consumer privacy protection, including the lack of comprehensive policy:

> "Much of the personal data used on the Internet, however, is not subject to comprehensive Federal statutory protection, because most Federal data privacy statutes apply only to specific sectors, such as healthcare, education, communications, and financial services or, in the case of online data collection, to children" (The White House 2012:6).

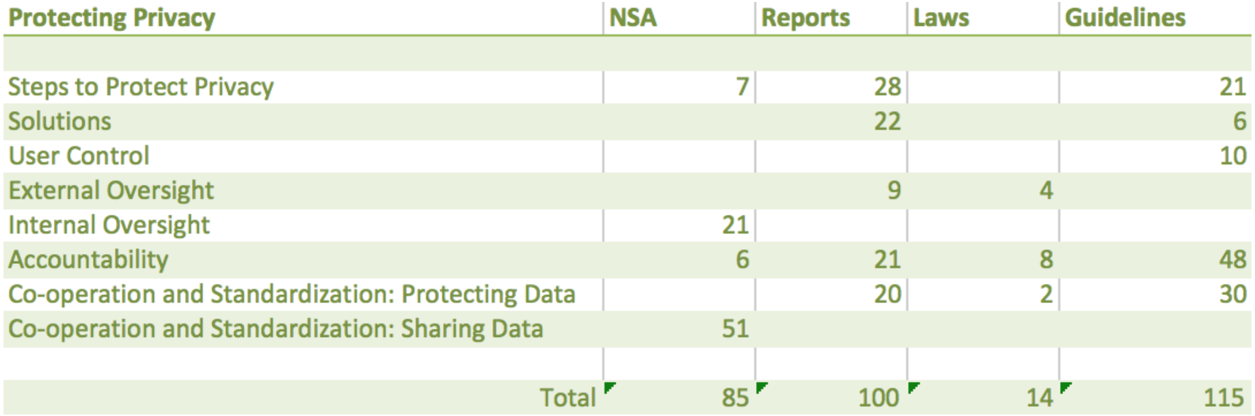
In the foreword to The Consumer Privacy bill, the authors contradicted this statement, saying, “The consumer data privacy framework in the United States is, in fact, strong. This framework rests on fundamental privacy values, flexible and adaptable common law protections and consumer protection statutes, Federal Trade Commission (FTC) enforcement, and policy development that involves a broad array of stakeholders”(The White House 2012:i) While the authors tempered this optimistic statement somewhat, the endorsement of existing consumer data privacy protection contradicted statements contained within those guidelines and the other documents used in this study.

The Big Data report in particular established the history of privacy law in the United States. Fair information practice principles, or FIPPs, were created in 1973 and established in the 1974 Privacy Act and today, “form the bedrock of modern data protection regimes.” (Executive Office of the President 2014:17) “The FIPPs articulate basic protections for handling personal data. They provide that an individual has a right to know what data are collected about him or her and how it is used. The individual should further have a right to object to some uses and to correct inaccurate information. The organization that collects information has an obligation to ensure that the data are reliable and kept secure.” (Executive Office of the President 2014:17) Still, as with the rest of the existing legal privacy protections, the NSA documents demonstrate practical concerns with existing legal privacy protections.

While the NSA documents did demonstrate an interest in legality, they also showed some current limitations of legal oversight. They also show that data are collected on U.S. citizens as well as foreign nationals, referring to efforts to minimize, or remove personally identifiable information from, data collected on U.S. citizens (NSA 27; 37). The Big Data

Report argued that minimization is increasingly ineffective for protecting private data, and the use of the technique shows that surveillance programs collect information on U.S. citizens as well as foreign nationals. The theme “legality of dataveillance” therefore demonstrated inconsistencies between public statements and private practices, and illuminated the limitations of current privacy protections.

Protecting Privacy: Accountability, Transparency, and Oversight



Protecting Privacy	NSA	Reports	Laws	Guidelines
Steps to Protect Privacy	7	28		21
Solutions		22		6
User Control				10
External Oversight		9	4	
Internal Oversight	21			
Accountability	6	21	8	48
Co-operation and Standardization: Protecting Data		20	2	30
Co-operation and Standardization: Sharing Data	51			
Total	85	100	14	115

Fig. 5: Protecting Privacy in the Face of Legal, Social, and Technological Change. The reports and guidelines both discussed measures to protect privacy, but these measures were not consistent with those demonstrated in the NSA documents. While the reports and guidelines both stressed the importance of transparency and external oversight for maintaining a robust democracy, the NSA documents only demonstrated internal oversight. Additionally, while co-operation and standardization was presented in the reports and guidelines as a way for protecting data, in the NSA documents, co-operation and standardization were used to share data collected under FISA court warrants with multiple law enforcement agencies, that are not supposed to operate under the FISA court.

Because of the legal system’s privacy protection limitations, several documents suggested or, in the case of the laws, codified privacy protections. The final theme, “Protecting Privacy” encompassed these discussions and revealed incompatibilities between the suggestions made in the reports and guidelines and standard NSA practices. The reports and guidelines were still the consistent categories, calling for accountability facilitated by transparency and oversight as a way to protect privacy. The Big Data report also discussed the need for more extensive user controls that would allow users to control how much information was collected about them (Executive Office of the President 2014:62). The Consumer Privacy and OECD guidelines similarly advocated for use and collection limitations that would restrict the amount of data that are collected and also the ways companies use those data (OECD 2013:14; The White House 2012:1, 6, 15, 16, 21). User control and collection limitation help individuals manage the data that is collected about them on the front end, while use limitations protect their data once it has already been collected. Accountability, transparency, and oversight theoretically apply to all stages of the process, but the NSA documents indicate differing standards of accountability and transparency than were evident in the reports and guidelines.

The accountability code appeared in the guidelines, the PATRIOT Act, and the Privacy Act. In his introduction to the Privacy Act, President Obama stated that, “A democracy requires accountability, and accountability requires transparency” (Privacy Act 1974:44). That act also affirmed the need to have transparency in order to have government accountability, establishing the right of citizens to their own information or information about their government. The PATRIOT Act, however, removed accountability for people who “in good faith produce tangible things under and order pursuant to section [215…] Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context” (USAPATRIOT 2001:17). Not only are people not required to divulge their involvement and disclosure of information pursuant to a FISA warrant, they are also outright prohibited from discussing those warrants with anyone, including legal counsel. That inhibits the possibility for journalists and advocates to investigate or question the program, thereby allowing the programs to operate in secret without external review. The PATRIOT Act did establish some accountability for law enforcement implementing an ex parte order, requiring records of all installed surveillance devices that identify the officers that installed and/or accessed the device, the dates and times of installation, uninstallation, and access, the configuration of the device, and information collected by the device (USAPATRIOT 2001:17), but overall it still limited government accountability where earlier laws enhanced it.

The guidelines discussed accountability differently than the laws. The Consumer Privacy discussed the need for FTC enforcement that holds companies accountable for protecting sensitive personal information (The White House 2012:2, 29). However, those guidelines also stated that companies and consumers share responsibility for protecting their information. While "Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights" (The White House 2012:1), consumers also have a responsibility when choosing privacy settings and sharing personal data (The White House 2012:13). The OECD guidelines, however, stressed that data controllers alone are accountable for personal data under their control and never mentioned the responsibility consumers or individuals bear for managing their own data (OECD 2013:16).

While accountability was portrayed as an important way to protect privacy, "transparency," according to the documents that discussed it, is the principle way of ensuring accountability. The Big Data report and Consumer Privacy guidelines generally applauded the way the U.S. government deals with privacy issues, giving the Obama administration in particular credit for transparency (Executive Office of the President 2014:9). The Big Data Report, which presented transparency as essential for democracy, gave multiple examples of the government's commitment to transparency, including its establishment of data.gov, a central site for all publicly accessible government data. While it is the only document in this study published following the Snowden revelations, there was no discussion of the ramifications of top-secret, ongoing surveillance programs for transparency.

The OECD Guidelines and Consumer Privacy guidelines also both emphasized the need for transparency when using data. The four coded segments from the OECD guidelines all spoke of member countries' obligation to uphold principles of transparency. The openness principle (OECD 2013:15) in that set of guidelines was similar to the Fair Information Practices enumerated in the Privacy Act. That document established principles of access to personal information held by the government: "Each agency that maintains a system of records shall—(1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him" (Privacy Act 1974:47).

In his note at the beginning of the privacy act, President Obama asserted his commitment to transparency, and upholding the Privacy Act in order to perpetuate the vital role it plays in democracy (Privacy Act 1974:44). He exhorted government agencies and employees to respect the Freedom of Information Act:

> The Freedom of Information Act should be administered with a clear presumption: In the face of doubt, openness prevails. The Government should not keep information confidential merely because public officials might be embarrassed by disclosure, because errors and failures might be revealed, or because of speculative or abstract fears. Nondisclosure should never be based on an effort to protect the personal interests of Government officials at the expense of those they are supposed to serve. In responding to requests under the FOIA, executive branch agencies should act promptly and

> in a spirit of cooperation, recognizing that such agencies are servants of the public (Privacy Act 1974:44).

The 13 segments from the Consumer Privacy report that were coded for "protecting privacy" spoke of consumer rights to easily accessible and understandable information about how their personal data is collected and used, as well as the ability to correct inaccurate data (The White House 2013:13, 48). One segment discussed the need for more transparency in credit markets (The White House 2012:47). Two codes discussed the Obama administration's commitment to government transparency (The White House 2012:2, 20). Like "transparency," "oversight" was portrayed in the documents as a way of ensuring accountability. This code appeared most often in the reports and guidelines, but the laws discussed oversight, as well. Section 502 of the PATRIOT Act stated, "On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests for the production of tangible things under section 402" (USAPATRIOT 2001:17). "Safeguarding Privacy" also gave the responsibility for oversight of data mining programs to Congress: "There is also a critical need for Congress to exercise appropriate oversight, especially given the fact that many data mining programs may involve classified information which would prevent immediate public disclosure" (DOD 2004:10). The report also recommended managerial and judicial oversight, including a 5-part checklist for ensuring oversight of data mining and recommending that the Secretary create "meaningful" oversight mechanisms (DOD 2004:5, 8).

The OECD guidelines discussed the need for oversight 8 times, and the Consumer Privacy guidelines implicitly referred to the need for oversight when discussing accountability and enforcement, in statements that call for FTC enforcement, and government accountability. The Big Data report referred to a lack of oversight for government employees who deal with data: "In the past, users and system administrators might have been issued a login and username and granted total access, sometimes without an audit trail monitoring their use" (Executive Office of the President 2014:28). Later, that same report stressed the need for various arenas of government to experiment with the potential of Big Data, but only while being subjected to appropriate accountability and oversight measures (Executive Office of the President 2014:66). The cybersecurity legislative proposal also recommended oversight that includes congressional reporting (DOD 2004:2, 4).

The NSA documents discussed privacy in the context of steps taken to protect and properly handle sensitive data (NSA 30 12). The DTI report, for example, referenced the creation of 430,000 terrorism-related records, and deletion of "50,000 subjects whose nexus to terrorism was refuted, or did not meet current watchlisting criteria" (NSA 30 2). Another presentation stated that each agency will "minimize the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning unconsenting U.S. persons consistent with the need of the U.S. to obtain, produce, and disseminate foreign intelligence information" (NSA 43). Not only are data on U.S. citizens clearly being acquired, there is no cross-agency standardized protocol for disposing of such information. The AuroraGold project apparently includes "auto-minimization" (NSA 27 2).

No segments of the NSA documents met the criteria for the "accountability" code, but there were several references to oversight. In the documents, this oversight was entirely internal, team-based or FISA court-based (NSA 2C, NSA 21). Sometimes, specific analysts or people with specific levels of clearance were the only people allowed to conduct certain surveillance, but it was unclear who except their superiors within the agency has oversight over these individuals (NSA 14, NSA 15). Reference was made to NSA standards (NSA 27 2) and observance of rules and indications of authorities requesting investigations (NSA 39 49). User monitoring, or internal audits of IC-wide users were conducted by the NSA "to guarantee correct investigations and the observance of rules and indications" (NSA 39). The respective agencies would be notified of non-compliance, and persons found to be conducting inappropriate surveillance would be removed (NSA 43), but there was no reference to external or Congressional oversight. There was also minimal evidence of collection limitation in the NSA documents, aside from references to minimization of data collected on U.S. citizens. Most of the documents referencing collection celebrated escalating collection capabilities and quantities of information (NSA 30 5, 6, 8, 10, 12; NSA 32 2; NSA 34 11; NSA 43; NSA 43 16, 20, 30; NSA 44 1).

In addition to accountability, transparency, and oversight, the reports and guidelines also presented cooperation and standardization as a method of protecting privacy. The code "standardization and cooperation" was used across all four document categories, but had an entirely different meaning in the NSA documents than in the reports, guidelines and, to a lesser extent, the laws. The reports and guidelines presented standardization and cooperation as a necessary measure that, like transparency, accountability, and oversight, is necessary to protect individual data. For example, The Big Data report explicitly dealt with a lack of cooperation and inter-departmental standardization that poses challenges for data and privacy protection: "Many of the databases DHS operates today are physically disconnected, run legacy operating systems, and are unable to integrate information across different security classifications. The Department also carries out a diverse portfolio of missions, each governed by separate authorities in law...Ensuring information is properly used falls to six offices at DHS headquarters" (Executive Office of the President 2014:27). Likewise, "Safeguarding Privacy", the Privacy Protection Study Commission Report, the Big Data Report, the OECD guidelines, and the Consumer Privacy guidelines all recommended improving standardization and cooperation with respect to data privacy protections (DOD 2004:9, 10; The White House 2011:1; Executive Office of the President 2014:37, 48; OECD 11, 16, 17; The White House 2012:2, 7). Inter and intra-governmental cooperation was one recurring theme. "Safeguarding Privacy" stated that, "government efforts to protect national security and fight crime and to protect privacy will be enhanced by the articulation of government-wide principles and a consistent system of laws and processes" (DOD 2004:10). The Big Data report likewise suggested adopting its recommendations "across all agencies and security levels" (Executive Office of the President 2014:37). That report also encouraged cooperation between public and private sectors (Executive Office of the President 2014:48), as do the OECD guidelines, which also advocated inter-government cooperation: "The continuous flows of personal data across global networks amplify the need for improved interoperability among privacy frameworks as well as strengthened cross-border cooperation among privacy enforcement authorities" (OECD 2013:11). The Consumer Privacy guidelines likewise encouraged global cooperation, specifically international operability of data privacy frameworks through mutual recognition and enforcement cooperation. (The White House 2012:2, 7).

The PATRIOT Act also explicitly encouraged cooperation, although its intent was less clear in that document. The results of the PATRIOT Act's references to cooperation are demonstrated in the NSA documents. Orders issued under Section 216 automatically applied "to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order" (PATRIOT 18). Under Section 414, the Act mandates that visa entry and exit data systems interface with law enforcement databases (USAPATRIOT 2001:83). The NSA documents demonstrated this cooperation with other government agencies, including the CIA, FBI, TSC, TSA, NGA, DoS, DHS, CPB, DIA, DEA, US Army Special Forces, the Bureau of Diplomatic Security, INTERPOL, and GCHQ (NSA 30 9, NSA 34 6, NSA 37 1). There were references to information sharing with the CIA and FBI, and to training agents from the other departments (NSA 30 8). The Directorate of Terrorist Identities (DTI) partnered with the CIA to use information obtained on foreign governments through that agency's HYDRA program, which clandestinely accessed foreign government's databases and mined the data found there. (NSA 30 9). In the instance discussed, DTI provided the names of 555 Pakistani subjects. The HYDRA program in turn vetted these names against Pakistani passports, enhancing the information on all 555 of those subjects (NSA 30 9).

The NSA documents demonstrate cooperation in other ways. While in most cases, the cooperation can be seen as resulting directly from the PATRIOT Act, this cooperation did not function as a privacy protection. Cooperation with private businesses demonstrated in the NSA documents included the NSA's use of data collected by gmail, facebook, Hotmail, Yahoo, Apple, Google, Skype, paltalk.com, YouTube and AolMail from their customers under their terms of use. Rather than serving to protect individual or consumer privacy, as the reports and guidelines indicated, the NSA's cooperation with private corporations actually violated these individual privacies. As dictated by section 215 of the PATRIOT Act, the corporations turned over the information but did not disclose to anyone, including the surveillance subjects, that they had done so. One slide referenced the two types of collection the program uses: upstream, which collects communications on “fiber cables and infrastructure as data flows past” (NSA 3). The other collection took data directly from the servers of the aforementioned companies, calling into question how voluntary corporate cooperation with the NSA actually is.

Indeed, the NSA’s cooperation appears to be limited and coercive. Aside from working with the four other countries (Australia, Canada, New Zealand, and the UK) in the Five Eyes, there was no evidence in the NSA documents of cooperation with other countries. Rather, the governments of literally every other country not in the Five Eyes were authorized as surveillance targets, along with “Entities openly acknowledged by a Foreign Government or Governments to be Directed and Controlled by Such Foreign Government or Governments” (NSA 1). This list included the United Nations, the World Bank, the European Union, the African Union, and OPEC (NSA 1). The secretive nature of warrants provides no recourse for appeal and, as a whole, the NSA programs make a mockery of the standardization and cooperation exalted in the reports and guidelines as a valuable method for protecting privacy.

The themes that emerged throughout the analysis of the data in this study, when compared together, paint a picture of post-9/11 dataveillance. Technological innovations made this type of surveillance possible, but the social insecurity and desire for protection in an uncertain world that followed the 9/11 terrorist attacks allowed a fundamental change in the existing legal framework. The PATRIOT Act, which codified those changes, was inconsistent with the previous laws analyzed in this study because it limited civil liberties and extended governmental surveillance powers where the earlier laws extended privacy protections and standards of government transparency and accountability. Additionally, the PATRIOT Act relied heavily on the invocation of terrorist threats to justify the changes it made; the earlier laws never reference these threats at all.

The reports and guidelines were most thematically similar of all the document groups, consistently portraying technology as a facilitator of data mining programs. The social risks and benefits of these technologies were thoughtfully considered in both the reports and guidelines; neither the laws nor the NSA documents considered these potential ramifications. Privacy was also presented as a fundamental and constitutionally protected American right in the reports and guidelines. While the laws did not discuss privacy in the same way as the reports and guidelines, the ECPA and the Privacy Act both extended individual privacy protections, and therefore were thematically similar to the reports and guidelines in that respect. The PATRIOT Act continued to be distinct from the other laws, but it too contained provisions designed to protect privacy. Meanwhile, the NSA documents were again inconsistent, adhering to legal standards but employing methods of privacy protection that the reports and guidelines discredited. The NSA documents also contained no references to the ideological importance of protecting privacy. Furthermore, while the reports and guidelines presented external oversight and transparency as essential for democratic government, and standardization and cooperation as a valuable tool for protecting data, the NSA documents demonstrated only internal oversight, no transparency, and used “cooperation” to access increasing amounts of personal data.

Discussion

Hypothesis 1: The NSA documents will display different themes than the reports, laws, and guidelines.

Finding: The NSA documents displayed similar themes as the other document categories, but their meaning often contradicted their usage in the reports, laws and guidelines. The risk society model predicts that attempts to predict risk in contemporary society results in contradictions, but the control society model would portray this contradiction as a deliberate attempt to mislead the public.

Hypothesis 2: The reports and guidelines will be thematically consistent.

Finding: Of all the document categories, the reports and guidelines were the most thematically consistent.

Hypothesis 3: The laws will be thematically consistent with the reports and guidelines.

Finding: The laws were not thematically consistent with each other, and the PATRIOT Act curtailed civil liberties where the ECPA and the Privacy Act protected them. The laws were more similar to the reports and guidelines than the NSA documents, but were a distinctive category.

Hypothesis 4: The control society theoretical model predicts that data collection will be haphazard, corporations and competition will play a prominent role in surveillance, codes will be used to de-individuate targets of surveillance, and the intent of surveillance is to control populations.

The risk society theoretical model predicts that data collection will be actuarial and precise, based on risk models and focused on risk prevention.

The risk society theoretical model is the best theoretical explanation of post-9/11 surveillance, as represented by the NSA's surveillance program.

Finding: The NSA surveillance programs collected data haphazardly and corporations played a prominent role in surveillance. Codes were used to de-individuate targets of surveillance, but the question of intent is subjective. Given the scope of the surveillance programs' data collection, the collected information cannot currently be analyzed effectively. Contradictions are inherent in the program, and its existence is justified by the presence of terrorist threat. Both the risk society and control society models are applicable to the NSA's surveillance programs.

The results illuminate a discrepancy between public and private governmental representations of privacy and transparency that is best explained by the risk management theoretical model. Although the public documents were fairly consistent across the laws, reports, and guidelines, with the guidelines and reports almost thematically indistinguishable, the NSA documents employed different language and thematic representations. For example, standardization and cooperation was presented in the reports and guidelines as a tool for enhancing privacy protections, but in the NSA documents was a way of collecting even more data, often without the consent of the "cooperating" parties. Similarly, collection limitation was presented in the reports and guidelines as a way of limiting outside intrusion into consumers' records, but in the NSA documents was portrayed as a limitation to be overcome. NSA's surveillance programs are justified by previous threats but focused on the prevention of further crimes. Furthermore, the volume of information indicates a lack of both control and oversight in the face of unknowable dangers. The risk management theoretical model therefore best explained the thematic differences in the public documents versus the NSA documents, but the control society model also appeared to have some applicability.

While similar themes were present across all of the document groups, the portrayal of these themes was most consistent across the reports and guidelines. Themes in the reports and guidelines also tended to be consistent with those in the laws, which formed a more distinct category because of their formal, legal construction. However, the majority of themes in the NSA documents were inconsistent with the other document categories. This was only partially explained by their technical nature, and indicated deliberate framing in the public documents to convey a message more harmonious with American ideals of privacy and freedom. One reason the NSA documents were so distinct is that they, like the laws, were written differently from the reports and guidelines. They were by far the most technical documents; the NSA is fundamentally a bureaucratic organization, and the majority of the NSA documents were intended for technicians, to serve as progress reports and provide training. Unlike the public documents, the NSA documents were also obviously not intended for an external audience. Thoughtful treatment of American ideals had no place in the NSA documents; the intended audience was presumably already convinced of the merits of the program. Still, practical explanations for the dissimilarity of the NSA documents to the rest of the documents used in this study did not fully justify the discrepancies. These discrepancies, particularly those regarding privacy protection and the importance of oversight and accountability, appear to confirm the direst predictions about the PATRIOT Act. While the most controversial sections have not been allowed to expire, they have also not been amended to provide additional oversight or accountability, and the NSA remains a wing of government almost wholly free from external review. Without the Snowden leaks, the program would still be entirely hidden from the public; NSA and other programs like it are apparently exempt from the requirements of accountability and transparency that the reports, guidelines, and laws all portray as essential for democracy.

Indeed, there were major discrepancies in the portrayal of accountability and transparency between the public and NSA documents. The reports and guidelines referred to the important roles that accountability and transparency play in protecting freedoms, and stated that neither the government nor the private sector should be exempt from these requirements. Moreover, the reports and guidelines written for the Obama administration professed a particular commitment to the principles of accountability of transparency and discussed a number of steps the administration has taken to ensure transparency. In addition, the Consumer Data Privacy Report also discussed how technology allows the government to more easily hold businesses accountable for upholding standards of data privacy protections. The laws, meanwhile, codified the privacy protections discussed in the reports and guidelines. The Freedom of Information Act, for example, set standards for governmental transparency and enabled citizens to access information collected about them. However, the PATRIOT Act was dissimilar from the other laws in this study because, while they all dealt with surveillance, the ECPA and the Privacy Act both elevated the importance of individual privacy protections while the PATRIOT Act limited privacy protections and expanded government surveillance, using the threat of terrorism as a justification. The laws used in this study were all created in response to specific events that demonstrated shortcomings in the existing legal frameworks. However, while the ECPA and Privacy Act were a response to public pressure for increased privacy protections, the PATRIOT Act was passed in a climate of instability and fear that followed the 9/11 attacks. That it expanded government surveillance powers where the earlier laws limited them lends support to the Risk Society model, but also could be construed as supporting the control and surveillant assemblage explanations of the advance of government power and erosion of democratic safeguards and process.

Where the Freedom of Information Act increased individual access to information that the government collects on them, the PATRIOT Act instead dictated that information collected on foreign nationals and suspected terrorists, or even information collected incidental to the pursuit of foreign nationals or suspected terrorists, is explicitly not subject to the protections given by the Freedom of Information Act. Furthermore, although the PATRIOT Act did include accountability and privacy protections, explicitly banning searches based solely on constitutionally protected rights and requiring law enforcement officers and agencies to track their investigations and report to Congress semi-annually, these are limited protections. James Clapper, the head of the NSA, lied to Congress in 2013 about the collection of bulk data, a fact that only came to light because of the Snowden leaks. This raises serious questions about the effectiveness of the accountability provisions contained within the PATRIOT Act. Because only a small number of people are actually privy to the exact nature of governmental bulk data collection initiatives, standards of accountability and transparency are nearly impossible to enforce. Without evidence, lies are indistinguishable from facts and, in order to protect the ideals of privacy and transparency present in the reports and guidelines, provisions should be made to enhance accountability.

Currently, the FISA Court, established to support the legality of covert data mining programs, is the only means of external oversight for the NSA program, and its work ends when it either grants or denies permission for searches. Since its creation, it has only denied eleven of more than 33,900 (.03%) requests for surveillance (Eichelberger 2013) and the NSA documents raise serious questions about the extent of the government's commitment to transparency, as well as the limitations of accountability in top-secret data mining initiatives. The NSA operates like a fourth branch of government, wholly opaque and subject to none of the checks and balances enshrined in the Constitution to protect the people from governmental overreach.

The documents' discussion of terrorism raised further questions about motives. Although in the public documents terrorism was really only discussed in the PATRIOT Act and "Safeguarding Privacy", those two documents discussed it at such length, that it appeared to be a justification for unprecedented governmental surveillance. In the documents that discussed it, terrorist threats were presented as unprecedented: "This new threat is unlike anything the nation has faced before" (DOD 2004:1). This appeared to be deliberate framing and functioned as a powerful justification: since both modern technology and the threat the U.S. faces from terrorism are unprecedented, unprecedented uses of terrorism are justified. One explanation for this discrepancy is the timing of the documents: The PATRIOT Act was passed slightly over a month after the 9/11 attacks, and "Safeguarding Privacy" was written in 2004, when the attacks were still relatively fresh, thereby making terrorism a more evocative justification for amending freedoms and implementing dataveillance than at other points in time. Additionally, the change of Presidential administrations between those and later documents might also account for a change in focus.

Moreover, risk prevention was a consistent theme across all four document categories. Discussions of technology were likewise prominently featured in all four document categories and often interwoven with discussions of risk prevention, but these discussions were not consistent between the public and NSA documents. As usual, the reports and guidelines were consistent with each other, addressing similar aspects of technology and extolling the benefits of both technology and the data mining it facilitates. The reports and guidelines also acknowledged some of the controversy about privacy rights generated by governmental and corporate uses of technology and paid particular attention to the use of big data to stimulate economic productivity and growth. Meanwhile, the NSA documents' discussion of the benefits and problems with technology centered not on ethical dilemmas, but rather ways of overcoming technological limitations that limit data collection. For example, while use/collection limitation is portrayed in the reports and guidelines as a method of protecting individual data privacy, in the NSA documents, the code was used in documents that described collection limitations as an obstacle to be overcome. The connotation of collection limitation in the NSA documents, therefore, was entirely negative, while in the reports and guidelines it was positive. Indeed, in the NSA documents all limitations on data collection were considered negative; the intent of the program, as described in the PowerPoints by its technicians, was to collect and store ever-increasing amounts of data. Every technological advance that facilitated this was celebrated.

While the justifications for collection and also the uses of the data by NSA adhered more strictly to the risk society model, the emphasis on collecting massive amounts of data adhered more closely to the control society theoretical model. Rather than the actuarial precision predicted by the risk society model, the NSA programs actually appeared to demonstrate the haphazard data collection predicted by the control society model. Both the risk society and control society models were suggested by the NSA's analysis of its abundance of data with sophisticated tools and models, but their ultimate emphasis on predicting and averting disaster through their unbridled data collection still indicates the risk society model.

The risk society model was further suggested by the emphasis on crime prevention present in the reports, guidelines, laws and NSA documents. As represented in the reports and guidelines, the intent of surveillance was not to discipline or control the American population but rather prevent future undesirable events. Additionally, targets of surveillance in the NSA documents were foreign nationals and suspected terrorists, but the sheer volume of collected data implied that true control remains elusive, another important component of the risk society model. Control is elusive precisely because of the lack of oversight. While before, because of the relative difficulty of obtaining permission for them, searches used to be necessarily targeted, the staggering amount of information collected by the NSA program actually obscures useful data.

The "cooperation and standardization" code was another demonstration of the thematic differences between the NSA documents and the public documents, but was more suggestive of the flows of information facilitated by technology than any specific theoretical surveillance model. A broad code, present across all four document categories, "cooperation and standardization" was applicable to many different aspects of big data collection and use. For example, the reports and guidelines suggested cooperation as a way to increase the potential of big data, and cooperation and standardization between government and private sector systems was encouraged, as was intra-governmental and industry-wide standardization. In the reports and guidelines, cooperation and standardization was further presented as having the potential to maximize economic potential, enhance privacy protection, and increase national security. However, its representation in the NSA documents suggested both that this cooperation is not always voluntary, as in the case of the NSA directly tapping into company servers without the company's consent, and potentially detrimental to civil liberties, as when intelligence agencies share information obtained under FISA with law enforcement officials, thereby circumventing Title III.

The NSA documents demonstrated interest in legality further implied the risk society model. While, unlike in the reports and guidelines, there were no lengthy discussions of the trade-offs between benefits and drawbacks of technology, and there were only tangential references to privacy protection, such as discussions of "minimizing" data collected on American citizens, there were several references to following rules, laws and protocols. The NSA program did not appear to be run by a group of reckless lawbreakers, but debates about the morality of the program were wholly absent. Again, the documents were technical in nature and so discussions like those found in the reports and guidelines would be out of place. The interest in legality underscored the bureaucratic nature of the organization; these were not the people charged with writing the laws but rather the technicians who implemented the programs created by changes in laws. Still, the demonstrated interest in legality again suggested that, rather than a semi-nefarious attempt to control unruly populations, the NSA program is rather an example of a sprawling, disjointed government trying to prevent future risks.

However, while the NSA documents included in this study indicate an interest in legality and use internal audits and enforcements to ensure compliance, the lack of external oversights individuate the program from the ideals presented in the reports and guidelines, and the lack of transparency and accountability itself constitutes a threat. While the government extolled its attempts to regulate commercial collection and use of data in its official reports, the NSA documents demonstrated that governmental collection and use of data is similarly unregulated, and the government uses data collected in the private sector for purposes not intended at the time of its collection, making the government a questionable regulator.

There were several other instances of framing throughout the data collected. Privacy was consistently portrayed as a fundamental American right and value across the reports, guidelines, and laws. Both the reports and guidelines made the case for extending American ideals of privacy to non-citizens, and Presidential administrations were portrayed as committed to upholding the privacy principle and all other constitutionally protected freedoms. It would be an admittedly hard sell to do otherwise, and stating in a public document that privacy is important and non-citizens deserve the same protections as citizens is not the same as codifying these protections through the legal system. In this case, what appeared more important was what was not said: while the reports and guidelines lauded steps taken to protect privacy, they omitted discussions of the steps taken to infringe upon existing privacy protections. Threats to privacy resulting from governmental uses of technology were likewise minimized. While threats were discussed, they were portrayed as resulting primarily from external parties. The American government was portrayed as committed to transparency and accountability and also as a protector of constitutional rights and freedoms. Top-secret surveillance programs were understandably not discussed, but leaks of previously confidential information were likewise ignored. The only report written after the Snowden leaks, The Big Data Report, was commissioned by President Obama in response to outcry resulting from the leaks but mentioned them only once. Calling them an example of "insider threat," the report lumped in Snowden with military personnel who attacked their own bases, entirely sidestepping the issue of his motivations, or the general reaction of the American public at discovering their government had been covertly collecting massive amounts of data from major Internet companies for years. The vague discussion of potential threats to privacy resulting from technology and big data in that report therefore seemed to be a way of appearing to address issues while sidestepping controversy. While the use of framing was not necessarily indicative of any theoretical model, it did suggest an attempt at controlling the perceptions and beliefs of the public and therefore appears to be more suggestive of the control society model than the risk society model.

The NSA programs' wide range of targets and demonstrably varied reasons for targeting individuals, corporations, and foreign nations for surveillance further indicated limitations to the applicability of the risk management model. The economic motivations and struggle for dominance in the world economy demonstrated in the NSA documents were more consistent with the Control Society model than the risk society model. Echoes of attempts at control were also demonstrated in the PATRIOT Act, particularly in Section 1016, which discussed cyber and physical infrastructure maintenance necessary for, among other things, economic prosperity. It did not refer to the necessity of covert surveillance programs or corporate complicity to achieve these economic advantages but its emphasis on economic superiority, which was also present in the reports and guidelines, suggested less than wholly altruistic or fear-based motives for surveillance. Both the control society and risk society models apply to the findings of this study; neither was demonstrably incorrect. While the current state of surveillance resembles a risk society, this study does not preclude the future possibility of a society that more closely resembles control society if the NSA programs continue as they are. Paradoxically, revelations about the NSA's programs, by furthering individual perceptions of surveillance, may even speed this process causing individuals to modify their behavior, just like the prisoners did in Foucault's Panopticon.

Conclusion

Contemporary surveillance is not only ubiquitous in contemporary society but is also increasingly palatable to the general public. While the government justifies its data collection by the presentation of threats, the public is already accustomed to willingly surrendering its information to online businesses in exchange for perceived rewards, something that the risk society model does not wholly predict. Meanwhile, while the heterogeneity of contemporary society suggests the futility of any kind of control model, incarceration rates in this country indicate that the government has not abandoned its attempts at control. However, the risk society model appeared to be the most appropriate theoretical model to explain the results of this qualitative analysis of the NSA's surveillance program. While the inconsistencies between the public and private documents suggested deliberate attempts to frame, or control, the message received by the American public, indicating that aspects of the control society model are also present in post-9/11 surveillance society, the unwieldy size of the programs, the implied and discussed threats present throughout the document categories, and the emphasis on preventing future undesirable events most strongly suggested the risk society model. As indicated by the literature, technology plays a large role in facilitating surveillance programs. However, without the precise convergence of a catastrophic terrorist attack and the subsequent change in law, contemporary surveillance would not be possible (or, at least, legal). After 9/11, a daily barrage of threats are presented to the American public—whether it be ISIS, or Al Qaeda, or nuclear weapons in Iran, or cyber attacks by China—and provide continuing justification for the existence of programs like the NSA's. What used to be unthinkable has become routine and contemporary society is shaped by the ongoing, unending struggle to avert undesirable and unpredictable future events.

Contemporary surveillance is complex in every way, its existence possible because of interconnected networks and unprecedented technology, but equally facilitated by social and legal changes. This study demonstrated the limitations of the existing legal system to protect privacy given the continuously and rapidly evolving nature of technology and the will to collect ever more data on more and more citizens, both foreign and domestic. The protections suggested in the reports and guidelines were practically unenforced, and the NSA was shown to operate as a wholly opaque branch of the government. The NSA's surveillance programs were consistent with each of the theoretical models studied, lending credence to both. Still, the program substantively cannot enact the type of control consistent with either the control society or disciplinary model, and so the risk society was shown to be the most appropriate model to explain contemporary 9/11 surveillance. As technology progresses, however, so too will surveillance, creating the possibility that a control society will eclipse risk society. The most effective way of combatting this eventuality is the legal system; changes made or suggested outside this system lack the enforceability necessary for implementation. Further empirical studies of contemporary surveillance are also necessary to provide more data about the characteristics of specific surveillance programs and the demonstrable effects of this surveillance.

Works Cited

ACLU. 2011. *Reform the Patriot Act | A Primer.* (Retrieved from https://www.aclu.org/free-speech-national-security-technology-and-liberty/reform-patriot-act-primer on October 27, 2014).

Agger, Ben. 1991. "Critical Theory, Poststructuralism, Postmodernism: Their Sociological Relevance." *Annual Review of Sociology*. 17(1991): 105-131.

Amoore, Louise and Marieke De Goede. 2005. "Governance, risk and dataveillance in the war on terror." *Crime, Law & Social Change.* 43: 149-173.

Bankston, Kevin S. 2007. "Only the DOJ Knows: The Secret Law of Electronic Surveillance." *University of San Francisco Law Review*. 41:589-635.

Beck, Ulrich. 2000. "Risk Society Revisited: Theory, Politics and Research Programmes" *The Risk Society and Beyond: Critical Issues for Social Theory.* Ed: Adam, Barbara, Ulrich Beck and Joost Van Loon. Thousand Oaks: California. SAGE Publications, Ltd.

Beck, Ulrich. 2006. "Living in the world risk society." *Economy and Society*. 36(2006):329-345.

Bennett, Colin J. 2011. "In Defence of Privacy: The concept and the regime." *Surveillance and Society*. 8(4): 485-496.

Bennett, Colin J., Andrew Clement and Kate Milberry. 2012. "Editorial: Introduction to Cyber-Surveillance." *Surveillance and Society.* 9(4): 339-347.

Best, Samuel J. and Brian S. Kreuger. 2008. "Political Conflict and Public Perceptions of Government Surveillance on the Internet: An Experiment of Online Search Terms." *Journal of Information Technology & Politics*, 5(2):191-212.

Boyle, James. 1997. "Foucault in cyberspace: Surveillance, sovereignty, and hardwired censors." *University of Cincinnati Law Review*. 66: 177-205.

Campbell, John Edward and Matt Carlson. 2002. "Panopticon.com: Online Surveillance and the Commodification of Privacy." *Journal of Broadcasting & Electronic Media*. 46(4):586-606.

Deleuze, Gilles. 1990. "Postscript on the Societies of Control." *October*. 59: 3-7.

Department of Defense, Technology and Privacy Advisory Committee. 2004. *"Safeguarding Privacy" in the Fight against Terrorism (TAPAC Report).*

Dupont, Benoît. 2008. "Hacking the Panopticon: Distributed Online Surveillance and Resistance. *Sociology of Crime Law and Deviance.* 10:259-280

Eichelberger, Erika. 2013. "FISA Court Has Rejected .03 Percent of All Government Surveillance Requests*. Mother Jones.* Retrieved April 20, 2015. (http://www.motherjones.com/mojo/2013/06/fisa-court-nsa-spying-opinion-reject-request).

Electronic Privacy Communications Act of 1986 (ECPA), Public Law 99-508, Statutes at Large 100 (1986).

Executive Office of the President. 2014. *Big Data: Seizing Opportunities, Preserving Values.* Washington, D.C. Retrieved March 11, 2015. (https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf)

Epic.org: Electronic Privacy Information Center. 2014. *Electronic Communications Privacy Act: Introduction to ECPA.* (Retrieved from http://epic.org/privacy/ecpa on October 27,2014).

Fernandez, Luis, Amory Starr, John Noakes, and Manuel Caro. 2006. "Does Surveillance Chill? The Impacts of Government Surveillance on Progressive Political Activity in the US, 1998-2005." Paper presented at the annual meeting of the American Sociological Association, Montreal Convention Center, Montreal, Quebec, Canada Online.

Flick, Uwe, Ernst von Kardoff, and Ines Steinke. 2004. *A Companion to Qualitative Research*. London: SAGE Publications.

Foucault, Michel. 1989. *Discipline and Punish*, trans. Alan Sheridan. New York: Random House.

Giddens, Anthony. 1990. "Post-Modernity or Radicalized Modernity?" *Social Theory: The Multicultural and Classic Readings*. Ed. Charles Lemert. Boulder, CO: Westview Press. 485-491.

Green, Stephen. 1999. "A Plague on the Panopticon: Surveillance and power in the global information economy." *Information, Communication & Society.* 2:1: 26-44.

Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State.* New York, NY: Metropolitan Books

Haggerty, Kevin D. and Richard V. Ericson. 2000. "The surveillant assemblage." *British Journal of Sociology*. 51(4): 605-622.

Kelley, Michael B. 2013. "NSA: Snowden Stole 1.7 MILLION Classified Documents and Still Has Access To Most Of Them." *Business Insider*, December 13. Retrieved December 11, 2014 (http://www.businessinsider.com/how-many-docs-did-snowden-take-2013-12).

Kreuger, Brian S. 2005. "Government Surveillance and Political Participation on the Internet." *Social Science Computer Review*. 23(4):439-452.

Lipton, Jacqueline D. 2009. "Digital Multi-Media and the Limits of Privacy Law." *Case Western Reserve University Journal of International Law*. 42(3): 551-571.

Lyon, David. 2001. "Facing the Future: Seeking ethics for everyday surveillance." *Ethics and Information Technology*. 3: 171-181.

Lyon, David. 2002. "Editorial. Surveillance Studies: Understanding visibility, mobility, and the phenetic fix." *Surveillance and Society*. 1(1):1-7.

Lyon, David. 2004. "Globalizing Surveillance: Comparative and Sociological Perspectives." *International Sociology*. 19(2): 135-149.

Lyon, David. 2007. "Surveillance, Security and Social Sorting: Emerging Research Priorities." *International Criminal Justice Review*. 17(3): 161-170.

Lyon, David. 2014. "Surveillance, Snowden, and Big Data: Capacities, consequences, critique." *Big Data & Society.* 1(2): 1-13.

Mann, Susan Archer. 2012. *Doing Feminist Theory: From Modernity to Postmodernity*. New York: Oxford.

Marx, G.T. 2007. "Desperately Seeking Surveillance Studies: Players in Search of a Field." *Contemporary Sociology.* 36(2): 125-130.

Marx, Gary T. and Glenn W. Muschert. 2007. "Personal Information, Borders, and the New Surveillance Studies." *Annual Review of Law and Social Science*. 3: 375-395.

Morgan, David L. 2014. *Integrating Qualitative and Quantitative Methods*. New York:SAGE Publications.

OECD. 2013. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* (Retrieved from http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm on October 27, 2014).

Orwell, George. 1949. *1984*. New York, NY: Harcourt, Brace and Company.

Oulasvirta, Antti, Aurora Pihlajamaa, Jukka Perkio, Debarshi Ray, Taneli Vahakangas, Tero Hasu, Niklas Vainio, Petri Myllymaki. 2012. "Long-term Effects of Ubiquitous Surveillance in the Home." Paper presented at *UbiComp* Annual Conference, Sept. 5-8, Pittsburgh, USA. Retrieved December 12, 2014 (https://people.mpi-inf.mpg.de/~oantti/pubs/ubicomp2012-oulasvirta.pdf).

Privacy Act of 1974, Public Law 93-579, Statutes at Large 88 (1974).

Posner, Richard A. 2008. "Privacy, Surveillance, and Law." *University of Chicago Law Review.* 75: 245-260.

Saldana, Johnny. 2012. *The Coding Manual for Qualitative Researchers.* Thousdand Oaks, CA: SAGE Publications.

Simone, Maria A. 2009. "Give me liberty and give me surveillance: a case study of the US Government's discourse of surveillance." *Critical Discourse Studies*. 6(1):1-14.

Stanley, Jay. 2004. *The Surveillance-Industrial Complex: How the American Government is Conscripting Businesses and Individuals in the Construction of a Surveillance Society.* American Civil Liberties Union (ACLU). New York, NY: ACLU. Retrieved 19 October, 2014 (https://www.aclu.org/files/FilesPDFs/surveillance_report.pdf)

Torpey, John. 2007. "Through Thick and Thin: Surveillance after 9/11." *Contemporary Sociology*. 36(2): 116-119.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Public Law 107-56, Statutes at Large 115 (2001).

U.S. Department of Health and Human Services (HHS). 2014. *The Privacy Act | HHS.Gov.* (Retrieved from http://www.hhs.gov/foia/privacy/ on October 27, 2014).

U.S. Privacy Protection Study Commission. 1977. *Personal Privacy in an Information Society (Privacy Commission Report*). Retrieved March 11, 2015 (http://epic.org/privacy/ppsc1977report).

Waldo, James. 2007. "Executive Summary." Pp 1-15 in *Engaging Privacy and Information Technology in a Digital Age*, edited by J. Waldo, H.S. Lin and L.I. Millett. National Academies Press.

Warren, Samuel D. and Louis D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review.* 4(5).

Westin, Alan F. 1968. *Privacy and Freedom.* New York, NY: Atheneum.

The White House, Office of the Press Secretary. 2011. *FACT SHEET: Cybersecurity Legislative Proposal*. Retrieved March 11, 2015 (http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal on October 27, 2014).

The White House. 2012. *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*. Retrieved March 11, 2015 (https://www.whitehouse.gov/sites/default/files/email-files/privacy_white_paper.pdf).

Wilshusen, Gregory C. 2012. *Federal Law Should be Updated to Address Changing Technology Landscape,* Testimony before the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, U.S. Senate.

Willcocks, Leslie P. 2006. “Michel Foucault in the Social Study of ICTs: Critique and Reapparaisal.” Working paper, Department of Information Systems, London School of Economics and Political Science, London, UK.

Zedner, Lucia. 2005. “Securing Liberty in the Face of Terror: Reflections from Criminal Justice.” *Journal of Law and Society*. 32(4): 507-533.

Appendix: NSA documents[*]

NSA 1: *In the Matter of Foreign Governments, Foreign Factions, Foreign Entities, and Foreign-Based Political Organizations DNI/AG 702(g) Certification 2010-A*. Contains a list of foreign governments "not recognized by the United States," factions of foreign nations substantially not composed of U.S. persons, entities openly acknowledged by foreign governments, foreign-based political organizations, and entities controlled by foreign governments that are subject to U.S. dataveillance.

NSA 2A, NSA 2B, NSA 2C: A list of frequently asked questions about Boundless Informant, this document has been declassified and explains what the program does.

NSA 3A, NSA 3B, NSA 3C, NSA 3D: A PowerPoint for Global Access Operations explaining how Boundless Informant differs from previous programs, details about the program, and technical tips for executing the program.

NSA 4: This graphic shows the amount of data collected each day for the last 30 days, the largest volume of records collected (6,142,932,557 records), and the top 5 techs.

NSA 5: This document contains a map showing where data collection is available across the globe.

NSA 6: Dated Jan 2008, this document includes an overview of records collected across the globe, including a breakdown of Digital Network Intelligence (DNI) and Dial Number Recognition (DNR) records collected by country. A pop-up detail shows that 203,190,032 records have been collected in the United States.

NSA 7: This document contains collection information for the United States, including project names, the top 5 projects, the top 5 validator IDs, and the top 5 IP addresses.

NSA 8: This chart shows collection information for France for the last 30 days, including a graph broken down by day, the most volume and the top 5 techs.

NSA 9: A review of October through December 2011, this document discusses CNE access to Belgacom GRX Operator.

NSA 10: This document discusses VALIDATOR, a backdoor access program under FOXACID that targets Windows computers.

NSA 11: This document discusses OLYMPUSFIRE, a software implant on Windows PC that provides the NSA 24/7 access to the targeted computers.

NSA 12: QUANTUM, another program within the NSA's surveillance program, is targeted for yahoo, Facebook, and static IP systems. A list of realms it can target is included.

[*] All documents received from TheIntercept.com

NSA 13A, NSA 13B, NSA 13C, NSA 13D, NSA 13E, NSA 13F: These documents contain illustrations how QUANTUM works.

NSA 14: Another slide about QUANTUM, this document contains information on who can use the program and how targets are selected.

NSA 15: Also about QUANTUM, this slide explains how to exploit web browsing with QUANTUM.

NSA 16A, NSA 16B, NSA 16C, NSA 16D, NSA 16E, NSA 16F: These documents contain technical information about how to collect data using QUANTUM.

NSA 17: This document discusses QUANTUMNATION and how it works.

NSA 18A, NSA 18B: These documents contain technical information for using FOXACID.

NSA 19: A graph showing collection information for Poland over the last 30 days, including a breakdown by days, the most information collected, and the top 5 techs.

NSA 20: This PowerPoint slide shows the corporate cooperators and discusses same-day cooperation between the NSA/CSS Threat Operations Center (NTOC) and the FBI.

NSA 21: This PowerPoint slide also shows the corporate cooperators and contains a graphic demonstrating how the NSA program works.

NSA 22: This PowerPoint slide shows NSA Based Reporting June 2011-May 2012.

NSA 23: This PowerPoint Presentation is an overview of NSA and how it works with the help of corporate collaborators.

NSA 24: A week in the life of NSA reporting, this document shows a sampling of reporting topics from February 2-8, 2013 for Mexico, Japan, and Venezuela.

NSA 25: This affidavit demonstrates how information collected through the use of dataveillance was used in a domestic criminal trial.

NSA 26: This PowerPoint presentation contains an overview of the AURORAGOLD program: "The mission of the AURORAGOLD (AG) project is to maintain data about international GSM/UMTS networks for the Wireless Portfolio Program Office (WPMO), the Target Technology Trends Center (T3C/SG4), and their customers. Analysis of this data supports: a) An understanding of the current state, b) Trending, or time-series analysis, from the past through to the future, and c) Forecasting of the evolution of global GSM/UMTS-based networks."

NSA 27: A PowerPoint presentation on AURORAGOLD, this contains future technology trends, illustrations of how AURORAGOLD works, and goals for future data collection with AURORAGOLD.

NSA 28: The AURORAGOLD working aid, this document contains technical information for using the program.

NSA 29: Designed for the SIGDEV conference in June 2012, this presentation contains information about AURORAGOLD and why it should be more broadly used.

NSA 30: This document contains the DTI's strategic accomplishments for 2013

NSA 31: This short memo addresses large router hacking and enumerates ways in which this ability can aid surveillance.

NSA 32: This presentation demonstrates the acceleration of technology; detecting Network Operation Centers (NOC) is now automated.

NSA 33: This presentation serves as a "roundtable," discussing ways to improve data collection.

NSA 34: Titled *Mobile Networks in MyNOC World*, this presentation contains technical information, a picture of Prince Charles and Camilla attending a presentation, and also evidence of collaboration to enable better exploitation of Belgacom.

NSA 35: This report discusses NSA invisibility across 18 programs, including several anti-virus softwares.

NSA 36: Titled *IR.21 – A Technology Warning Mechanism*, this presentation discusses emerging models for trends and forecasting, wireless evolution paths, analytic frameworks, and AURORAGOLD.

NSA 37: This memo is about sharing metadata beyond the NSA.

NSA 38: This document is for employees being "indoctrinated" on SENTRYEAGLE, and contains information about that program.

NSA 39: This is an administrator's guide for *Hacking Team*: "The Hacking Suite for Governmental Interception."

NSA 40: This is a system administrator's guide for *Hacking Team*: "The Hacking Suite for Governmental Interception."

NSA 41: This is an analyst's guide for *Hacking Team:* "The Hacking Suite for Governmental Interception."

NSA 42: This is a technician’s guide for *Hacking Team:* “The Hacking Suite for Governmental Interception.”

NSA 43: This presentation addresses sharing communications across the U.S. Intelligence community, a program called ICREACH.

NSA 44: This document celebrates the first-ever collection of a 4G Cellular signal, in 2010.

Vita

The author was born in Culver City, CA. She obtained her Bachelor's degree in advertising from Boston University in 2007. She joined the University of New Orleans sociology graduate program in 2013.