Title

Watching the Watchers: Surveillance in the United States

Author

Burke, Colin

Publication Date

2022

UNIVERSITY OF CALIFORNIA SAN DIEGO

Watching the Watchers: Surveillance in the United States

A dissertation submitted in partial satisfaction of the
requirements for the degree Doctor of Philosophy

in

Sociology (Science Studies)

by

Colin Maxwell Burke

Committee in charge:

Professor Kevin Lewis, Chair
Professor Amy Binder
Professor John Evans
Professor Kelly Gates
Professor Juan Pablo Pardo-Guerra

2022

The Dissertation of Colin Maxwell Burke is approved, and it is acceptable in quality and form for publication on microfilm and electronically.

University of California San Diego

2022

DEDICATION

To Stephie, Calvin,
& my grandparents.

TABLE OF CONTENTS

LIST OF FIGURES

Chapter 2

Chapter 3

Chapter 4

LIST OF TABLES

Chapter 2

Chapter 3

ACKNOWLEDGMENTS

I would like to first thank my advisor and dissertation chair, Kevin Lewis, for his incredible mentorship, support, and guidance during my time at UCSD. Words cannot adequately express my gratitude and appreciation for everything that Kevin has done for me at every stage of my graduate career. I am also thankful to my committee members – Amy Binder, John Evans, JP Pardo-Guerra, and Kelly Gates – who have been incredibly supportive throughout my UCSD journey and challenged me to become a better scholar and writer. I also want to extend many thanks to our wonderful graduate coordinator, Teresa Eckert, who has been a constant source of support in navigating the uncertainties and administrative hurdles of graduate school. I would also like to extend my sincere gratitude to all the faculty in the UCSD Sociology department and Science Studies program that I have worked with and learned from over the years.

I would also like to acknowledge my support system of family and friends. I am so grateful and appreciative of my wife, Stephanie, whose endless love, patience, and encouragement made this journey possible. Also, to my son, Calvin, who has been a source of inspiration and love when I need it most. I would also like to thank my parents who have provided me with love, support, and encouragement to pursue my dreams. I am also thankful to my fellow graduate students for their friendship and support, with special thanks to Armand Gutierrez, Hee Eun Kwon, Nima Rassooli, and Karina Shklyan.

Chapter 2, in full, is a reformatted reprint of the material as it appears in *Surveillance and Society* 2020. Burke, Colin. 2020. “Digital Sousveillance: A Network Analysis of the US Surveillant Assemblage.” *Surveillance & Society* 18(1): 74-89. The dissertation author was the primary investigator and author of this paper.

VITA

2013	Bachelor of Science, Sociology, Northern Arizona University
2013	Bachelor of Science, Criminology, Northern Arizona University
2015	Master of Science, Applied Criminology, Northern Arizona University
2020	Master of Arts, Sociology, University of California San Diego
2022	Doctor of Philosophy, Sociology (Science Studies), University of California San Diego

PUBLICATIONS

2018	"Political Action Committees." *The SAGE Encyclopedia of Surveillance, Security, and Privacy.* Bruce A. Arrigo, eds. Routledge. (co-authored with Lynn Jones).
2020	"Digital Sousveillance: A Network Analysis of the US Surveillant Assemblage." *Surveillance & Society* 18(1): 74-89.
2020	"Social Media Surveillance in Schools: Rethinking Public Health Interventions in the Digital Age." *Journal of Medical Internet Research* 22(11): e22612. (co-authored with Cinnamon Bloss).

ABSTRACT OF THE DISSERTATION

Watching the Watchers: Surveillance in the United States

by

Colin Maxwell Burke

Doctor of Philosophy in Sociology (Science Studies)

University of California San Diego, 2022

Professor Kevin Lewis, Chair

This dissertation represents a comprehensive study of modern surveillance practices in the US. Using large open sources of digital data and quantitative methodologies, I examine contemporary surveillance practices at three distinct levels: 1) structural: the nature and structure of the broader US surveillance network, 2) interactive: the positionality and connectivity between surveillance actors, and 3) physical/material: physical arrangement and material realities of digital infrastructures and surveillance actors. Such analyses are informed by a critical methodological lens of what I term digital sousveillance, which represents the co-optation of digital data and the use of computational methods and techniques to resituate technologies of control and surveillance of individuals to instead observe the observer. This methodological approach lends itself to an extensive range of methodological and theoretical tools, enabling critical examination of surveillance practices that are often hidden and, consequently, difficult to study. In evaluating and demonstrating the utility of such an approach, this dissertation explores the evolving structure of the network of public-private surveillance partnerships, examines the nature of the relationship between network embeddedness and economic capital in the context of surveillance organizations, and investigates the materiality of modern surveillance and its theoretical implications. In doing so, this research contributes to theoretical and empirical understandings of modern surveillance practices in the US, as well as a novel methodological approach to understanding them.

CHAPTER 1 — INTRODUCTION

Though often associated with today's institutions and technologies, the social practice of surveillance long pre-dates its modern conception. Early forms of surveillance, such as eavesdropping and the interception of physical communications, have been used for centuries (Locke 2010). Nonetheless, as will be discussed throughout this dissertation, modern forms of surveillance have transformed immensely from their earlier predecessors in terms of their nature, impact, and complexity. The transformations and changes to surveillance over the last several decades have not occurred in a vacuum, however; instead, they can be traced alongside broader societal shifts like industrialization and urbanization that affected almost every facet of contemporary social life. More recently, the rapid development of digital technologies, corporate and governmental infrastructures, and global interconnectivity has produced major societal shifts in power, identity, institutional practices, and interpersonal relations that have positioned surveillance as the dominant organizing practice of modernity (Lyon, Haggerty, and Ball 2012).

Today, it can be challenging to identify a single aspect of social life that remains untouched by surveillance. In many workplaces, employees are subject to constant monitoring of their activity to gauge performance and behavior (Ball 2009). Powerful nation-states, such as the US, have carried out mass surveillance programs that collect data and information about people around the globe in the name of national security and defense (Bamford 2009; Greenwald 2014; Maass and Poitras 2014). Even local law enforcement agencies in the US have been transformed by "big data" analytics and technological systems of surveillance that guide policing practices, often in harmful and discriminatory ways (Brayne 2017). Large corporations have also embraced surveillance as a capitalistic mode of operation, gathering massive amounts of behavioral, communications, and biometric data about consumers to pursue greater profits and power (Gates 2011; Zuboff 2019). These examples are just some of the ways that surveillance practices have shaped and defined modern institutions and daily life.

While the shape and scale of modern surveillance may be enough to render it an important object of study, it is also worth considering the broader significance and implications of modern surveillance for society. Though public attention to surveillance-related concerns may have dissipated since the immediate aftermath of the Snowden revelations, the US government's programs for conducting mass surveillance have not. As revealed in February 2022, the Central Intelligence Agency (CIA) has been conducting a secret mass surveillance program that has included the gathering of data belonging to American citizens (Volz 2022). With the prevalence of surveillance practices by governmental and private entities, it is reasonable to assume that the average person is subject to some form(s) of monitoring or data gathering.

As surveillance becomes more embedded in our daily lives, the implications of such practices become even more substantial. Rights to privacy and fourth amendment protections aside, surveillance can cast a chilling effect on the expression and speech of those who are aware or concerned that they are being monitored (Richards 2012). For instance, government mass surveillance of journalists has been shown to disrupt investigative styles of journalism that are crucial to holding powerful institutions accountable and rely upon keeping sources of information, such as whistleblowers, protected and confidential (Waters 2018). Also, as discussed in Chapter 4, the growth and scale of mass surveillance in the public and private sectors also pose serious environmental concerns. The increasing volume of data collection for surveillance purposes has led to the growth in the number of large data storage facilities that consume immense amounts of energy powered by fossil fuels (Masanet et al. 2020; Story 2014). Taken together, the consequences and implications of modern surveillance are significant and worthy of greater scholarly and public attention.

This introductory chapter lays the groundwork for the rest of the dissertation, starting with a brief background of the subfield of surveillance studies. It then concludes with a structural outline and overview of the research aims, objectives, and questions of the three middle chapters.

SURVEILLANCE STUDIES

Over the past two decades, such immense social changes have heightened academic interest in surveillance practices, resulting in the emergence and growth of the "surveillance studies" subfield, which has brought about a more organized, multidisciplinary approach to studying these phenomena. The contribution of this subfield is thus to "foreground empirically, theoretically and ethically the nature, impact, and effects of a fundamental social-ordering process" (Lyon et al. 2012). Surveillance studies scholars face considerable challenges and obstacles when studying their objects of interest compared to other disciplines and subdisciplines. Despite its ubiquitous nature, surveillance remains a social practice that is often concealed from the public and is thus, in many cases, unobservable. Even in the cases where surveillance practices are publicly visible and widely known, such as the efforts by private companies to gather massive amounts of data on consumers, the precise nature and scale of such practices remain a black box to the public.

Their complex, widespread, and evolving nature has made the conceptualization of modern surveillance practices challenging for surveillance scholars. While this dissertation makes no attempts to weigh in on such definitional debates, it is worth considering some of the ways that "surveillance" has been defined and operationalized in the field. As discussed further in Chapter 4, many conceptions of surveillance rely upon the ideas of Michel Foucault. This is especially the case when it comes to the concept of the "panopticon," which has served as the guiding metaphor for much theoretical work in surveillance studies. Nonetheless, as perhaps expected, there is no consensus on a definition of surveillance and scholars have produced a wide range of conceptualizations over the last few decades. Giddens (1986:181), for example, views surveillance through the lens of the nation-state: "Surveillance as the mobilizing of administrative power – through the storage and control of information – is the primary means of the concentration of authoritative resources involved in the formation of the nation-state." Similarly, Dandeker (1990:vii) defines surveillance, not in the "narrow sense of 'spying' of people but, more broadly, to refer to the gathering of information about and the supervision of subject populations in organizations." The inclusion of organizational power in such conceptualizations of surveillance is crucial as it highlights the role of particular actors in carrying out surveillance practices and its intrinsic linkages to existing power hierarchies. More critically, such definitions accentuate that surveillance practices are purposeful and often carried out under organizational actors' specific motives and agendas.

More recently, surveillance scholars have come to conceptualize surveillance as expanding outside the domains of organizations and governance to become more neutral and decentralized. Haggerty and Ericson's (2000) concept of the "surveillant assemblage," a key concept of the second chapter of this dissertation, portrays modern surveillance as a transformation of powerful observational hierarchies to enable instead the use of technologies for monitoring and scrutiny by both institutions and everyday citizens. Others, such as Hier (2003), have taken a more critical stance towards the apparent democratization of modern surveillance and instead view contemporary surveillance as processes of social control in ways that both level and reinforce societal hierarchies. Hier (2003) suggests that such a distinction is essential as it enables the appropriate formation of sites and modes of resistance as social and discursive rather than technological. Such theoretical contributions evidence the myriad ways that surveillance has been defined and conceptualized by scholars of surveillance studies. Undoubtedly, the development and emergence of new digital technologies and, as a result, new forms of surveillance will continue to shape scholars' conceptualizations of modern surveillance.

CHAPTER OVERVIEW

This dissertation represents a comprehensive study of modern surveillance practices in the US. More specifically, it examines contemporary surveillance practices in the US through the critical methodological lens of what I term "digital sousveillance." Digital sousveillance represents the "co-optation of digital data and the use of computational methods and techniques (e.g., network analysis) to resituate technologies of control and surveillance of individuals to instead observe the observer—as a method for studying surveillance" (Burke 2020:77). This methodological approach lends itself to an extensive range of methodological and theoretical tools, enabling critical examination of surveillance practices that are often hidden and, consequently, difficult to study. In demonstrating the utility of such an approach, this dissertation addresses the following broad research questions:

1. How can utilizing a digital sousveillance approach to studying surveillance contribute to our understanding of modern surveillance practices?
2. How has surveillance and, more specifically, the structure of the network of public-private surveillance partnerships changed from the 1970s to the 2000s?
3. What is the nature of the relationship between network embeddedness and economic capital in the context of surveillance organizations?
4. What can the material linkages between surveillance infrastructures and surveillance organizations tell us about the materiality of modern surveillance?

This dissertation investigates modern surveillance in the US at three distinct levels: 1) structural: the nature and structure of the broader US surveillance network, 2) interactive: the positionality and connectivity between surveillance actors, and 3) physical/material: physical arrangement and material realities of digital infrastructures and surveillance actors. This multi-level research approach enables a more holistic investigation of surveillance as a phenomenon and how it has permeated different elements of modern society. Below, I briefly overview the specific aims of the three articles that make up the body of the dissertation, as well as trace the linkages between them that bring this research together as one cohesive body of work.

Chapter 2 of this dissertation serves as the introduction to the concept of digital sousveillance as a methodological approach to studying surveillance and draws on Haggerty and Ericson's (2000) concept of "surveillant assemblage" to critically analyze the amalgamation of public and private actors involved in carrying out surveillance in the US. In doing so, this chapter aligns the politics of assemblage thinking and sousveillance to challenge the idea that digital data merely serves as a conduit for surveillance and exploitation. It instead highlights the potential of these data and methods as sousveillance tools, conceivably allowing private citizens and scholars alike the ability to "watch the watchers."

In contrast to past surveillance and social networks research, which has primarily been limited to analyses of particular actors, cases, and time periods, this research casts an extensive net, examining a vast network of over 31,000 public and private organizations and tracing changes to this network over the period of several decades. Using quantitative network analytic methods, this research examines the changes and development of the U.S. surveillant assemblage from the 1970s to the 2000s to 1) draw attention to the "blurring" of public and private surveillance in the contemporary moment, 2) link the structural changes and patterns within this vast network over time to socio-historical events and processes, and 3) in a more critical sense, suggest that the growing number of public-private partnerships involved in conducting mass surveillance poses a significant threat to our civil liberties. This chapter thus sets the stage for digital sousveillance as a methodological approach to studying surveillance and brings to light new insights into the network of public-private partnerships of surveillance that have emerged and developed in recent years.

Chapter 3 of this dissertation builds upon the methodological approach and findings of the first article to better understand the nature and implications of the network positionality and connectivity between surveillance actors US surveillant assemblage during the 2000s. This research thus digs deeper into the contemporary network of surveillance actors to gain insights into the relationship between surveillance organizations' network position and economic outcomes. It also goes further in considering the extent to which this crucial relationship is conditional on various organization-level factors, such as organization type, ownership, and industry.

Chapter 4 examines the material linkages between surveillance infrastructure and organizations to evidence the need for continued attention and emphasis on the material realities of contemporary surveillance practices. Drawing on theoretical ideas from the organization and infrastructure studies literature, this research investigates the materiality of surveillance through an analysis of two primary examples: 1) the geographies and physical arrangement of surveillance infrastructures and organizations and 2) surveillance capitalism and the materiality of contemporary digital surveillance technologies. This research thus grounds the structural and interactional analyses of Chapters 2 and 3 in the material realities of modern surveillance practices. In doing so, this work pushes back on the recent turn in surveillance studies towards emphasis on the immaterial and abstract elements of surveillance.

Chapter 5 concludes the dissertation by summarizing the key high-level findings of each of the previous chapters. It then outlines the broad academic contributions and societal implications of this research and finishes with a discussion of some of the limitations of this work and future directions for research in this area.

CHAPTER 2 — DIGITAL SOUSVEILLANCE: A NETWORK ANALYSIS OF THE US SURVEILLANT ASSEMBLAGE

INTRODUCTION

The field of surveillance studies has long been concerned with the relationship between public and private organizations regarding carrying out surveillance (Fyfe and Bannister 1996; Lyon 2001; Wakefield 2002). While it is a given that private entities play a crucial role in allowing the government to engage in surveillance, whether through "backdoors" (Crampton, Roberts, and Poorthuis 2014) or "revolving doors" (Hayes 2012), we know far less about how this vast assemblage of public and private organizations actually operates. When private corporations are implicated in helping government entities spy on their citizens, as was the case with several companies named in the documents released by Edward Snowden, the immediate reaction of companies is always an attempt to distance themselves from any association to government surveillance activities. The fear of being associated with government spying plays into the secretive nature of the surveillance industry, as companies fear that consumers will react negatively to such an association. Because of the tight-lipped nature of the US government, as well as the private corporations involved in surveillance activities, the study of what some have termed the "surveillance-industrial complex" has struggled to "unmask" the actors involved. Questions about *who* is involved in this assemblage, *to what extent* they are involved in carrying out surveillance activities, and *how* this contemporary form of public-private surveillance has emerged are still relatively unanswered.

This article aims to answer these unresolved questions and introduce a new methodological approach to the study of surveillance that I call *digital sousveillance*. To illustrate the potential of this approach, I employ quantitative network analysis to trace changes in the vast network of public and private organizations, or what I refer to as the " US surveillant assemblage," involved in surveillance operations in the United States from the 1970s to the 2000s. Drawing on data from the Transparency Toolkit's ICWatch database, I demonstrate the potential of digital sousveillance as a critical research method, bringing together digital data and robust computational techniques to gather, visualize, and analyze this assemblage of public and private organizations. The results of the network analysis indicate that the US surveillant assemblage is becoming increasingly privatized, and the line between "public" and "private" is becoming blurred as private organizations are, at an increasing rate, partnering with the US government to engage in mass surveillance. I conclude by outlining the limitations of these analyses and the dangers posed by the contemporary structure of the US surveillant assemblage.

BLURRING PUBLIC AND PRIVATE: THE SURVEILLANCE-INDUSTRIAL COMPLEX

Drawing on Eisenhower's age-old concept of "military-industrial complex," Ben Hayes (2012) developed the term "surveillance-industrial complex." While the surveillance-industrial complex does not amount to a comprehensive theory of surveillance, by employing this concept we can make important theoretical assumptions about the corrosive nature of the state-corporate nexus on political culture, democratic governance, and social control. First, it intimates the "revolving door" between those public entities which are officially tasked with security and those private actors that provide the new methods of surveillance and control that will enable them to do so. Second, it highlights the political and economic model that underpins these social relations. Lastly, it puts forth a critical understanding of the implications of this public-private nexus: that the surveillance-industrial complex promises to “deliver ever more pervasive, intrusive and effective surveillance technologies in perpetuity” (Hayes 2012:167-168). The surveillance-industrial complex consists of many distinct actors and is strategically positioned at the center of many of the transformations in population control, policing, and intelligence gathering (Hayes 2012), while at the same time remaining mostly out of public sight and only ever showing itself in a way that fails to reveal the particularity of these public-private relations (van der Vlist 2017). The task of mapping this complex nexus of public and private is thus a challenge due to its secretive nature.

The partnership of the US government with private corporations to conduct surveillance is not a recent phenomenon. As far back as World War I, telegraph and cable companies like Western Union turned over all telegraphic communications to the earliest predecessor of the NSA, known as the “Cipher Bureau” (Bamford 2009). The leveraging of public-private partnerships for purposes of intelligence gathering continued up until the mid-1970s. It was around this time that much of the American public shifted from general trust in public institutions to dramatic distrust. Revelations surrounding the FBI and CIA, the Watergate episode, and other Nixon administration intrusions provided concrete examples of government abuse of power that made the public, as well as private companies, wary of intelligence operations. In light of the attacks on September 11, 2001, the perceived need for surveillance and other intelligence-gathering operations intensified. While solicitation and attempts to gather information from private entities for intelligence purposes may not have been received well by private actors in the decades following the 1970s, the opposite was true in the immediate aftermath of the 9/11 attacks. The perceived need for intelligence for counter-terrorism purposes was great, and the private sector was ready to provide it.

SURVEILLANCE-INDUSTRIAL COMPLEX AS SURVEILLANT ASSEMBLAGE

While the concept of the surveillance-industrial complex is useful in providing a conceptual framing of the public-private nexus regarding surveillance, it alone is relatively limited in its theoretical capacity to capture the complexity of surveillance as a phenomenon. I utilize Haggerty and Ericson's (2000) concept of "surveillant assemblage" to move beyond the dualism of "public" and "private," and to highlight the multiplicities and nuances of these partnerships. Below, I outline the concept of surveillant assemblage and its operationalization in this article.

The origins of assemblage as an analytical concept can be located in the writings of Deleuze and Guattari (1987). The term has since been used by several scholars (Abrahamsen and Williams 2009; Collier and Ong 2005; Marcus and Saka 2006; Sassen 2006) to denote an understanding of structures that is not confined to a distinct scale (such as local/global or micro/macro) (Bueger 2014). An assemblage may seem structural as "an object with the materiality and stability of the classic metaphors of structure, but the intent in its aesthetic use is precisely to undermine such ideas of structure" (Marcus and Saka 2006: 102). This does not mean disavowing the notion of structure completely (indeed, network analysis relies upon some semblance of structure), but rather acknowledging its dynamic and fluid nature. What some have called "assemblage thinking" thus represents an attempt to refuse totalities and embrace social life as a nonlinear, heterogeneous alignment of emerging and continuously moving parts (Bleiker 2014). This also means paying attention to the complex relationships between these multiple actors and the broader forces that impel them to act in the way they do (Lisle 2014: 72). In the case of surveillance, there is no single, centralized agency that coordinates the totality of surveillance systems and operations. What perhaps makes this assemblage so unique, and indeed powerful, is its ability to integrate discrete surveillance systems and actors.

Haggerty and Ericson (2000) draw on Deleuze and Guattari (1987) to describe what they call the "surveillant assemblage." In speaking of *the* surveillant assemblage, however, they are not referring to a stable, fixed entity. Because it is "multiple, unstable and lacks discernible boundaries or responsible governmental departments," the surveillant assemblage cannot be dismantled by just eliminating a technology or mode of surveillance, nor can it be confronted by focusing criticism on a single bureaucracy or institution (Haggerty and Ericson 2000: 609). Much surveillance research tends to concentrate on the capabilities of discrete technologies or social practices and emphasizes how they cumulatively pose a threat to civil liberties. This research is also too often overly concerned with local sociotechnical instances of surveillance, in observing the propagation of what Latour (2005) calls "oligoptica" – durable but extremely narrow views of the broader whole (Murakami Wood 2013). It is thus necessary to recognize that the surveillant assemblage takes a variety of forms and therefore cannot be captured through one case study. This is because surveillance, as a phenomenon, is driven by the need to bring systems together, to combine different social practices and technologies and integrate them into a larger whole.

As Buchanan (2015) warns, however useful and analytically revealing assemblage theory may be, in practice the use of the concept of assemblage is often indistinguishable from that of an adjective, serving more to *name* than *frame* a problem. It is thus crucial to explicitly outline the specific ways in which assemblage, as a concept, contributes to this study both analytically and methodologically. As previously indicated, approaching surveillance as a multiplicity is an invitation to go beyond binaries and dualisms. Classifications such as state/non-state, human/non-human, and public/private are not explanatory frameworks, but rather distinctions that require explanations and attention to how they are enacted in surveillance discourses (Bueger 2014). Going "beyond dualisms," however, does *not* mean dismissing the categories of "public" and "private" altogether, as they still serve as useful characterizations of the type of organizations that engage in surveillance. Indeed, the distinction between public and private is particularly important for surveillance given the differing legal, as well as social, expectations placed on public and private organizations when it comes to issues of privacy. Instead, conceptualizing this network as an assemblage means greater emphasis and attention to how these classifications are actually enacted in surveillance discourses and how these two mutually exclusive categories of actors interact in ways that may problematize their respective classifications.

DIGITAL SOUSVEILLANCE AS METHOD

Representing an assemblage in an academic narrative always entails a political choice in the sense that it decentralizes power and authority away from the state (Bueger 2014). Assemblage thinking thus lends itself to critical analysis of the formations and multiplicities under study and acknowledges the complexity of surveillance and socio-technical objects, viewing them as entangled and used simultaneously as modes of exploitation as well as *resistance* (van der Vlist 2017). It thus aligns with the practice of what Mann, Nolan, and Wellman (2003: 19) call "sousveillance," which seeks to resist dominant modes and structures of power within surveillance by inverting the organizational gaze to "watch the watchers."

While social media data and digital data, in general, have been utilized for surveillance by public and private organizations alike (Brayne 2017; Greenwald 2014; Lyon 2014; Zuboff 2019), there have been few attempts to co-opt these data to surveil the state and its private partners. To this end, I build on the concept of sousveillance to introduce *digital sousveillance* – that is, the co-optation of digital data and the use of computational methods and techniques (e.g., network analysis) to resituate technologies of control and surveillance on individuals to instead observe the observer – as a method for studying surveillance.

The use of digital data and computational methods is nothing new for the social sciences; however, they have been largely under-utilized in the field of surveillance studies with few exceptions (Introna and Gibbons 2009; van der Vlist 2017). Although not necessary for the act of sousveillance, pervasive digital technologies and the data they generate can make sousveillance more effective (Mann and Ferenbok 2013). Many of the reasons that state and private organizations use digital data and computational methods for surveillance are the same reasons why the field of surveillance studies should also consider using them. The most obvious advantage of using digital data for studying surveillance is its sheer size and depth. Not only do digital data allow for a larger sample, but they also often contain in-depth, relational information. The use of open-source data has the additional advantage of greater transparency and reproducibility. Perhaps most important to those studying a hidden phenomenon like surveillance is that digital data may also allow for access to information that would otherwise not be available. This study, for example, uses open-source social media data to trace the linkages between public and private organizations, something that, given the secretive nature of the surveillance-industrial complex, would be difficult to observe otherwise. Digital sousveillance, of course, does not constitute a rejection of “small data,” or qualitative methods of studying surveillance. Indeed, digital sousveillance methods are perhaps best used as a complement to these methods, allowing for exciting new pathways for interdisciplinary and collaborative studies of surveillance. The methodological toolkit of digital sousveillance is extensive, allowing for the use of a wide range of computational methods, including robust statistical analyses, computational content analysis, machine learning, and network analysis. The digital sousveillance toolkit also has the advantage of accessibility, as many of these tools are available and achievable through free, open-source software and programming languages.

It is also important to consider the ethics of using digital sousveillance as a method for studying surveillance. First, there is *flexibility* in how digital data are interpreted and produced. Algorithms are not technical, self-contained objects, but instead objects that embody the socio-political values and biases of their authors (Eubanks 2018; Noble 2018). This means moving beyond digital data as representationalist and towards seeing them as performative; the composition and interpretation of these bits of data in effect produce the life and body of the subject into “data doubles” (Matzner 2016; Raley 2013). As Cheney-Lippold (2017:11) notes, “we are ourselves, plus layers upon additional layers of algorithmic identities.” Digital sousveillance requires considerable attention to how these algorithmic identities are produced and vary across different contexts. Second, those engaging in digital sousveillance also need to exercise *accountability*. As outlined by Boyd and Crawford (2012), accountability is broader than concepts of privacy in that it applies even when there is little to no expectation of privacy. Professional standards and ethics do not disappear when working with publicly accessible data. The size, depth, and sensitive nature of digital data necessitate additional attention to the implications of their use. The ICWatch dataset, for instance, also contains sensitive data, such as individuals' names, photographs, and geographical locations.[1] Those engaging in digital sousveillance need to be aware of the potential harm that can come from publishing and making these types of data more visible and accessible.[2] Accountability is essential to prevent scholars of surveillance from falling into the same harmful, intrusive behaviors and abuses of power that they are attempting to dismantle.

This study thus seeks to demonstrate the potential of digital sousveillance as a critical research method, bringing together robust computational analytic techniques to gather, visualize, and analyze this complex and often hidden assemblage of actors. Below, I detail the data and methods used to accomplish this task.

DATA AND METHODOLOGY

This article uses network analytic techniques to map the historical development of the US surveillant assemblage, and its public-private linkages, from 1970 to the 2000s. The primary sources of network data for this article are drawn from the Transparency Toolkit's

[1] The inclusion of individuals with no actual surveillance-related affiliations that were inadvertently scraped in the original IC Watch dataset is also particularly problematic. These data underwent an extensive process of data cleaning, both manually and using computational techniques. A "fuzzy matching" algorithm was used to eliminate redundancies in the data, such as variations in organizational names (e.g. US Army, Army, United States Army, etc.). In addition, these data were manually audited to remove profiles incorrectly included in the dataset.

[2] The open publication or presentation of these types of sensitive individual-level data are not only unnecessary for the study of surveillance, but also raise considerable ethical issues due to the unintended harm they may cause. It also serves to incorrectly assign "blame" to particular individuals, while lessening attention to the role of broader organizational and institutional structures that maintain and perpetuate mass surveillance. This paper attempts to protect the privacy of these individuals by focusing the analyses on the organizational level.

ICWatch database. Transparency Toolkit is an organization that uses open-source data to bring greater public visibility to surveillance and possible human rights abuses. The data employed in this article are scraped from individual profiles on LinkedIn. The scraper collected public profile information based on a list of search terms that consisted of the names of surveillance programs identified in the Snowden documents. If an individual's profile contained terms or names from one of these programs, the scraper collected the entire profile, including job history (job title, company, start/end date, and description for each job), skills, educational history, and location/area. Information about the organizations mentioned in the profiles, including company size, industry, and the type of organization (e.g., government agency, public company, etc.) was added to the dataset.

These data were chosen in large part because they provide a glimpse into a phenomenon that is often kept hidden from public view and academic research. Up until the release of the Snowden documents in 2013, public knowledge about the extent and nature of US government surveillance was mostly based on speculation and what little information had been willingly revealed by the US government. Thus, little academic work has been done on the surveillance industry, let alone on the ways and extent to which they interact with nation-states and other government entities (Murakami Wood 2013). The inaccessibility of US government intelligence organizations, as well as their private partners, means the avenues for the study of this phenomenon are incredibly limited. These sources are thus essential objects of study because they represent one of the only ways of studying US government surveillance directly.

The temporal scope of this analysis spans from 1970 until 2009. The primary network analysis will compare four distinct periods: 1970-1979, 1980-1989, 1990-1999, and 2000-2009. This comparison of networks allows for a greater understanding of how the US surveillant assemblage has developed over this period. The 1970s is an appropriate starting point because this time represents a crucial moment in the development of the US surveillant assemblage. As previously discussed, the 1970s marked a shift from general trust in public institutions to dramatic distrust. The expansion of partnerships and networks of intelligence gathering operations in recent decades stands in stark contrast to the doubt and skepticism of the 1970s. Thus, tracking these networks up to the contemporary moment is crucial to understanding the modern formation of this assemblage.

In total, 25,479 individual profiles[3] are identified in the data. This represents a considerable sample as the total intelligence community workforce has been estimated to be around 183,000 people, of which 58,000 are privately contracted (Shorrock 2016). As noted above, each of these individuals' profiles contained information on the organizations and companies presumed to be involved in US surveillance programs. These organizations and companies represent the primary unit of analysis. The network data were originally two-mode data, with organizations *indirectly* tied together based upon their shared affiliation with particular surveillance programs. These types of networks are often referred to as "affiliation networks" (Wasserman and Faust 1994). Connections in this two-mode network represent the tie between the surveillance program(s) mentioned in an individual's profile and the organization(s) that the individual worked for. For example, if an individual worked on the PRISM program, all organizations listed in the individuals' profile would

[3] At the time of original collection, the ICWatch dataset contained over 27,000 individual profiles. This number was reduced to around 25,000 after cleaning the data and removing profiles that were inadvertently sampled. Additional individual profiles from new data sources (i.e., Indeed) have been added to the ICWatch dataset since the time the data used here were collected, though not all of these new data have clear relevance to surveillance. For instance, the portion of the new data from the "FBI/DHS hack" contains the names, titles, phone numbers and email addresses of individuals working for the FBI and Department of Homeland Security. The sample here thus represents a subset of the ICWatch dataset as currently composed.

be connected to the PRISM program. However, since the aim of this article is to map the linkages among organizations, this two-mode network (surveillance program-to-organization links) was collapsed into a one-mode network (organization-to-organization links). A connection in this network thus represents a tie between two organizations based on their shared affiliation with particular surveillance programs identified in individuals' profiles. For instance, if Individual A worked on PRISM and worked for Booz Allen and Individual B worked on PRISM and worked for the NSA, a connection is drawn between Booz Allen and the NSA.

It is important to acknowledge that the connections between these organizations are drawn based on an *assumed* shared affiliation with surveillance programs. One limitation of these data is that they do not contain information about the nature or direction of the relationship between these organizations, nor do they detail the specific surveillance-related activities of these organizations. There are, therefore, several possibilities when it comes to the nature of the linkages between these organizations, such as engagement in actual spying on behalf of the government, financial relationships, research and development, or the exchange of surveillance-related goods and services. The type of connection between organizations is presumably dependent upon the type of organizations involved. Each actor, public or private, operates in light of its own logics, agendas and local constraints (Ball et al. 2015; Haggerty and Gazso 2005). For instance, a university tied to the NSA may be involved in research and development whereas a telecommunications company may provide the NSA with access to communications data and infrastructure. Framing these partnerships as an assemblage requires acknowledging the multiplicity of the connections between organizations, meaning these connections also result in the linkage of physical (fiber-optic cables, cell towers, servers) and digital infrastructures (data, algorithms, code, software), technical objects, knowledge, and discourses.

Cytoscape, a network analysis software, was used to generate four network graphs. The visual layout used to map these networks is called the "Group Attributes Layout," which groups the nodes in a circle based on an attribute they have in common. In this case, the nodes are grouped based on whether they are public or private organizations. Node size was scaled based on the node's degree. In other words, larger nodes represent organizations that have a larger number of connections to other organizations. The nodes are color-coded, with blue representing "public" entities and red representing "private" entities[4]. To illustrate the extent and structure of public-private connections, ties or edges between nodes are also color-coded. Purple edges represent heterophilic ties (ties between public and private organizations), and grey edges represent homophilic ties (ties among public organizations or ties among private organizations). An edge-bundling algorithm was used to bundle edges with similar destinations and connections to create greater space within the graphs and render these connections clearer. In addition to the graphs, statistical measures of network connectivity and homophily/heterophily were calculated using Cytoscape and a Python package, NetworkX, for each of the four temporal periods to allow for a quantitative means of comparison and tracking of the changes to the US surveillant assemblage over time.

[4] For the purposes of this analysis, "public" entities only consist of US government organizations. Public universities or similar institutions that are funded by the US government are considered "private" organizations in this analysis. This was done to clearly distinguish agents working on behalf of the state (e.g., US Military, NSA, CIA, etc.) to engage in surveillance from those that, although they are directly or indirectly funded by the state, tend to operate outside of the realm of government.

RESULTS & ANALYSIS

As noted above, the data are analyzed in four distinct sections representing each decade from the 1970s through the 2000s. In the following section, network graphs (Figures 2.1-2.4) are shown to visually illustrate the networks and to provide a literal "map" of the changes to this assemblage over time. These visualizations alone are insufficient to draw robust empirical conclusions. To compensate for this, network statistics and measures are provided to allow for a clear, empirical means of comparison between each network. I thus rely upon statistical network analyses, including measures of network structure as well as measures of homophily/heterophily for each decade, to support and expand upon the insights gained from the graphical network representations.

MAPPING THE US SURVEILLANT ASSEMBLAGE

The 1970s represented a crucial period for the US surveillance-industrial complex. In this decade, the American public's general trust in public institutions shifted to dramatic distrust. Numerous concrete examples of government abuse of power, such as revelations surrounding the FBI and CIA, the Watergate episode, and other Nixon administration intrusions, resulted in both the public and private companies experiencing increased wariness of intelligence operations. This led to a series of reforms in the mid-to-late 1970s, such as FISA, that was aimed at preventing further abuses by the US government and severely limiting their ability to surveil American citizens. Because these shifts occurred late in the 1970s, it is unlikely that they had an immediate effect on the ties between public and private organizations within this network. Thus, it might be expected that the 1970s network is quite heterophilic, with extensive connections between public and private organizations as was the case leading up to these changes.

Figure 2.1 displays the network graph for the years 1970 through 1979. Immediately apparent is that the most significant nodes in the network in terms of degree are government entities. This indicates that these particular government organizations are the most well-connected in this network. While private actors are present, they are, overall, smaller in terms of degree, meaning that these private organizations had fewer numbers of connections within the network. Nonetheless, the notable presence of public-private ties (purple) in the graph evidences that, as hypothesized, these relations were quite common and certainly did not cease to exist despite some of the changes later in the decade mentioned above. There is also far less homophily (grey edges) among public organizations when compared to private organizations. Also, there are several clusters of public-private ties outside of the most central group of nodes in the two groups, suggesting that this network is quite decentralized.

The 1980s is of particular interest because it represents the period we might expect to illustrate the earliest effects of the changes in policy and public opinion during the mid-to-late 1970s on the US surveillant assemblage. The 1980s continued the trend of increased concern and skepticism that characterized the late 1970s. In 1981, President Ronald Reagan signed Executive Order (EO) 12333, which required each intelligence agency to establish procedures for the collection of electronic communications using "the least intrusive collection techniques feasible within the United States or directed against United States persons abroad" (qtd. in Donohue 2016). This decade also witnessed the passage of several privacy laws governing private information, including the Privacy Protection Act (1980) and the Electronic Communications Privacy Act (1986). Public concerns about privacy threats in this decade had also increased dramatically, with 48% of survey respondents reporting that they were “very concerned about threats to their personal privacy” compared to only 31% in the late 1970s (Kumaraguru and Cranor 2005; Raynes-Goldie 2010). While the findings of the Church Committee led to significant reform, many of the same flaws began to reappear by the mid-1980s as the executive branch and intelligence community found new ways to avoid legal obstacles and carry out mass surveillance (Murphy 2014). In particular, the revelations around the Iran-Contra affair in 1986 involving the Reagan administration and the CIA cast doubt upon the ability of Congress and the public to manage and oversee the intelligence community. As the Congressional Iran-Contra Joint Committee concluded, “secrecy was used not as a shield against our adversaries, but as a weapon against our own democratic institutions” (qtd. in Schwarz and Huq 2008: 57).

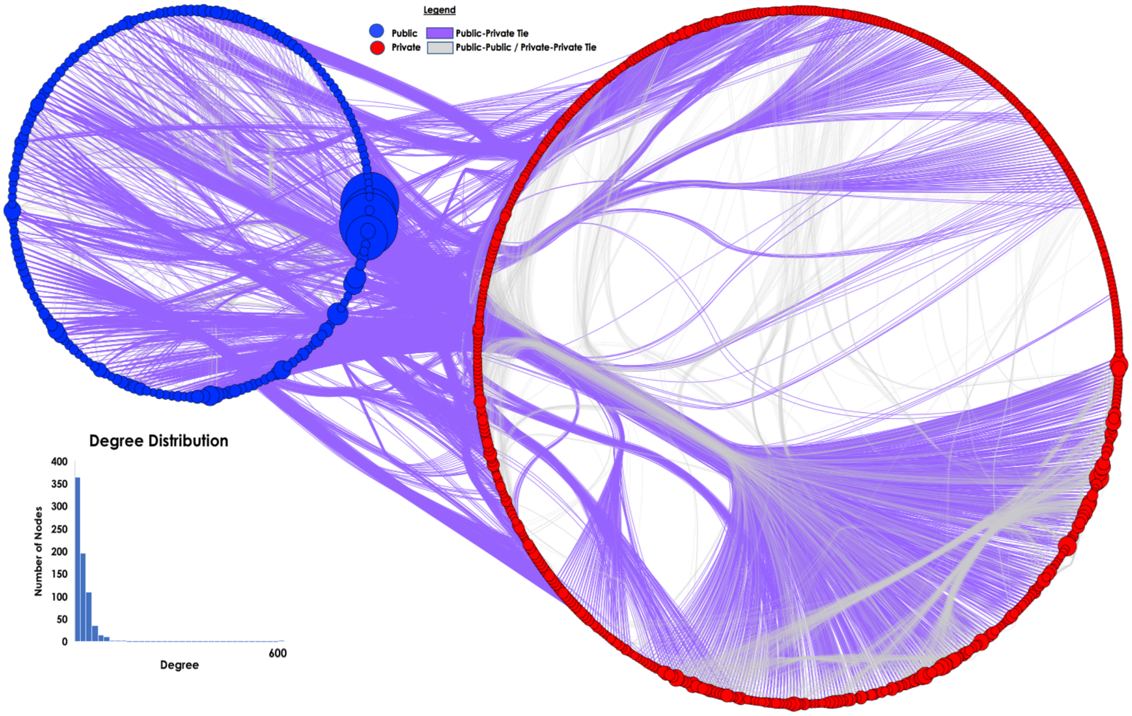

Figure 2.1: Network graph, 1970-1979.

Figure 2.2 depicts the network graph for the years 1980-1989. Like the 1970s, the 1980s network contains larger, highly-connected government organizations. Also, network ties between public and private organizations are the majority by a substantial margin. There appear to be a higher proportion of relations between private organizations and other private organizations compared to the 1970s network. Also, in contrast to the 1970s network, there are several well-connected government organizations and private organizations that seem to be more prominent in terms of node size and degree. The 1980s network thus appears to be more centralized regarding the number of connections among nodes than the previous network.

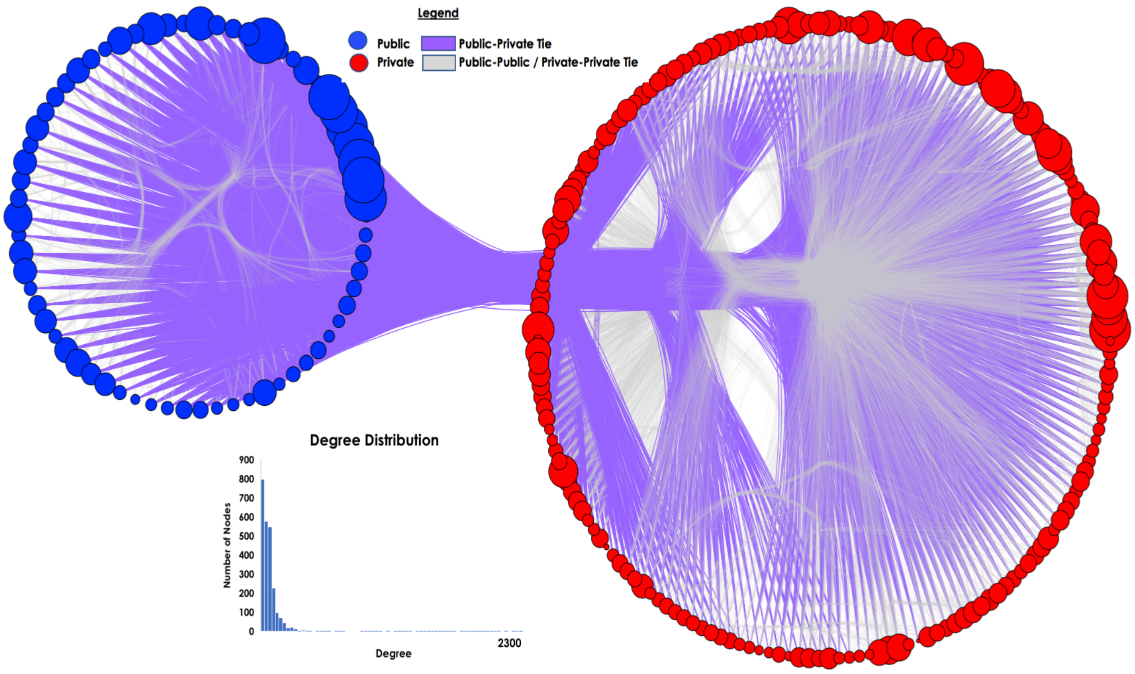

Figure 2.2: Network graph, 1980-1989.

Although the 1990s represented a somewhat "calm" (at least visibly) period regarding surveillance-related events, it might be expected that the inability of the 1980s-era policies to regulate government surveillance may have led to an expansion of the US surveillant assemblage. It might be easy to read into the sheer size of this network (see Table 2.1) in the 1990s and confirm such a hypothesis. However, this is more likely an artifact of the dataset itself, as there is an inherent bias towards recent employment history on LinkedIn considering the age of the platform as well as the age of its users. Given the lack of significant surveillance and privacy-related events, the 1990s serves as a useful transitional point and comparison to the influx of such events in the 2000s and post-9/11 era.

The network for the 1990s (Figure 2.3) appears to be qualitatively different from that of the 1970s and 1980s. Beyond just the increase in the sheer number of organizations and ties within the network, there is an apparent shift in the prominence of private organizations within the US surveillant assemblage. While private organizations were reasonably small in terms of degree and importance in the 1970s and 1980s compared to government organizations, private organizations in the 1990s are on par with the significant, highly connected government actors in the network.

With the events of the 1980s and the status-quo approach of the 1990s, the stage was already set for a dramatic expansion in the 2000s of public and private partnerships to carry out mass surveillance on a global scale. The terrorist attacks on September 11, 2001 gave the US government the immediate legal and public support necessary to expand law enforcement and executive powers to grow the US surveillant assemblage exponentially. The passage of the USA PATRIOT Act in the immediate aftermath of the 9/11 attacks, as well as subsequent laws billed (albeit falsely) as "surveillance reforms," such as the Protect America Act (2007) and the FISA Amendments Act (2008), dismantled the restrictions put into place in the 1980s.

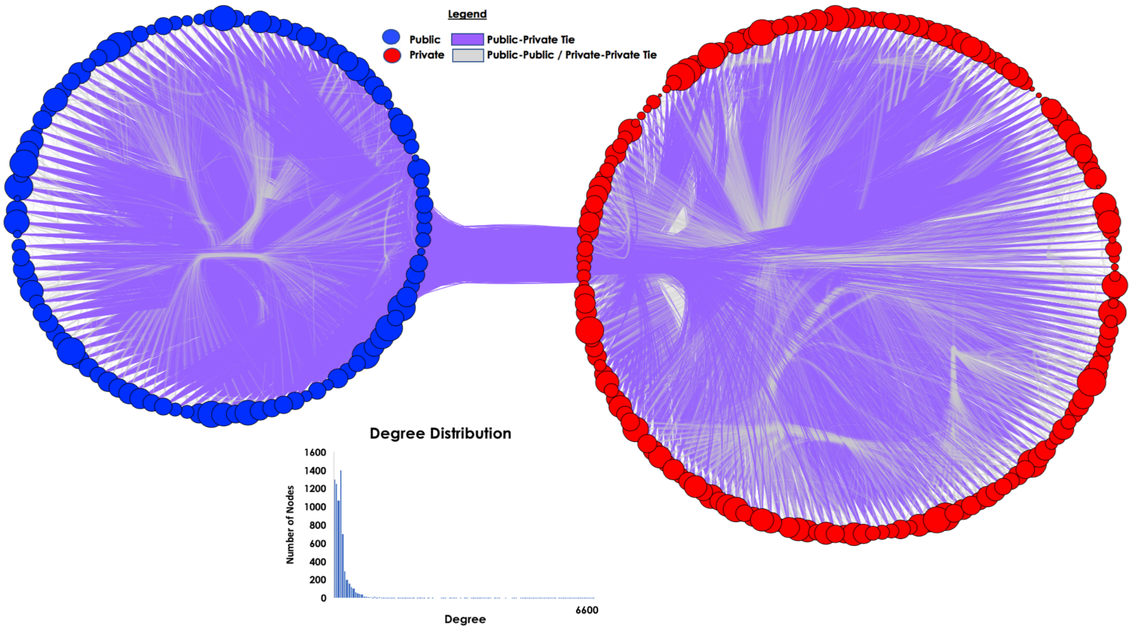

Figure 2.3: Network graph, 1990-1999.[5]

The US surveillant assemblage continued to carry out mass surveillance through covert surveillance programs. One such program was PRISM, which allowed the NSA to collect private communications from the world's largest internet companies, including Google, Facebook, Microsoft, and Apple. PRISM was particularly significant because it allowed the NSA to obtain virtually anything it wanted from the servers of internet-based companies that hundreds of millions of people around the world now use as their primary means to communicate (Greenwald 2014). Although the NSA documents claimed the PRISM program was run with the assistance of the private companies many denied knowledge of any such program (Greenwald and MacAskill 2013).

[5] This graph represents a sample of the original network. To present a more readable graph, only the top 5% of nodes in terms of degree are included in this visualization. Network statistics and degree distributions are, however, calculated using all nodes and edges.

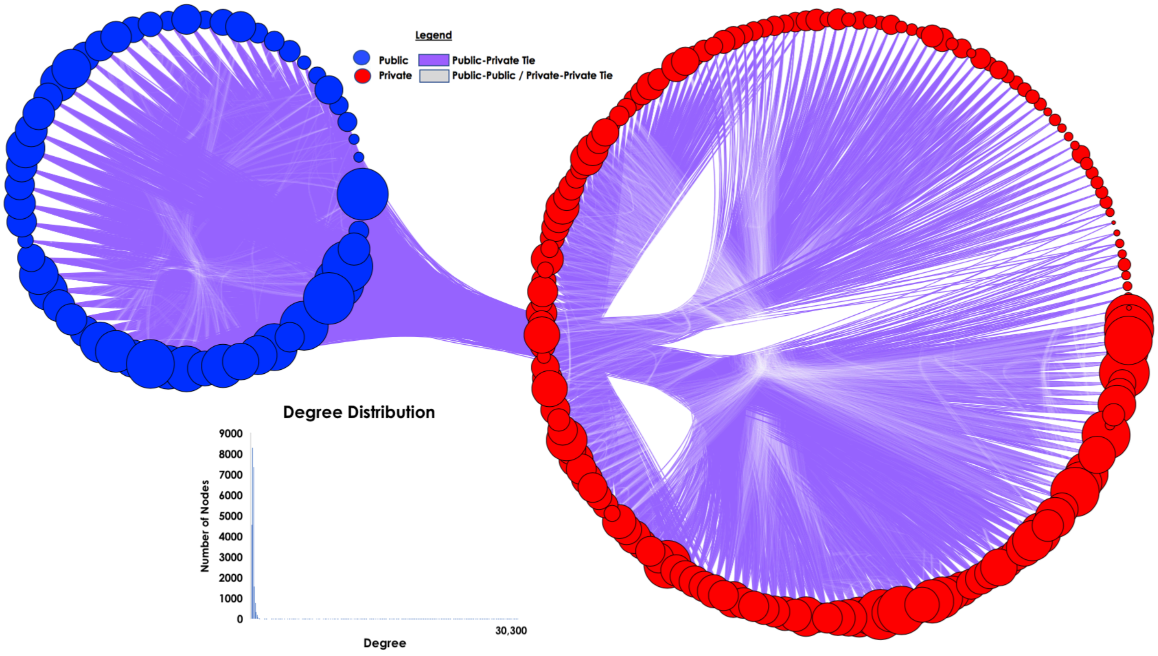

Figure 2.4: Network graph, 2000-2009.[6]

The most striking feature of the network graph is the overwhelming presence of private organizations as the dominant nodes in terms of degree within the network. In contrast to the three previous networks, private organizations have overtaken government organizations as the most well-connected actors in the US surveillant assemblage. There is also clustering of public-private ties, most noticeable on the private side of the graph with two major groups of public-private ties clustered together. There also seem to be, proportionately speaking, fewer public-public and private-private ties than there were in previous decades. This would seem to indicate that connections between public and private organizations were more frequent during this period. In the following section, I rely upon statistical network analytic methods to support these graphical illustrations and to draw

[6] This graph also represents a sample of the original network. To present a more readable graph, only the top 1% of nodes (in terms of degree) are included here. Network statistics and degree distributions are, however, calculated using all nodes and edges.

more direct empirical conclusions about the structure of the US surveillant assemblage from the 1970s to the 2000s.

STRUCTURE OF THE US SURVEILLANT ASSEMBLAGE

Table 2.1 displays several network statistics for the four periods examined here. These measures indicate the level of network connectivity. Multiple measures are provided to illustrate changes to various structural elements of the network and as a robustness check. The networks were analyzed as undirected networks – as organizations that had no discernible directional relationship or tie with each other. Within a network, all nodes that are connected form a connected component. The number of connected components indicates the overall connectivity of a network. A lower number of components, therefore, suggests stronger connectivity among organizations, whereas a higher number of components suggests weaker connectivity among organizations. By this measure, the 1970s-1990s had weaker connectivity, while the 2000s had robust connectivity between the various actors. The second measure, the clustering coefficient, denotes the extent to which nodes in a graph tend to cluster together and form “triangles” (connections between three mutually-connected nodes). The clustering coefficient is relatively stable from the 1970s until the 1990s but increases noticeably in the 2000s. This would seem to indicate that organizations in the 2000s were more likely to form a tightly knit and highly connected group than in past decades. The network diameter represents the largest distance between two nodes. A smaller diameter indicates greater connectivity and centralization within the network (and vice versa). There was no real difference between the four networks for this measure. The fourth statistic, network centralization, measures how the network is distributed in terms of degree. Centralized networks have a value closer to one, whereas decentralized networks have values closer to zero. The centralization of the networks increased over time, going from 0.783 in the 1970s to 0.911 in the 1980s to 0.919 in the 1990s and 0.976 in the 2000s. This is in line with previous measures and would seem to indicate again that the US surveillant assemblage becomes more centralized and highly-connected in the 2000s. Lastly, the characteristic path length gives the average distance between two connected nodes and is also used to indicate the connectivity of the network. A shorter path distance suggests greater connectivity within the network. The characteristic path length was relatively constant across the four networks.

Table 2.1: Measures of network connectivity.

	1970-1979	1980-1989	1990-1999	2000-2009
Nodes	743	2443	6961	31,015
Edges	10,189	95,939	708,517	1,048,575
Connected Components	13	9	14	1
Clustering Coefficient	0.838	0.856	0.834	0.966
Network Diameter	5	4	4	5
Network Centralization	0.783	0.911	0.919	0.976
Char. Path Length	2.010	1.996	1.988	2.004

The evidence provided in Table 2.1, overall, suggests that the US surveillant assemblage became more centralized and highly connected over time. Some measures like network diameter and characteristic path length are relatively constant. Others, such as the number of connected components, clustering coefficient, and network centralization suggest that there is a considerable shift in the structure of the US surveillant assemblage over time. While the structure of this assemblage is useful in furthering our understanding, these measures are unable to uncover the extent of public-private partnerships and how that aspect of the assemblage has changed over time. In the next subsection, I discuss the measures of network homophily and heterophily used to evaluate the extent and likelihood of public-private linkages within each network.

HOMOPHILY/HETEROPHILY IN THE US SURVEILLANT ASSEMBLAGE

Given the higher degree of connectedness within the US surveillant assemblage in recent years, it might be reasonable to expect that public and private organizations would be more likely to connect in the 2000s networks. To test this hypothesis, I ran a series of quantitative analyses of network homophily and heterophily (Table 2.2, below). The first statistical measure is called attribute assortativity. This is used to measure the level of correlation between connected nodes for the values of an attribute (categorical or scalar) of the nodes (organizations). Attribute assortativity ranges in value from -1 to 1, with -1 representing a dissortative network, where nodes tend to connect to nodes with dissimilar attribute values, and 1 representing an assortative network, where nodes tend to link to nodes with similar attribute values. The attribute used for this measure was whether the organizational node was public or private. In this context, it measures whether organizations in these networks were likely to link with organizations that matched their value for the public/private variable. By this measure, the 1970s and 2000s were dissortative, whereas the 1980s and 1990s were assortative. In other words, the 1970s and 2000s networks had a higher tendency of linkages between public and private organizations compared to the 1980s and 1990s.

The second statistical measure used is degree assortativity. Similar to attribute assortativity, degree assortativity measures the tendency within networks for organizations to associate with organizations of a similar number of connections (degree). Taking these results together, all four networks were dissortative, meaning organizations tended to link with organizations with a different number of connections (e.g., highly-connected organizations were connected with lowly-connected organizations). Interestingly, the degree assortativity value for the 2000s is much more dissortative than the previous networks. This indicates that there is a much higher tendency in the 2000s for organizations with a smaller number of connections to link with organizations with a more substantial number of connections.

In addition to measures of assortativity, Table 2.2 displays the percentage of ties between public organizations, between private organizations, and between public and private organizations. The measure of primary concern here, of course, is the percentage of ties between public and private organizations. By this measure, the 2000s network had a higher percentage of public-private relations compared to earlier years. This supports the attribute assortativity measure in that the dissortative 1970s and 2000s networks had a higher percentage of public-private relationships when compared to the assortative 1980s and 1990s networks. Similarly, the odds-ratios of public-private ties were about twice as high for the 1970s (0.72) and 2000s (0.85) networks than they were for the 1980s (0.38) and 1990s (0.36) networks. The likelihood of public-private ties is thus highest for the 2000s network.

Table 2.2: Measures of network homophily/heterophily.

	1970-1979	1980-1989	1990-1999	2000-2009
Attribute Assortativity	-0.001	0.081	0.090	-0.064
Degree Assortativity	-0.171	-0.144	-0.112	-0.590
Public-Public Ties (%)	22%	21%	22%	17%
Private-Private Ties (%)	47%	58%	57%	47%
Public-Private Ties (%)	46%	38%	38%	48%
Odds-Ratio: Public-Private Tie	0.72	0.38	0.36	0.85

Overall, the measures of homophily and heterophily displayed in Table 2.2 seem to indicate that there were greater tendencies and likelihoods of public-private connections in the 1970s and 2000s networks compared to the 1980s and 1990s. This supports the graphical evidence provided in the previous section that suggested the 2000s network is quantitatively different from prior decades. The 2000s network is highly centralized, well-connected, and heterophilic – that is, the 2000s network had a greater tendency for public-private partnerships than previous years, as well as a greater tendency for connections between nodes of differing degree values. Interestingly, network statistics and measures for the 1980s and 1990s were nearly identical, meaning the explosion of public-private partnerships in the 2000s was not something that built up over time in a linear fashion as might have been expected. This would seem to suggest that there is something unique about the 2000s that allowed for this to occur, the most obvious possibly being 9/11 and the various legal and institutional changes that occurred in its aftermath.

DIGITAL SOUSVEILLANCE OF THE NSA

While the above network analyses evidence the ways that the topology and overall structure of the US surveillant assemblage have shifted in recent decades, it is also crucial for sousveillance purposes to bring to light some of the specific connections between public and private organizations. In this section, I briefly examine the public and private connections of the NSA in the 2000s. The NSA was one of the most prominent organizations in the dataset with over 26,000 connections in the 2000s network alone. This is perhaps unsurprising given that the NSA likely engages in more surveillance than any government organization in the world (Greenwald 2014). Given the significance of the NSA's role in the US surveillant assemblage, it serves as a useful case for further analysis and as an example of the sousveillance potential of these data. Exploring this specific case within the 2000s period also presents an opportunity to more closely examine the extensive level of privatization shown by the earlier network analyses.

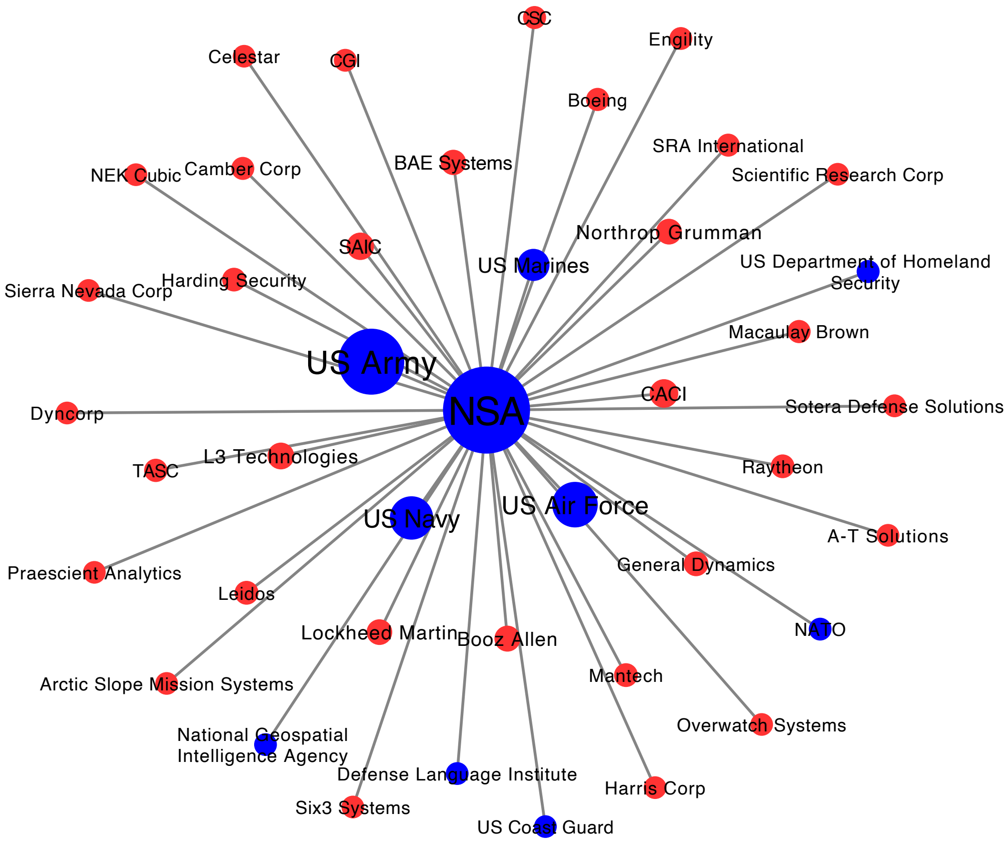

Figure 2.5: NSA network graph, 2000-2009.

Figure 2.5, above, represents the ego network graph for the NSA during the 2000s era.[7] Immediately apparent is that the closest ties to the NSA are the different branches of the US military. Outside of these organizations, however, the vast majority of the organizations connected to the NSA are private companies. Among the most prominent private actors within the NSA's network are Leidos, Booz Allen, General Dynamics, L3 Technologies, SAIC, and CACI. This is perhaps unsurprising as these are some of the biggest corporations in the privatized intelligence industry. Leidos, Booz Allen, SAIC,

[7] This graph represents a subset of the NSA's ego network. For visual purposes, only the most prominent actors in terms of degree are included here.

General Dynamics, and CACI alone employ nearly 80% (45,000 people) of the private contractors working in the intelligence industry (Shorrock 2016).

Most of the companies listed above provide different surveillance-related software, hardware, and analytics services. For example, among the connections to the NSA is Praescient Analytics. They note on their website that they "partner with a series of cutting-edge software companies to deliver training, integration, customization, and embedded analytic services to clients across the public and private sectors" (Praescient Analytics 2019). Among the software companies listed as Praescient Analytics' partners are IBM, Semantic Research, and Palantir Technologies. Documents released by Edward Snowden revealed Palantir as the company that built the software for the NSA program XKEYSCORE, which collected citizens' emails, chats, web-browsing traffic, pictures, documents, voice calls, webcam photos, web searches, and much more (Biddle 2017). Palantir is perhaps the greatest example of the dangers of growing private involvement in the US surveillant assemblage. The company has been involved in recent controversy over its ties to the Cambridge Analytica scandal (Confessore and Rosenberg 2018), recent deportation efforts by ICE (Woodman 2017), and the development of intrusive digital analytics systems for local law enforcement agencies (Brayne 2017; Harris 2017). This illustrates how the US surveillant assemblage, including this particular sub-network, also represents a vast network of infrastructure, socio-technological objects, knowledge, and discourses that make it possible for these organizations to carry out surveillance. It is these heterogeneous elements of the US surveillant assemblage that make it so powerful and, in some cases, dangerous.

DISCUSSION

Before discussing the conclusions of this article, it is essential to acknowledge the limitations of these data. First, as previously mentioned, the actual nature of these connections and the extent of interaction between organizations to engage in surveillance is unknown. Similarly, the directionality of these relationships is unclear; there is no way of knowing (with these data alone), for example, whether a government agency has contracted a private entity for surveillance-related services or if there is a mutual exchange of goods and services. Second, this analysis is unable to fully account for the effects of external historical events, such as changes to regulatory or institutional dynamics, on the structure of the US surveillant assemblage. While some historical context is provided with the network analyses, the conclusions made about the role of these events in producing these changes are speculative. Third, the use of social media data inherently limits the generalizability of these findings. While large digital datasets are often celebrated for providing access to "complete" populations, specific populations are more likely to turn up in datasets like the one used here (Harris 2017). This dataset also fails to capture individuals who do not have a LinkedIn profile. Due to the sampling method of the scraping algorithm, it also does not capture those who had a LinkedIn profile and were involved in surveillance practices but did not explicitly mention a surveillance program in their profiles. Additionally, individuals working in particular industries or organizations may be less likely to use LinkedIn or to report their involvement in surveillance programs in their profiles. This may explain why universities, despite being known collaborators on defense research, are less prevalent in the data than private companies. Lastly, these data are limited in that they tend to favor more recent linkages between organizations due to the younger demographic of LinkedIn users and the tendency for users in general to favor recent job history in the profiles. Given the stark differences in terms of sample size and composition of the four time periods, conclusions about the structural and topological changes to the US surveillant assemblage over time, although supported by the current analyses, remain speculative and caution should be exercised in attempting to extrapolate these results.

This paper draws on Haggerty and Ericson's (2000) concept of "surveillant assemblage" to critically analyze the amalgamation of public and private actors involved in carrying out surveillance in the US. It also makes a methodological contribution to the field of surveillance studies by illustrating the potential of digital sousveillance as a method for studying surveillance. In doing so, this paper aligns the politics of assemblage thinking and sousveillance to challenge the idea that digital data merely serves as a conduit for surveillance and exploitation. It instead highlights the potential of these data and methods as sousveillance tools, conceivably allowing private citizens and scholars alike the ability to "watch the watchers." Digital sousveillance thus serves as a form of resistance to the dominant actors and power structures of mass surveillance. Future work could utilize digital sousveillance, as used here, to complement theoretical and historical studies of surveillance and pursue new interdisciplinary and collaborative studies of surveillance. Network analysis could, for instance, be used to build upon these analyses to trace networks of individual actors engaged in surveillance. Other methods, such as topic modeling or sentiment analysis, could lend empirical support to past studies of surveillance discourse and understandings of how discourse is framed by those actively engaged in surveillance practices.

The results of the network analysis indicate that the US surveillant assemblage is becoming increasingly *privatized*; indeed, the line between "public" and "private" is becoming blurred as private organizations are, at an increasing rate, partnering with the US government to engage in mass surveillance. The recent growth of the private sector's involvement in surveillance practices poses significant problems. By subjecting individuals to surveillance, governments, as well as their corporate partners who control the digital realm, can monitor and silence differing opinions and views. This global digital space, referred to by some as the "digital commons," plays a crucial role in allowing for the democratization of expression, as well as increased civic engagement and participation (Wonders, Solop, and Wonders 2012). The growing commodification of the global digital commons by private actors is problematic in that it subjects the users of this space to increased observation and scrutiny and facilitates the movement of private information into the hands of other parties, such as law enforcement agencies (Brayne 2017). As a result, the digital commons becomes a "backdoor" (Crampton et al. 2014) or "revolving door" (Hayes 2012) through which government(s) can not only observe users of the space but also do so in ways that avoid laws and regulations meant to protect those users. The simple fact that the surveilled know they are being watched has a chilling effect on civil liberties and the freedom of expression that is fundamental to a functioning democracy (Richards 2012). The growing involvement of private actors within the US surveillant assemblage thus presents a grave danger to the global digital commons and democracy as we know it. More work, by activists and scholars alike, is needed to continue to unmask these actors and to allow the public to better understand their entanglement with this vast surveillant assemblage.

Chapter 2, in full, is a reformatted reprint of the material as it appears in *Surveillance and Society* 2020. Burke, Colin. 2020. “Digital Sousveillance: A Network Analysis of the US Surveillant Assemblage.” *Surveillance & Society* 18(1): 74-89. The dissertation author was the primary investigator and author of this paper.

CHAPTER 3 – THE CONDITIONALITY OF EMBEDDEDNESS AND ECONOMIC CAPITAL: THE CASE OF SURVEILLANCE ORGANIZATIONS

INTRODUCTION

Sociology has long been interested in how social structure impacts the distribution and obtainment of economic capital. The idea that economic action can be fully understood only by examining the social relations within which actors are embedded has become a widely accepted staple of sociological thought (Granovetter 1985). It has also become the basis for a wide range of research by sociologists and organizational scholars alike that have brought empirical support to long-standing theories about the relationship between organizations' embeddedness and economic outcomes (Mizruchi and Stearns 2001; Uzzi 1999). While these studies have effectively demonstrated that networks and embeddedness are crucial elements for understanding economic outcomes, most have failed to fully consider the conditional nature of embeddedness in such organizational contexts (Mizruchi, Stearns, and Marquis 2006). Further, past studies that have examined conditional embeddedness, the idea that the relationship between organizations' embeddedness and economic outcomes may be contingent on other factors, have focused solely on how this relationship varies over time or across characteristics of individuals within organizations. Ironically, these studies of organizations have omitted the potential conditionality that may result from characteristics of their primary unit of analysis, organizations.

This study thus examines an extensive network of surveillance organizations to consider the extent to which the impact of embeddedness on economic outcomes is conditional on various organization-level factors, such as organization type, ownership, and industry. The growth of the apparatus of public and private surveillance organizations into multiple industries and sectors of the economy will allow for greater insight into how the relationship between embeddedness and economic outcomes plays out within an extensive, diverse organizational network. This level of network growth and diversity also means the surveillance organizational network has become structured in such a way that it could enable the observation of nearly every aspect of Americans' lives. For purposes of transparency and accountability alone, this case also provides a crucial opportunity to improve our understanding of what kinds of organizations are embedded within such surveillance networks and how they operate.

To this end, this paper employs OLS regression techniques to analyze a novel relational dataset that combines network data on partnerships between surveillance organizations and financial data on contracts awarded to such organizations by the US government. The results of these analyses suggest that while there is a strong relationship between surveillance organizations' embeddedness and economic capital, the directionality and degree of this relationship were conditional on organization type, ownership type, and industry. These findings pose significant implications for understanding the relationship between social structure and economic capital in the context of organizational networks more broadly and enhance our understanding of the structure and nature of the US surveillance and government contracting apparatus.

CONDITIONAL EMBEDDEDNESS & ORGANIZATIONS' ECONOMIC CAPITAL

Sociologists and other organizational scholars have established a strong link between organizations' embeddedness and economic outcomes across organizational contexts. The idea that economic action can be fully understood only by examining the social relations within which actors are embedded has become a widely accepted idea within sociology (Granovetter 1985). It has served as the basis for a wide range of research that has attempted to bring empirical support to theories about the relationship between organizations' embeddedness and economic outcomes. For example, Uzzi (1999) investigated how social embeddedness affects an organization's acquisition and cost of financial capital in middle-market banking, finding that organizations' economic outcomes in this sector were a product of organizational characteristics and the socially arranged opportunity structures within which they are embedded. Mizruchi and Stearns (2001), on the other hand, found that while banking organizations preferred to deal with those that they trust, an organization's embeddedness hindered their ability to close deals with other banking organizations. In their study of American trade policy, Dreiling and Darves (2011) concluded that higher levels of embeddedness facilitated greater collaboration and political unity amongst organizations advocating for free-trade policies. Similarly, Ingram and Roberts (2000) found that embeddedness led to enhanced collaboration, mitigated competition, and better information exchange amongst competing organizations in the Sydney hotel industry. Each of these studies effectively demonstrates a strong relationship between embeddedness and organizations' economic outcomes. That said, the substantial variation in terms of the quality and directionality of this relationship across different organization contexts suggests that this relationship may ultimately be conditional on other factors.

Conditional embeddedness, the idea that the relationship between organizations' embeddedness and economic outcomes may be contingent on other factors, was introduced by Mizruchi, Stearns, and Marquis (2006) in their study of borrowing amongst large US corporations. Though they were able to establish a connection between embeddedness and organizations' ability to acquire financing, the impact of such embeddedness was found to be historically contingent and significantly affected by changes to the institutional environment over time. Other research has also found evidence of conditional embeddedness at the individual level of analysis. Burt (1997), for instance, showed that the sparse structure of relations that facilitated the rapid promotion of male managers had the opposite effect for women and that minority managers were also largely denied the benefits of such social structures in some contexts. A study by Ortiz de Mandojana and Aragon-Correa (2015) found that the impact of embedded relations between board directors on corporate performance was contingent on the diversity of such relations and directors' links to parent firms.

While time and individual-level characteristics may serve as important factors for the potential conditional nature of organizations' embeddedness, it is essential to consider other possible dimensions of this conditionality. Though organizations are frequently used as the primary unit of analysis, absent from the organizational network literature in this area is work that explores how this conditionality may be affected by the characteristics of the organizations themselves. An organization-level examination of the conditional nature of the relationship between organizations' embeddedness and economic outcomes could benefit our understanding of the nature of this conditionality by bringing organizations to the forefront of this conversation. Given the wide range of possible organizational characteristics, this approach to conditional embeddedness opens the potential for many different lines of inquiry across a myriad of organizational contexts. This study thus examines the extent to which the relationship between embeddedness and economic capital is conditional upon different types of organizations, ownership, and industry. Though these organizational characteristics are far from exhaustive, they serve as valuable starting points for organization-level analyses of conditional embeddedness and economic capital. Below, I discuss the case of surveillance organizations and its connection to these ideas.

THE CASE OF SURVEILLANCE ORGANIZATIONS

In the years since 9/11, newly passed legislation, such as the Patriot Act, as well as advances in digital technologies, have fueled the growth of surveillance in the US to previously unimaginable levels. Consequently, this has been followed by the substantial expansion of the network of public and private organizations involved in these surveillance practices (Ball et al. 2015; Brayne 2017; Burke 2020). In 2019, $381.2 billion worth of contracts were awarded by defense agencies alone (Government Accountability Office 2019). As this study shows, the US surveillance apparatus has grown in such a way that what typically constitutes a “surveillance organization” is no longer limited to only intelligence agencies, law enforcement, and defense contractors. Indeed, organizations contracted by the US government to engage in surveillance practices operate in various industries, including defense and space, information technology, law, finance, energy, and education. The expansion of surveillance practices into these sectors means that surveillance organizations represent a valuable case for the study of organizational networks more broadly. However, the stakes and consequences of this network are arguably far more severe than other organizational networks. The growth of this apparatus of public and private surveillance organizations into multiple industries and sectors of the economy also means the network has become structured in such a way that it could enable the observation of nearly every aspect of Americans’ lives. For purposes of transparency and accountability alone, it is thus crucial that we understand what kinds of organizations are embedded within such networks and how they operate. The privatization of surveillance has also meant a growth in the number and size of contracts handed out by the US government to carry out such efforts. While economic capital plays a significant role in maintaining and perpetuating this network of surveillance organizations, we still know very little about how economic capital is distributed within this inter-organizational network.

The US government annually awards hundreds of billions of dollars in contracts to private organizations to meet the needs of government agencies and the military (usa.gov n.d.). Although these public-private partnerships have existed in the US for several decades, the growth in their use has accelerated since the 1980s (Becker and Patterson 2005). In contrast to private sector contracts, government contracts are subject to numerous statutes, regulations, and policies which seek to encourage maximum competition, ensure proper spending of taxpayers' money, and provide the government with special contractual rights, including the right to unilaterally change contract terms and conditions or terminate the contract altogether (Legal Information Institute n.d.). For example, the US government contracts are bound to goals set by the Federal Acquisition Streamlining Act (FASA) to award specific percentages of contracts to different kinds of disadvantaged organizations. These goals include awarding 23% of contracts to small businesses, 5% to small disadvantaged businesses, 3% to service-disabled and veteran-owned small businesses, and 5% to women-owned small businesses (US Small Business Administration 2019a). The process of awarding government contracts is thus assumed to be reasonably straightforward: organizations place competitive bids, and then organizations are selected for contract awards by government agencies based on the strength and cost of their bids with some additional consideration for organizations classified as disadvantaged.

The regulatory and legal constraints on contract selection processes alone should, theoretically, limit the impact of external factors, such as organizations' embeddedness, on the distribution of economic capital. However, even in such a constrained environment, persistent problems with selecting and awarding government contracts raise questions about the potential for external factors to play a considerable role in how economic capital is distributed. For instance, although competition is a heavily regulated element of the contract process, many contracts are still not competitively sourced. In 2019, 36.5% of the $586.2 billion in contracts awarded government-wide and 46.2% of the $381.2 billion awarded by defense agencies were non-competitive sole-source contracts, meaning contracts were awarded to a single organization without any kind of competitive bidding process (Government Accountability Office 2019). Recent work by Dahlström, Fazekas, and Lewis (2020) suggests that these kinds of non-competitive contracts are most often tied to politicized government offices, indicating potential political favoritism and partisanship in the non-competitive contract selection process. Also, despite the rule-intensive environment, contract decision-making officials possess significant discretion to "set specific product or service requirements," "establish criteria for evaluating proposals," and "determine the respective weighting of evaluation criteria for each bid/proposal process" (Brunjes and Kellough 2018:520). Consequently, contracting officials may play a significant gate-keeping role in selecting organizations, especially when it comes to disadvantaged organizations (Brunjes and Kellough 2018; Fernandez, Malatesta, and Smith 2013; Smith and Fernandez 2010; Zarit 2018).

Past explanations of economic capital in the broader context of government contracting have thus primarily focused on the legal and regulatory constraints placed on contracting agencies or the decision-making of individual contracting officials. Entirely left out of such explanations within this context are the role of social structure and the organizations themselves. This omission is especially glaring given the complex social dynamics (i.e., political favoritism and partisanship) shown to play a role in the contract decision-making process. This selective, discretionary nature of contract awards could, in theory, create an environment where organizations' position within the broader network structure could play a significant role in their acquisition of economic capital. Further, this relationship between embeddedness and economic capital may vary significantly across organizations, given the use of specific organizational characteristics as criteria for contract awards. The case of surveillance organizations could therefore be useful in providing significant insights into the nature of conditional embeddedness within the context of government contracting and organizational networks more broadly. The following section outlines the data and methods used to investigate this case.

DATA

The primary source of data for this study came from Transparency Toolkit's ICWatch database. Transparency Toolkit is a non-profit organization that uses digital tools and open-source data to bring greater public awareness of surveillance practices and potential human rights violations. The ICWatch data used here consists of individual profiles scraped from the popular professional networking website, LinkedIn.com. To develop this database, Transparency Toolkit used a web scraper algorithm to collect public profile information based on a list of search terms that included the names of surveillance programs identified in documents released by Edward Snowden in 2013. If an individual used words or names from one of these programs in their job descriptions, the scraper collected the entire profile, including information about which surveillance program they participated in, job history (job title, company, start/end date, and description for each job), skills, educational history, and geographical location/area. Information about the individuals' employers (organizations) mentioned in these profiles, including organizational industry, was also included.

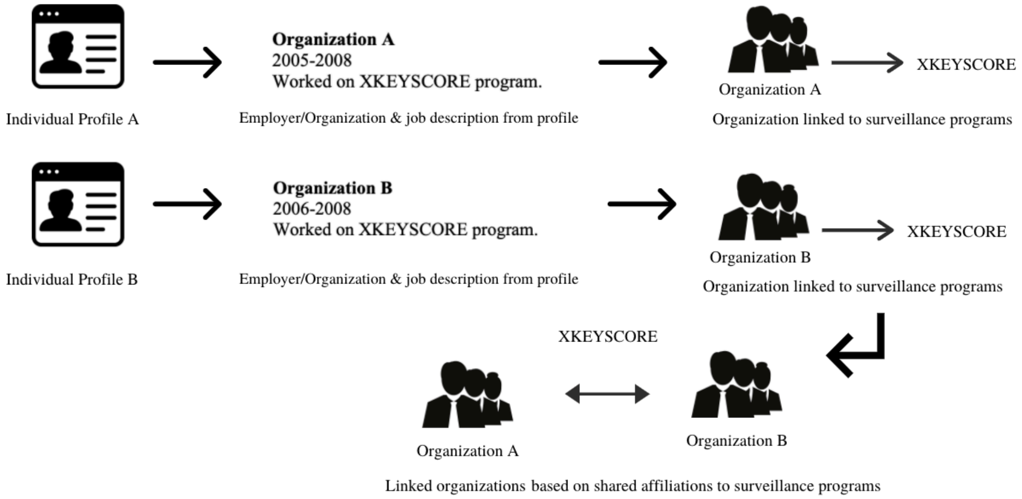
Individual Profile A
Organization A
2005-2008
Worked on XKEYSCORE program.
Employer/Organization & job description from profile
Organization A
XKEYSCORE
Organization linked to surveillance programs
Individual Profile B
Organization B
2006-2008
Worked on XKEYSCORE program.
Employer/Organization & job description from profile
Organization B
XKEYSCORE
Organization linked to surveillance programs
XKEYSCORE
Organization A
Organization B
Linked organizations based on shared affiliations to surveillance programs

Figure 3.1: Conversion of Individual Data to Inter-Organizational Network Data.

Figure 3.1 depicts the process of converting these individual-level profile data into organization-level network data. This conversion to network data was necessary to measure the primary independent variable of interest, organizations' embeddedness. Organizations thus represent the primary unit of analysis in this study. As illustrated in Figure 3.1, organizations were identified using the employment histories listed in individuals' profiles. These organizations were then linked to specific surveillance programs mentioned by individuals in their job descriptions. The connections between these organizations and their respective surveillance programs were then used to create connections between organizations based on their shared affiliations to surveillance programs. Thus, organizations presumed to be working on the same surveillance programs, such as "PRISM" or "XKEYSCORE," would be connected in this network. While these organizations are affiliated with one another through these programs, these data cannot speak to the exact nature of the ties between organizations. Given the vast, diverse nature of US government surveillance programs, these connections could represent several different types of relationships (i.e., financial, providing technical services, knowledge-sharing, etc.). The complete inter-organizational network data consisted of a total of 30,724 organizations and 1,048,575 inter-organizational ties.

In addition to the ICWatch data, this study also used data gathered from the public government spending database, USASpending.gov. A web scraper was used to gather additional data about the organizations in the original ICWatch dataset. The USASpending data complemented the ICWatch data with additional organizational variables, including information about organizations' geographical locations, organizational characteristics (e.g., organization type and ownership), and the number of and amount of money from US government contracts. The data from ICWatch and USASpending were combined to create one sizeable relational dataset.

As previously discussed, while the stereotypical "surveillance actor" is often assumed to be a secretive government agency or defense contractor, the organizations present in these data operate within various industries, including defense and space, information technology, law, finance, energy, and education. They were also diverse with regard to their organizational ownership and type. Thus, these data paint a picture of an incredibly expansive, far-reaching surveillance apparatus, with partnerships among a wide variety of organizations and across various industries and sectors.

DEPENDENT VARIABLE

The dependent variable of interest, economic capital, was operationalized using two different measures: the total number of government contracts received and the total amount of money received from government contracts. These two categories from the USASpending data represent essential measures of an organizations' involvement in surveillance programs. The organizations under study here operate within a capitalistic market, meaning they compete over scarce financial resources that come primarily through participation in various government surveillance programs. Analyzing these variables is crucial for understanding the organizational and institutional factors that drive organizations' economic outcomes. While the total number of contracts and dollars received are expected to be correlated, operationalizing economic capital with these two measures acted as a robustness check. It was also essential to include both measures, given the variability of government contracts. Measuring the number of contracts alone would place greater value on an organization that, for instance, received a higher number of contracts worth smaller amounts of money. Conversely, only including a measure of the total dollar amount received would mean a greater emphasis on organizations that, for example, received a small number of very high-value contracts. Thus, it was essential to include both measures to get a more reliable picture of economic capital in this context.

INDEPENDENT VARIABLES

Embeddedness, the primary independent variable of interest, was operationalized using eigenvector centrality, which Bonacich (2007: 555) frames as "a weighted sum of not only direct connections but indirect connections." In other words, eigenvector centrality measures the importance of an organization based on its connections to other well-connected organizations. Organizations with higher eigenvector centrality may be in an advantageous position to receive and transmit influence over other actors through their connections to highly connected others (Lakon, Godette, and Hipp 2008). Past studies have shown this measure to have significant implications for individual and group processes, including relations within and among organizations (Barnes-Mauthe et al. 2015; Moore, Eng, and Daniel 2003; Stefani and Torriero 2013).

In addition to embeddedness, this study also includes several control variables, including organization type, industry, and organizational ownership. The organization type variable controlled for and measured the effects of various kinds of organizations, including foreign government, local government, national government, state government, manufacturer of goods, small business, private university, and public university. It is important to note that these categories are not exhaustive or mutually exclusive, as not all organizations fall into one of these typologies, and some organizations fall into multiple typologies (e.g., small business and manufacturer of goods). Also, it is worth noting that the definition of "small business" for contracting purposes means the inclusion of organizations that are by no means small (in terms of the number of employees) at all. This is because the Small Business Administration's (SBA) criteria for what constitutes a small business varies by industry. For example, in manufacturing, the maximum number of employees ranges from 500 to 1,500, whereas the retail industry's maximum is $7.5 million in average annual receipts (US Small Business Administration 2019b). It is also essential to include such a measure as a control given the statutory emphasis on providing contracts to small business organizations. Though not exhaustive, these particular categories represent several types of organizations known to be involved in government surveillance programs (Bamford 2009; Greenwald 2014). Thus, the organization type category comprises multiple independent variables rather than a single categorical independent variable.

The organizational ownership variable controls for the effect of ownership on the dependent variables. This categorical variable breaks down into the following categories: US-owned, foreign-owned and located, foreign-owned and US-located, minority, female, and veteran. Like the organization type variable, the organizational ownership variable is not exhaustive or mutually exclusive. Some organizations fall under multiple ownership categories (e.g., minority and female), whereas others do not fall under any ownership category (e.g., government agencies). The ownership variable as operationalized here represents a collection of multiple independent variables measuring different types of ownership. These categories were drawn directly from the USASpending data. The first three categories measured whether a domestic or foreign entity owns an organization and whether its location was inside or outside the US. The final three categories of organizational ownership pertained to special disadvantaged categories of ownership. As previously noted, the US government is bound to goals set by the Federal Acquisition Streamlining Act (FASA) to award specific percentages of contracts to these kinds of disadvantaged organizations. Therefore, these organizations are of particular interest because they represent an opportunity to gauge their participation within this broad organizational network and evaluate the relative strength of such policies for promoting their inclusion.

The industry variable serves as a control for organizations' respective industries' effect on the dependent variables. This categorical variable included the following industries: defense and space, military, information technology, law, education and research, energy and resources, finance and business, and other. These categories are considered mutually exclusive and exhaustive, with all surveillance organizations falling into one of these categories. Thus, the industry variable represents a single categorical variable measuring the type of industry rather than a collection of independent variables. These categories were operationalized using the typologies initially listed in the ICWatch data. For purposes of analysis, the defense and space category is used as the reference category.

INTERACTION TERMS AND HYPOTHESES

Interaction terms were also included in the analyses to measure the relationship between embeddedness and economic capital across different organizational characteristics. These interaction terms represent the interaction between embeddedness and each of the independent variables described above. This allows for a more detailed understanding of the relationship between embeddedness and economic capital and, more specifically, the extent to which this relationship is conditional on different organizational characteristics. Analyses of the interaction between variables, in this case, can provide insights into how specific organizational characteristics impact this relationship and the intensity and direction of such an impact across different values of these characteristics.

In alignment with the independent variables previously discussed, this conditionality will be tested on three primary levels: organization type, ownership type, and industry. At a broad level, it is hypothesized that the relationship between embeddedness and economic capital will be conditional on these three variables. The degree and direction of such conditionality are thus expected to vary across each of these three categories. To this end, the following hypotheses were made:

H1: The relationship between embeddedness and economic capital will be conditional on organization type, ownership type, and industry.

H2: The national government, state government, manufacturer of goods, public university, and private university organization types will have a positive conditional effect on the relationship between embeddedness and economic capital, while the small business, local government, and foreign government organization types will have a negative conditional effect on the relationship.

H3: The US-owned and foreign-owned and US-located ownership types will have a positive conditional effect on the relationship between embeddedness and economic capital, while all other ownership types will have a negative conditional effect.

H4: Organizations' industry will have a conditional effect on the relationship between embeddedness and economic capital. Specifically, compared to the defense and space industry (reference), all other industries will have a lower conditional effect on the relationship between embeddedness and economic capital.

The following section outlines the methods used to test each of these hypotheses and investigate the conditionality of embeddedness and economic capital in the context of the network of surveillance organizations.

METHODS

This study utilized ordinary least squares (OLS) regression models to determine the independent variables' effects on the dependent variable, economic capital. OLS regression models were thus run to assess the independent variables' effects on both economic capital measures: the total number of government contracts received and the total amount of money received from government contracts. Breusch-Pagan tests for heteroscedasticity were run on each regression model to determine whether the variance of standard errors was consistent across observations. This was necessary because the presence of heteroscedasticity can cause OLS estimates to be inefficient and lead to faulty inferences when testing statistical hypotheses (White 1980). Both OLS regression models had heteroscedasticity present ($p < 0.001$). To address this, I used heteroscedasticity-corrected covariance matrix estimation (HCCME) to obtain robust standard errors for each model (Lindgren 2010; Zeileis 2004).

It is also important to note that while the coefficients and effect sizes from the regression models can be useful for additive linear models, they are often less insightful for multiplicative interaction linear models (Brambor, Clark, and Golder 2006). This is because the coefficients for independent variables only indicate the independent variable's marginal effect on the dependent variable for the unique and sometimes rare case in which the conditioning variable is zero. For this reason, marginal effects plots are thus included to provide a clearer interpretation of how the relationship between embeddedness and economic capital varies across different independent variables. The coefficients from each regression model are used to predict values of economic capital across different values of embeddedness for each independent variable. This allows for a more straightforward interpretation of the interaction terms and a better understanding of the extent that the relationship between embeddedness and economic capital is conditional on various organizational characteristics.

RESULTS

As previously discussed, economic capital was operationalized using two measures, the total number of contracts and the total contract amount. Tables and figures can be found at the end of this chapter. Table 3.1 presents the results of the two OLS regression models used to determine the effects of the independent variables on economic capital. Economic capital is operationalized as the total number of contracts in Model 1 and the total contract amount in Model 2. Coefficients and standard errors for the independent variables and interaction terms are provided for each model. Figures 3.2, 3.3, and 3.4 present the marginal effects plots of predicted values of economic capital (total contracts) for the organization type, ownership, and industry variables at different levels of embeddedness. Figures 3.5, 3.6, and 3.7 present the marginal effects plots of predicted values of economic capital (total amount) for the organization type, ownership, and industry variables at different levels of embeddedness.

The regression results for Model 1 indicate that several interaction terms were statistically significant ($p < 0.05$). The model had an adjusted R-squared value of 0.43, meaning the model explains 43% of the variance in the dependent variable, economic capital. Starting with the organization type category, the interaction between embeddedness and the local government, national government, manufacturer of goods, private university, and public university categories were all statistically significant. Among these five variables, all but the national government variable returned statistically significant, positive coefficients. This indicates that these four organization types may amplify the relationship between embeddedness and economic capital in a positive fashion. The national government organization type's significant negative coefficient, on the other hand, suggests that it may have a substantial reductive effect on the relationship between embeddedness and economic capital. This is supported by the marginal effects plots in Figure 3.2, which depict a more substantial positive slope for local government, manufacturer of goods, private university, and public university organization types compared to their respective reference categories. Conversely, the marginal effects plot for the national government organization type indicates, in stark contrast to the positive slope of its reference line, a robust negative slope with economic capital decreasing at higher levels of embeddedness. These results are somewhat surprising, as they go against the hypothesis (*H2*) that the national government organization type would have a positive conditional effect and the local government would have a negative conditional effect.

Among the ownership type interaction terms, the US-owned and female-owned terms were statistically significant with positive coefficients. Like above, this suggests that the US and female ownership may amplify the relationship between embeddedness and economic capital. This is supported by the margin effects plots in Figure 3.3, which indicate that the slope of the lines for both US and female ownership is positive. Further, the higher slopes for both categories when compared to the lines for their reference categories (non-US and male-owned) signifies that the relationship between embeddedness and economic capital is amplified for organizations with US and female ownership. While it was hypothesized (*H3*) that US-owned organizations would have a positive conditional effect, it was surprising to see the strong positive conditional effect for female ownership. The conditional effect of female ownership stands in stark contrast to other categories of disadvantaged ownership, such as veteran and minority ownership, where no meaningful conditional effects were found.

Regarding industry type, the military, finance and business, and other industry interaction terms were statistically significant. The coefficients for these three terms were negative, suggesting that the relationship between embeddedness and economic capital may be significantly weaker than the reference category, defense and space. The marginal effects plots in Figure 3.4 support this notion, as the slopes of the lines for these three industry categories, while positive, are substantially lower than that of defense and space. This indicates that the conditional effect is lower for the military, finance and business, and other industries when compared to the defense and space industry. Surprisingly, the energy and resources industry was found to be the lone industry with a more substantial conditional effect than the defense and space industry, and the conditional effect for the information technology industry was nearly identical to the defense and space industry. Notably, Figure 3.4 shows a significant gap between the conditional effects of the top three industries (energy and resources, informational technology, and defense and space) and all other industries. These results thus seem to provide some support for the hypothesis (*H4*) that the defense and space industry would have a stronger conditional effect on the relationship between embeddedness and economic capital than other industries.

The second column of Table 3.1 displays the OLS regression model results used to determine the effects of the independent variables on economic capital, operationalized as the total contract amount. The model had an adjusted R-squared value of 0.42, meaning the model accounts for 42% of the variance in the dependent variable, economic capital. The interaction terms for the organization type variables, the coefficients for the local government, national government, manufacturer of goods, small business, private university, and public university types were statistically significant. All but the national government and small business categories returned significant positive coefficients. These positive coefficients suggest that these variables amplify the relationship between embeddedness and economic capital. The marginal effects plots in Figure 3.5 support this notion, as the slope of the lines for these four variables is positive and higher than the slopes of their respective reference lines. This means that the increase in economic capital for each unit increase in embeddedness is higher for these variables when compared to their reference categories. In contrast, the negative coefficients for the national government and small business interaction terms suggest that these two organization types may have a significant reductive effect on the relationship between embeddedness and economic capital. This is supported by the margins effects plots in Figure 3.5 that illustrate the strong negative slope for the lines for both national government and small business organization types. These lines' slopes are in stark contrast to the positive slopes of the lines for their respective reference categories.

When it comes to the ownership type variables, the coefficients for the US and female-owned interaction terms were once again found to be statistically significant and positive. This supports the previous findings from the first OLS model that both variables amplify the relationship between embeddedness and economic capital. The marginal effects plots in Figure 3.6 also support this notion as the slopes of the lines for both ownership types are positive and higher than the slopes of the lines for their respective reference categories. Though other ownership categories did not return significant coefficients in the regression table, the marginal effects plots in Figure 3.6 provide some evidence that the relationship between embeddedness and economic capital might also be affected by other ownership types. The flat slope of the line pertaining to the foreign-owned and located ownership type and the more substantial slope of its reference line indicates that the relationship between embeddedness and economic capital may be weaker for organizations with foreign-owned and located ownership. On the other hand, the higher positive slope for foreign-owned and US-located ownership compared to its reference line suggests that this type of ownership amplifies the relationship between embeddedness and economic capital as hypothesized (*H3*).

Lastly, unlike the first OLS model, the second model returned no significant interaction terms pertaining to industry. While there is some differentiation among industries' marginal effects in Figure 3.7, it lacks the clear distinction seen in the previous industry marginal effects plot in Figure 3.4. The lack of significance among industry interaction terms in the second model makes it difficult to be confident that such differences are statistically meaningful. The lack of consistent results across both OLS models and marginal effects plots suggests that organizations' industry may not have a conditional effect on the relationship between embeddedness and economic capital as hypothesized initially (*H4*).

Overall, the analyses' results indicate that the relationship between embeddedness and economic capital varies across different categories of organizational types, ownership, and industry. As previously discussed, the use of two OLS models allowed for a more robust investigation of the conditional effects of these variables. Generally, the results from both models were consistent and provided evidence that certain kinds of organization and ownership types have a robust conditional effect on the relationship between embeddedness and economic capital as hypothesized (*H1, H2, H3*). While there was some evidence from the first model to suggest that industry may also play a role, the results of the second model showed no support for this hypothesis (*H4*).

DISCUSSION

This paper employed OLS regression techniques to analyze a novel relational dataset that combines network data on partnerships between surveillance organizations and financial data on contracts awarded by the US government. The results of these analyses suggest that while there is a strong relationship between surveillance organizations' embeddedness and economic capital, the directionality and degree of this relationship were conditional on organization type, ownership type, and industry.

Among the most critical variables that had an impact on this relationship was the organizational type. The results of both sets of regression analyses indicated that some organization types amplified the relationship between embeddedness and economic capital. More specifically, organizations falling under the local government, manufacturer of goods, private university, and public university categories were found to have more substantial effects when compared to other organizations. Figures 3.2 and 3.5 indicated that the relationship between embeddedness and economic capital was powerful for private and public universities. This means that network position is an especially strong influence on universities' ability to obtain economic capital through government contracts. Similarly, manufacturers of goods were also found to have a stronger relationship between embeddedness and economic capital than other organizations. This is perhaps to be expected, as manufacturers serve as a vital organization in the context of surveillance by producing the hardware and technologies necessary to conduct surveillance on a massive, global scale (Greenwald 2014).

The national government organization type, on the other hand, had a strong negative relationship between embeddedness and economic capital compared to all other organizations. This goes against what was initially hypothesized, as US national government organizations are deeply embedded within this organizational context. However, this disconnect could be explained by the fact that most national government organizations award surveillance contracts rather than receive them. Small businesses were found to have a positive relationship between embeddedness and total contracts, but a negative relationship between embeddedness and total contract amount compared to all other organizations. This divergence between OLS models indicates that embeddedness can be important for small businesses to acquire contracts but may have a reductive effect on contract dollars. The fact that highly embedded small businesses receive higher numbers of contracts yet lower dollar amounts raises some questions about government contracting processes. This may be evidence of a pattern of awarding numerous smaller (in terms of dollar amount) contracts to small businesses to adhere to legal guidelines that obligate contracting agencies to award a certain percentage of contracts to such organizations. Another possibility is that this results from the classification of some small businesses in certain industries based upon their earnings. In some industries, small businesses that earn over a certain threshold would cease to be classified as small businesses. Overall, these results evidence the conditionality of the relationship between embeddedness and economic capital in organizational networks and government contracting, specifically as it relates to organizational type.

The OLS regression results also evidence how the relationship between embeddedness and economic capital varies across different kinds of organizational ownership. Compared to other ownership types, US-owned, female-owned, and foreign-owned and US-located organizations were found to have a stronger positive relationship between embeddedness and economic capital. This suggests that these organizations' network position potentially plays a more significant role in obtaining economic capital than organizations with other ownership types. The results for US-owned and foreign-owned and US-located organizations suggest that the relationship between embeddedness and economic capital is stronger for organizations based in the US, whether owned by a domestic or foreign entity. This would indicate that geographical location plays an essential role in organizations' ability to leverage their network position to obtain economic capital (and vice versa). As previously noted, the strong conditionality regarding female ownership was surprising given its legal status and the strength of such conditionality compared to other types of disadvantaged ownership (i.e., veteran and minority ownership).

Given that female-owned organizations have historically been underrepresented when it comes to government contract awards, these results have potentially important implications for identifying methods of greater inclusion of organizations with female ownership. The strength of the relationship between embeddedness and economic capital for such organizations lends itself to policy solutions that provide mechanisms for enhancing female-owned organizations' network position, including promoting greater partnerships of female-owned organizations with other organizations. This finding also stands in contrast to past network studies at the individual level that have found strong negative conditionality relating to gender and, specifically, the differential outcomes between men and women of similar network positions when it comes to acquiring promotions and other economic outcomes (Burt 1997).

These findings pose significant implications for understanding economic capital in the context of organizations and government contracting and the consequences of this inter-organizational surveillance network's existence and structure. The strong association between embeddedness and economic capital indicates that not only does surveillance organizations' position with this inter-organizational network play a significant role when it comes to the distribution of government contracts but that it is conditional on the type of organization and its ownership. While past explanations of economic capital in government contracting have focused primarily on the institutional and individual levels to explain economic capital in this context, the results clearly show that organizations and, more specifically, the network structure of such organizations deserve greater consideration. Further, this study suggests that organizational scholars examining the relationship between organizations' network structure and economic outcomes should cast increased attention to the conditionality of this relationship and how it interacts with and varies across organizational characteristics, such as organizational type, ownership, and industry. The omission of such conditionality holds serious consequences, as scholars risk overlooking the structural mechanisms that lead to differential outcomes among organizations. As evidenced by the results of this study, the popular assumption that a more central social (network) position leads to greater or more successful economic outcomes is not always accurate in the context of organizations.

While this study focuses on the specific context of surveillance organizations, the findings may provide broader insight into the structural mechanisms that shape the distribution of economic capital in other organizational contexts. The sheer size and diversity of the network of surveillance organizations, analyzed here, lends itself to broader generalizability of these findings to many other kinds of organizational networks that exhibit similar network characteristics and rely upon the exchange of economic capital. As noted above, these findings also provide important insights into government contracting more broadly. The strong conditionality of female ownership, for example, suggests that policies and strategies that strengthen such organizations' network position may be effective in promoting more equitable access to economic capital. Similarly, the lack of a conditional relationship for other disadvantaged ownership categories, such as minority-owned and veteran-owned organizations, supports previous work that has highlighted the historical struggles and existing structural barriers for such organizations when it comes to acquiring economic capital.

It is also essential to acknowledge the limitations of this study. First, the use of social media data inherently limits the generalizability of these findings. While large digital datasets are often celebrated for providing access to "complete" populations, specific populations are more likely to turn up in datasets like those used here (Lewis 2015). This dataset also fails to capture individuals who do not have a LinkedIn profile. The sampling method of the scraping algorithm for the ICWatch dataset also does not capture those who had a LinkedIn profile and were involved in surveillance practices but did not explicitly mention a surveillance program in their profiles. Additionally, individuals working in particular industries or organizations may be less likely to use LinkedIn or report their involvement in surveillance programs in their profiles. As previously discussed, the relationship between organizations' embeddedness and economic capital is not necessarily unidirectional. Organizations with access to more resources and economic capital can presumably use such resources to situate themselves in advantageous network positions. Thus, while embeddedness may lead to greater economic capital for some organizations, the reverse may also be true. Caution should be exercised in interpreting these results, especially when assigning directionality and causality to the relationships between variables in this study. This is especially true for the interaction terms in the regression models, where the interpretation of relationships between multiple variables introduces additional complexity.

Table 3.1: OLS Regression Models of Independent Variables on Economic Capital

Variable (n=30,724)	(1) Total Contracts	(2) Total Amount
Constant	204.70*** (2.91)	43.40*** (2.03)
Network		
Embeddedness	691.76*** (94.32)	424.11*** (65.73)
Organization Type		
Foreign Government	-450.12** (145.13)	-214.09* (101.14)
Local Government	-241.74*** (14.20)	-233.50*** (9.89)
National Government	230.56*** (18.92)	271.21*** (13.19)
State Government	431.14*** (14.69)	270.77*** (10.24)
Manufacturer of Goods	118.88*** (9.74)	32.09*** (6.79)
Small Business	-180.62*** (6.92)	-77.32*** (4.82)
Private University	220.32*** (23.98)	70.07*** (16.71)
Public University	348.72*** (20.57)	228.01*** (14.34)
Ownership		
US-Owned	139.69*** (6.09)	80.91*** (4.24)
Foreign-Owned and Located	-57.06*** (13.44)	-17.30 (9.37)
Foreign-Owned and US-Located	177.99*** (37.49)	85.76** (26.13)
Minority	86.14*** (8.88)	46.72*** (6.19)
Female	-66.94** (21.25)	-59.95*** (14.81)
Veteran	42.54*** (11.85)	-14.36 (8.26)
Industry (Reference: Defense and Space)		
Military	-18.76 (9.96)	33.03*** (6.94)
Information Technology	-24.45*** (6.91)	20.30*** (4.81)
Law	-1.46 (13.87)	30.90** (9.67)
Education & Research	-12.09 (12.94)	32.89*** (9.02)
Energy and Resources	-51.75*** (13.21)	22.25* (9.20)
Finance and Business	-40.01*** (8.43)	10.51 (5.87)
Other	-43.79*** (8.64)	27.94*** (6.02)
Interaction Terms		
Foreign Government x Embed.	6998.50 (6070.30)	3868.48 (423.04)
Local Government x Embed.	640.42* (263.57)	552.16** (183.68)
National Government x Embed.	-1437.46*** (253.94)	-1017.03*** (176.97)
State Government x Embed.	78.85 (253.94)	4.54 (152.22)
Manufacturer of Goods x Embed.	1394.58*** (205.82)	823.89** (143.44)
Small Business x Embed.	-234.31 (189.85)	-570.67*** (132.31)
Private University x Embed.	7346.31*** (742.96)	3750.37*** (517.65)
Public University x Embed.	2085.01*** (630.13)	1766.81*** (439.14)
US-Owned x Embed.	685.00*** (130.97)	483.32*** (91.27)
Foreign-Owned and Located x Embed.	-321.98 (291.52)	-341.63 (203.16)
Foreign-Owned and US-Located x Embed.	1146.88 (989.91)	935.80 (689.87)
Minority x Embed.	-161.18 (208.25)	-5.50 (145.13)
Female x Embed.	1891.45** (710.22)	1269.10* (494.54)
Veteran x Embed.	-498.97 (294.18)	221.17 (205.01)
Military x Embed.	-462.76* (231.11)	-267.78 (161.06)
Information Technology x Embed.	17.23 (162.97)	-110.32 (113.57)
Law x Embed.	-478.80 (270.08)	2.05 (188.22)
Education and Research x Embed.	-525.55 (393.04)	-86.05 (273.91)
Energy and Resources x Embed.	273.00 (315.16)	-94.79 (219.63)
Finance and Business x Embed.	-605.05** (214.00)	-170.79 (149.14)
Other x Embed.	-472.20* (220.49)	-231.38 (153.66)
Adjusted R^2	0.43	0.42

Note: *** $p<0.001$; ** $p<0.01$; * $p<0.05$

Coefficients presented in Model 2 are in the millions (US dollars).

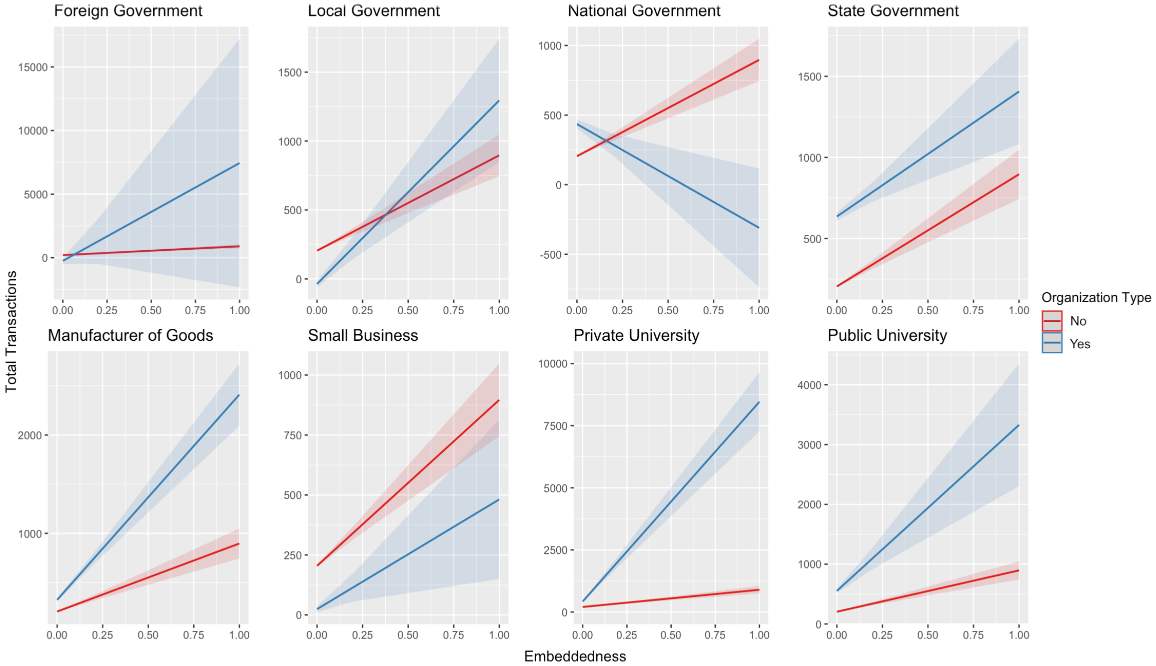

Figure 3.2: Predicted Effects of Embeddedness on Economic Capital (Total Contracts) by Organization Type

Note: Shaded areas depict 95% confidence intervals.

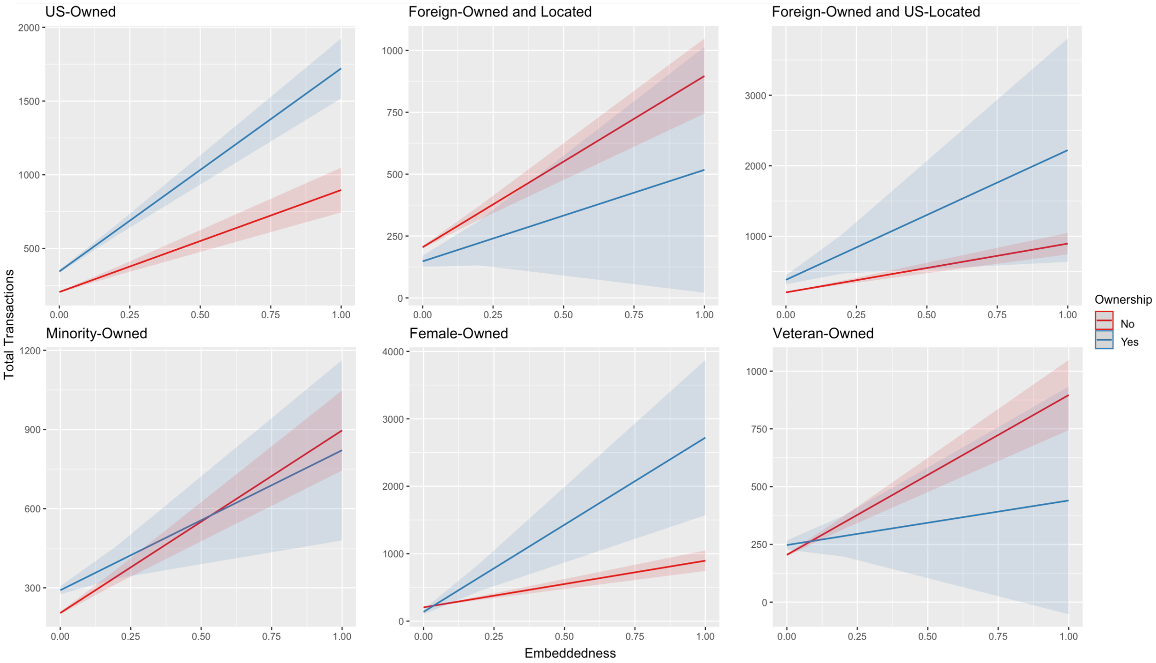

Figure 3.3: Predicted Effects of Embeddedness on Economic Capital (Total Contracts) by Ownership Type

Note: Shaded areas depict 95% confidence intervals.

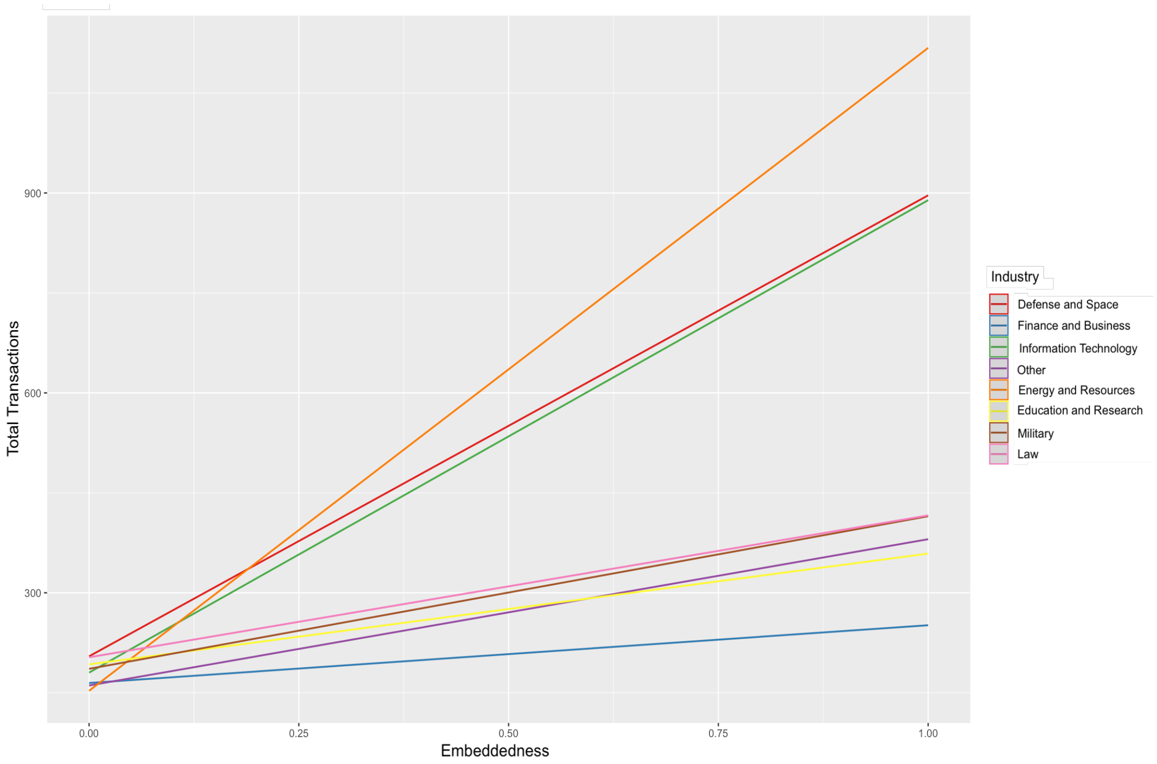

Figure 3.4: Predicted Effects of Embeddedness on Economic Capital (Total Contracts) by Industry

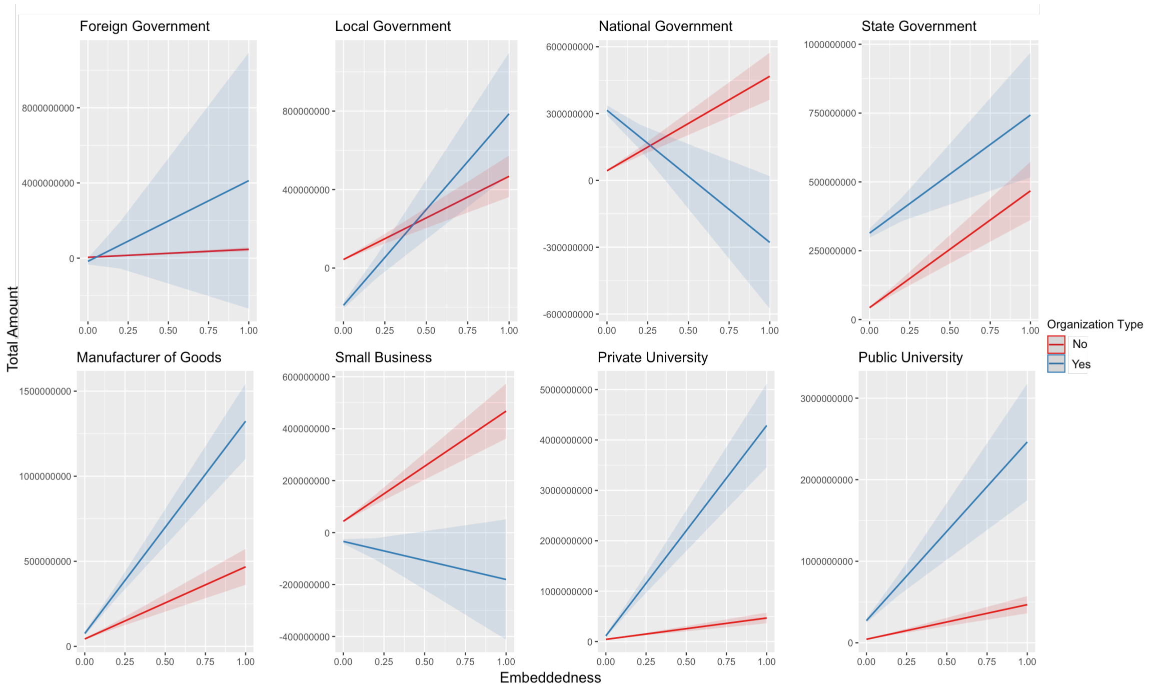

Figure 3.5: Predicted Effects of Embeddedness on Economic Capital (Total Amount) by Organization Type

Note: Shaded areas depict 95% confidence intervals.

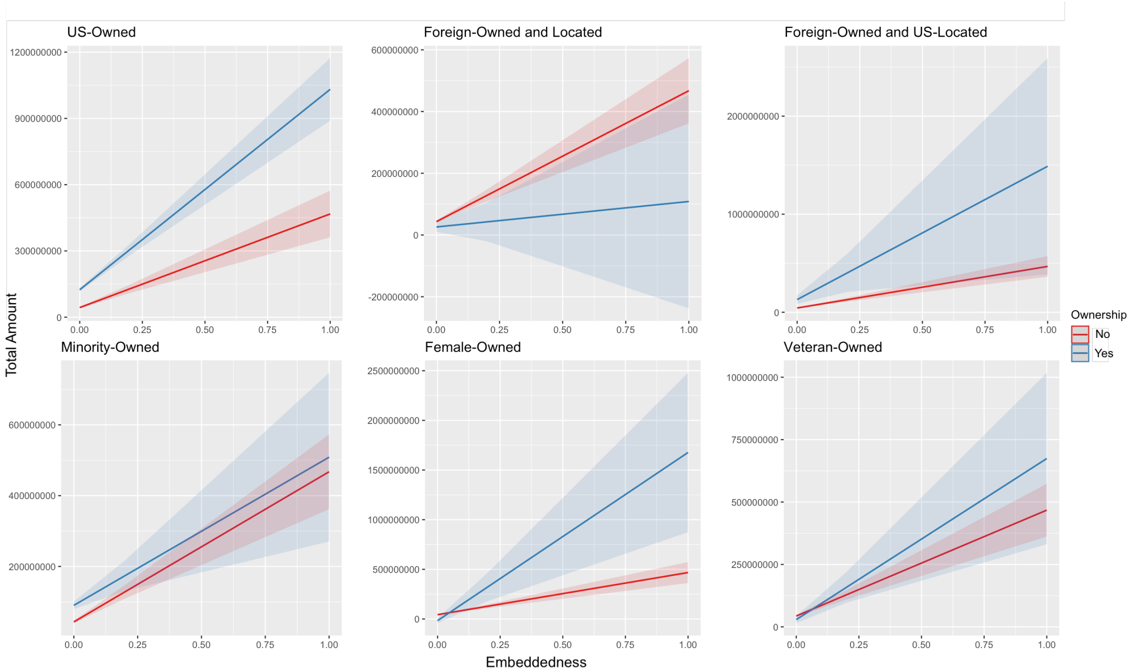

Figure 3.6: Predicted Effects of Embeddedness on Economic Capital (Total Amount) by Ownership Type

Note: Shaded areas depict 95% confidence intervals.

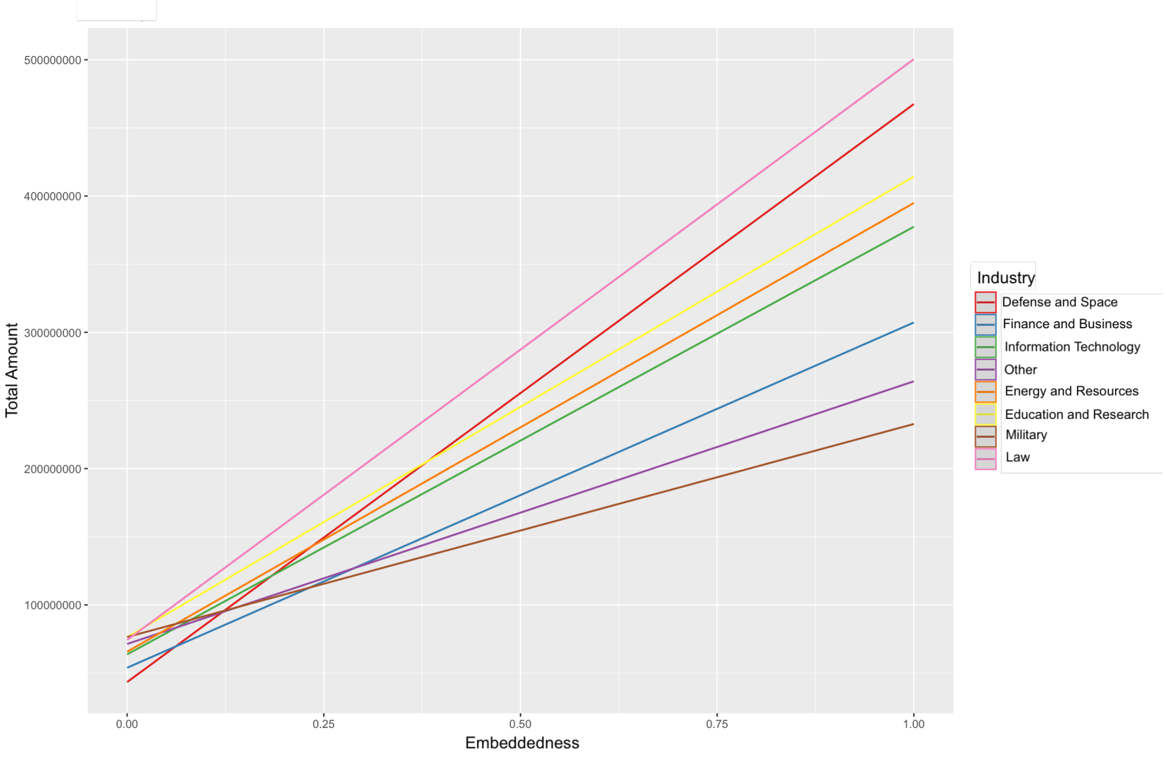

Figure 3.7: Predicted Effects of Embeddedness on Economic Capital (Total Amount) by Industry

CHAPTER 4: THE MATERIALITY OF SURVEILLANCE

INTRODUCTION

Scholars of science and technology studies (STS) and the broader social sciences have long been interested in the materiality of organizations and infrastructure in multiple contexts (Bowker and Star 2000; Cooren 2020; Edwards 1997; Hughes 1993; Latour 1996; Schiller 2006; Schüll 2012; Scott and Orlikowski 2014). In the context of surveillance, the rapid development of digital technologies developed or co-opted for surveillance purposes has led some surveillance scholars to question the limits of more materialist models, especially those derived from Foucault's panopticon, for understanding contemporary surveillance practices (Boyne 2000). While the panopticon has long stood as a concrete model of surveillance practices through visible means of discipline and control, surveillance in the "post-panoptic" society has been conceptualized as a decentralized system of heterogeneous parts that tracks and monitors bodies of information in more opaque and abstract ways (Haggerty and Ericson 2000). This turn towards post-panoptic models of surveillance thus places greater emphasis and attention on the more abstract, immaterial elements of contemporary surveillance practices, such as data, simulation, "cloud" storage, statistical algorithms, and computer code (Bogard 2012). In doing so, however, scholars risk overlooking the material realities of surveillance practices and their inherent ties to physical infrastructures that enable such practices. While there are certainly limitations to the panoptic model of surveillance, the recent dematerialization and theoretical abstraction of surveillance may also serve to further black-box such practices and the actors who carry them out, potentially cast attention away from more tangible and accessible sites of resistance to such practices, and can distract from the material consequences of such practices.

Drawing on materialist approaches to infrastructures (Parks 2015; Star 1999; Sterne 2013) and organizations (Orlikowski 2007), this paper examines the material linkages between surveillance infrastructure and organizations to evidence the need for continued attention and emphasis on the material realities of contemporary surveillance. To this end, this paper employs an analysis of two broad illustrations that evidence such materiality and their importance for understanding modern surveillance practices in the US: 1) the geographies and physical arrangement of surveillance infrastructures and organizations and 2) the material reality and consequences of contemporary surveillance. In the first part of this analysis, open data sources are used to map the geographies of surveillance infrastructure and organizations to identify patterns wherein the material arrangement of surveillance organizations closely aligns with those of two critical pieces of surveillance infrastructure: fusion centers and undersea internet cables. The second part of the analysis draws on Zuboff's (2019) concept of "surveillance capitalism" to examine the material reality and consequences of contemporary surveillance in relation to capitalistic modes of accumulation.

OPERATIONALIZING SURVEILLANCE ORGANIZATIONS AND INFRASTRUCTURES

As discussed later in this paper, there are a variety of types of actors and infrastructures involved in contemporary surveillance practices. It is thus necessary to start by specifying the operationalization of the two primary objects of study in this paper: surveillance organizations and surveillance infrastructures. The term "surveillance organization" broadly refers to organizational actors engaged in surveillance practices. As shown in the second article of this dissertation, modern surveillance organizations constitute both public and private organizations, with those from the private sector representing a wide range of industries. The diverse nature of surveillance organizations is indicative of the expansion of surveillance practices into nearly every aspect of modern life. For this reason, capturing all surveillance organizations within a single research study is incredibly challenging. Even the work of this dissertation, which examines over 31,000 different surveillance organizations, is limited in its ability to speak to all types of surveillance organizations. The specific limitations of these data are discussed in further detail later in this paper.

The term "surveillance infrastructure," on the other hand, is used to broadly refer to the physical, usually digital, "things" or heterogeneous system(s) of "things" (i.e., computer hardware, software, fiber optic cables, data storage) used to enable or engage in surveillance practices, including (but not limited to) digital data collection, transfer, and analysis. While categorized as surveillance infrastructures here, many such infrastructures were not built or developed with surveillance in mind yet have become crucial to making contemporary surveillance practices possible. For instance, the expansion of surveillance into nearly every aspect of modern daily life has rendered digital communications infrastructure and technologies (i.e., telephone poles, smartphones, laptops, wireless routers, and internet cable modems) crucial surveillance infrastructures. While the analyses in this paper focus on two prominent examples of surveillance infrastructure (fusion centers and undersea internet cables), there are myriad objects that, whether explicitly developed for surveillance purposes or not, represent surveillance infrastructures. However, before diving into such analyses, it is necessary to provide greater context around these two primary objects of study and contemporary surveillance practices in the US in general. The following section thus provides a brief background of modern surveillance in the US and some of the theoretical approaches used by surveillance scholars to understand it.

CONTEXTUALIZING MODERN SURVEILLANCE IN THE US

Surveillance in the US, at least in its modern digital form, can be traced as far back as World War I, when telegraph and cable companies like Western Union turned over telegraphic communications to the early predecessor of the National Security Agency (NSA), the "Cipher Bureau" (Bamford 2009). The terrorist attacks on September 11th, 2001 provided the public support needed to expand the US national security apparatus in previously unimaginable ways and paving the way for rapid implementation of laws like the Patriot Act in the immediate aftermath of 9/11 provided the legal mechanisms to scale the US government's surveillance capabilities. Further, the 1990s and early 2000s also saw the meteoric rise of the internet and new, digital forms of communication that presented new opportunities for surveillance of everyday life. In the context of the intelligence failures leading up to the 9/11 attacks, these digital technologies and infrastructures quickly came to be seen as surveillance tools; the growth of partnerships between the US government and private companies meant that such tools were made easily accessible for surveillance purposes (Greenwald 2014).

The partnership between private companies and government organizations has been a critical element of modern surveillance that has not only continued since World War I but has also seen considerable growth in recent years (Burke 2020). Surveillance operations in the US are no longer simply a government security exercise; they have become complex interactions between government agencies and private companies that leverage the nearly endless resources of the US government's national security apparatus to exploit the vast digital communications infrastructures and data operations of the private sector.

Despite the prevalence and sheer scale of surveillance practices by the US government and its private partners, it was not until recently that we learned of the extent and nature of such practices. The revelations by Edward Snowden in June 2013 provided unprecedented insights into the surveillance operations of the NSA and its private partners, revealing the massive scale of monitoring conducted on global populations and details about how they went about doing it (Lyon 2014). Further, it disclosed how "Big Data" technologies have expanded modern surveillance capabilities in recent years. Indeed, the current era of Big Data has cast a double image of surveillance: the familiar "legacy" version of targeted, purposeful spying and the emerging model of ubiquitous, opportunistic data capture (Andrejevic and Gates 2014). The latter image has come to represent what some have labeled "dataveillance," which denotes the systematic monitoring of people or groups using personal data systems to regulate or govern their behavior (Esposti 2014). Dataveillance in this context represents a "socio-algorithmic process" that captures and calculates "flecks of identity," the data trails of our everyday actions, such as our browsing history, financial transactions, and our movements as they are recorded by GPS coordinates on our mobile devices and RFID tags in passports and identity cards (Raley 2013:127). With dataveillance, the reach of today's surveillance organizations has effectively infiltrated nearly every aspect of everyday life. In the next section, I briefly overview theoretical approaches to modern surveillance, especially those related to the materiality of such practices.

THEORIZING MODERN SURVEILLANCE

The prevalence of surveillance practices in modern society has also driven up interest in academic work on the subject in recent years. Many surveillance scholars trace contemporary surveillance studies to the work of Michel Foucault, with some going as far as referring to Foucault as the "grandfather" of surveillance studies (Marx 2015). Foucault's writings in *Discipline and Punish*, especially, have served as conceptual foundations for both theoretical and empirical studies of modern surveillance. For Foucault (1977), Jeremy Bentham's idea of the "panopticon" – a large prison architecture that allows surveillance of prisoners without being seen – serves as a metaphorical symbol for the emergence of a disciplinary society where the violence and torture of the past are replaced with soft modes of power through persistent, yet unknowable surveillance, that serve as tools of discipline and control. The linkages made by Foucault between surveillance practices and concepts like power, discipline, control, and domination have been and continue to be highly influential on theoretical and empirical conceptions of surveillance (Allmer 2011). For instance, Poster (1990:121-122) draws on Foucault to suggest that today's "circuits of communication" and the data infrastructures they produce constitute a "Superpanopticon," characterized by new, problematic forms of surveillance that alter the "microphysics of power" across society. Mann, Nolan, and Wellman (2003) also draw on Foucault to argue that modern surveillance is a manifestation of "neo-panopticons" of social control with new technologies that simultaneously enable surveillance and sousveillance. Simon (2005) aligns the work of neo-Foucauldian surveillance scholars to argue for the relevance of panopticism for gaining deeper insights into the empirical nuances of modern surveillance practices.

While the influence of Foucault on contemporary surveillance studies is undeniable, some surveillance studies scholars have expressed skepticism regarding the continued relevance of Foucault's concepts and suggested that theoretical and empirical understandings of modern surveillance ought to move beyond panoptic framings. For instance, Lyon (1992:170) argues that the idea of the panopticon can be "very limited and misleading as a descriptive or explanatory concept" and largely fails to account for the varied contexts and networked nature of modern surveillance practices. In agreement, Haggerty (2006:27) states, "Foucault continues to reign supreme in surveillance studies and it is perhaps time to cut off the head of the king. The panoptic model masks as much as it reveals, foregrounding processes which are of decreasing relevance, while ignoring or slighting dynamics that fall outside of its framework." Haggerty and Ericson (2000) and Mann et al. (2003) questioned the utility of the panoptic model given the fundamental changes in the ways that societies conduct surveillance. Haggerty and Ericson (2000) draw on Deleuze and Guattari's (1987) ideas to instead propose the concept of "surveillant assemblage," which represents a shift from the panopticon model of surveillance to one that emphasizes the manipulation of immaterial data objects across digital networks rather than disciplining and controlling physical bodies in a confined space. Mann et al. (2003), in arguing for their concept of "sousveillance," view the limitations of the panoptic model as being unable to account for more non-hierarchical and decentralized forms of surveillance. Others, such as Bogard (2012), have gone further in developing models of surveillance centered on Baudrillard's (1994) idea of simulation that stands in stark contrast to the rigid materiality of the panopticon. The simulation model takes the abstraction of surveillance practices further in arguing for the dematerialization of modern (and future) surveillance into assemblages of digital technologies of prediction, profiling, and forecasting. In the words of Bogard (2012:30), simulations “are composed of digital codes and offer flexible control that can serve multiple functions, from predicting complex system behaviors to interactive and immersive training, planning and forecasting, profiling and preemptive intervention.” Thus, in such a model of surveillance, the physical and material become secondary to, and productions of, the immaterial and digital forms assembled by prediction-oriented, future-looking digital systems.

These theoretical approaches have moved surveillance studies towards models of surveillance that place greater emphasis on the immaterial and abstract elements of contemporary surveillance. While there are certainly limitations to the Foucauldian panoptic models of surveillance that have long served as foundations of theoretical work in surveillance studies, the recent turn away from the materiality of surveillance poses substantial risks on multiple levels. For instance, placing greater emphasis on abstract digital technologies, such as artificial intelligence or other algorithmic technologies, displaces attention to the role that material infrastructures play in enabling the functioning and scaling of such technologies in the context of surveillance. Further, on a more practical level, the immaterial forms of surveillance that have now become points of emphasis in some of these approaches serve as poor sites of empirical inquiry and targeted resistance, given their abstract, black-boxed, and invisible nature. In the next section, I briefly review theoretical perspectives of infrastructure and revisit the concept’s historical usage in the literature.

THEORETICAL APPROACHES TO INFRASTRUCTURES

Early use of "infrastructure" in the digital context can be traced back to early work in social studies of computing by Kling, Scacchi, and Jewett, where it was used to broadly refer to "those resources which help support the provision of a given service or product" (Kling and Scacchi 1982:7). Their conceptualization of digital infrastructure was an expansive rhetorical tool that placed the relational aspects of computing on the same level as computer hardware and equipment. These scholars were thus interested in exploring ways of understanding digital infrastructure as *social action*, viewing digital technology and systems not as something that emerges spontaneously without reason but instead as something inherently *social* in its inception and its usage (Lee and Schmidt 2017).

The term "infrastructure" generally evokes images of the collective equipment necessary for human activities and practices, such as buildings, bridges, railroad tracks, and communications networks (Bowker et al. 2009; Edwards et al. 2009). Thus, infrastructure typically exists in the background of other human activities; it is invisible and frequently taken for granted (Star 1999; Star and Ruhleder 1994). Concerning the added "digital" element used here, digital infrastructures refer loosely to situated socio-technical systems designed and configured to support digital activities and practices (Parks and Starosielski 2015). The broad subfield of "infrastructure studies" has seen the development of two major approaches to theorizing infrastructure: the "relationalists" and the "new materialists." Below, I briefly describe these two approaches and their contributions to the study of digital infrastructures.

The first approach, known as the "relationalists," is most associated with the work of three STS scholars: Geoffrey Bowker, Susan Leigh Star, and Paul Edwards. This approach stipulates that infrastructure is relative or "relational" and context-specific. Here, the focus of infrastructure studies should be on those left out, harmed, forgotten, unserved, and how research might rectify their situations (Sandvig 2013). This group of scholars thus hold that infrastructure is "fundamentally and always a *relation*, never a thing" (Star and Ruhleder 1994). While many digital infrastructures seem to "magically" function, relationalists suggest that an enormous amount of invisible work occurs behind the scenes to make it possible. Indeed, an essential element of digital infrastructure is its relationship with what Lee et al. (2006) refer to as "human infrastructure." The focus on the human component of digital infrastructure allows for greater attention and awareness of how it is used for different purposes and operates in specific social contexts. As Edwards (2003:187) points out, "Given the heterogeneous character of systems and institutions referenced by them, perhaps 'infrastructure' is best defined negatively, as those systems without which contemporary societies cannot function." For relationalists, this means that "there is no particular point in the sequence of infrastructure where things stop being social and become purely technical (or vice–versa), or where infrastructure itself stops—any thing that one points to has 'subordinate parts' (therefore, it has an infrastructure), and this infrastructure must also have an infrastructure, and so on" (Sandvig 2013:93). In the context of digital infrastructures, this means shifting attention away from these objects' materiality towards the social processes and structures that they are embedded within.

The second approach, known as the "new materialists," often refers to scholars in media studies and communication, including Jonathan Sterne and Lisa Parks. The study of infrastructure for the new materialists attempts to ground earlier cultural studies, focusing further attention on the materiality of infrastructures: roads, power systems, wires, signals, and dirt. While the relationalists, coming from the traditions of STS, tended to start with technology and then take a turn towards the idea that these technologies are social (or cultural, or economic), the new materialists are making the opposite turn, going from socio-cultural analyses to an analysis that leads an emphasis on the materiality of these infrastructures (Sandvig 2013). Parks (2015:356) thus calls on the humanities to investigate the physical infrastructures – the "stuff you can kick" – to "foster infrastructural intelligibility by breaking infrastructures down into discrete parts and framing them as objects of curiosity, investigation, and/or concern." For the new materialists, this means visiting infrastructural sites and objects, witnessing the infrastructural construction processes, and getting as close as possible to the physical structures themselves. In Parks and Starosielski's (2015) *Signal Traffic*, for example, they conduct critical studies of sites of digital infrastructure, including cybercafés in Turkey, mobile-telephone towers in the Middle East, and undersea cables in the Pacific. Like the relationalists, the new materialists take a critical approach to studying digital infrastructures by locating these material objects within systems of power and social hierarchies.

While both approaches offer utility for understanding infrastructures, this paper draws upon the materialist approach to infrastructure to ground its analyses of modern surveillance practices. The materialist approach helps ground the study of surveillance practices in their physical realities. Specifically, these approaches will provide a lens to examine the materiality of surveillance organizations and infrastructure. In the context of surveillance, the material relationship between surveillance organizations and infrastructure is essential to understanding modern surveillance practices. As previously discussed, infrastructures have provided the physical mechanisms needed to scale data collection, analysis, and storage for surveillance purposes on a massive scale. Such digital infrastructures are intimately connected to the thousands of organizations engaged in surveillance operations in the US. Of course, it is no coincidence that surveillance organizations are the same entities often tasked with developing and maintaining such infrastructures while simultaneously working to exploit them for their surveillance and (in the case of private organizations) profit-related motives. This kind of materialist turn was not isolated to infrastructures studies, however. In the next section, I briefly overview theoretical approaches to materiality in the subfield of organization studies.

MATERIALITY IN ORGANIZATIONAL CONTEXTS

Since Orlikowski's (2007) canonical essay on materiality in the organizational context, considerable work in organization studies has explored the critical role materiality plays in organizational structure and processes (Cooren 2020). As Fox and Alldred (2015) point out, there has been a long materialist thread throughout the history of social science inquiry, especially as it relates to Marxist and structuralist sociology. Nonetheless, recent work emphasizing materiality under the broad umbrella of "new materialism" has emerged in reaction to humanistic approaches to social science. While early forms of materialism were heavily criticized for being deterministic and reductionist in their reliance upon macro structures and super-structures, these new materialist ontologies view materiality in a "relational, emergent sense" (Coole and Frost 2010:27-28). Perhaps unsurprisingly, this conceptualization of materiality overlaps heavily with the approach of the relationalists in infrastructure studies discussed previously, and scholars from both groups borrow ideas from many of the same authors (Barad 2003; Deleuze and Guattari 1987; Latour 2005). In organization studies, however, this new materialist movement has often been contrasted with work towards the end of the 1990s and early 2000s heavily influenced by Foucault that focused on the discursive elements of organizations (Cooren 2020). Here, the work of the new materialists in organization studies was seen by some scholars as bringing greater attention to the material elements of organizations they felt were left out by Foucauldian analyses. However, some such as Hardy and Thomas (2015) have argued against the notion that discursive analyses fail to address organizations' materiality.

Materialist approaches to organizations have grappled with the same ontological questions and challenges that social science and STS scholars in other domains, including infrastructure studies, have faced. Like infrastructures (and arguably everything in existence), organizational contexts are characterized by both social and material elements. Instead of treating the social and the material as separate, independent spheres of organizational life, materialist organizational scholars have come to see these entities as closely intertwined with one another. For example, rather than frame organizational practices as "social practices" and risk reinforcing the idea that the material is not intrinsic to organizing, Orlikowski (2007:1438) proposes instead using the concept of "sociomaterial" borrowed from Mol (2003) and Suchman (2007) to denote the "constitutive entanglement of the social and the material in everyday organizational life." Such an approach thus emphasizes that "every organizational practice is always bound with materiality" and "is not an incidental or intermittent aspect of organizational life; it is integral to it" (Orlikowski 2007:1436). Organizational scholars utilizing such an approach are attempting to "reconsider the relationship between social and material considerations in the emergence and evolution of organizational practice, bringing back into focus the material specificities of physical and technological arrangements" (Mazmanian, Cohn, and

Dourish 2014). For instance, Scott and Orlikowski (2014) explore the entanglement of social meaning and materiality in the practice of anonymous evaluation and ranking in the hospitality industry using social media. Mazmanian et al. (2014) also employ this approach to understand the dynamics and mutual constituency of social and material technological arrangements in the NASA organizational context. Both studies evidence the importance of acknowledging the entanglement between the material and the social in organizational contexts, especially regarding the role of information technologies. This paper draws on these ideas to inform its analyses in the context of surveillance organizations and infrastructures.

ASSESSING THE MATERIALITY OF MODERN SURVEILLANCE

To explore the materiality of modern surveillance practices, this analysis first relies on open sources of data to map contemporary surveillance organizations and infrastructure. The first data source comes from the ICWatch database, containing data on over 31,000 surveillance organizations (Burke 2020; Transparency Toolkit n.d.). These data were used to produce the locations of surveillance organizations on the maps in Figures 4.1 and 4.2. It is worth pointing out that these data include a particular group of surveillance organizations that have taken part in the US government surveillance programs listed in the Snowden documents. Surveillance organizations from both the public and private sectors are thus included in these data, with nearly every industry and sector of the US economy represented to varying degrees (Burke 2020).

While this open-source database is currently the largest of its kind, it is by no means exhaustive, and it does exclude some organizations engaged or involved in surveillance practices to varying degrees. For instance, private organizations engaging in such practices outside the confines of the US government surveillance programs listed in the Snowden documents may not be included in these data. Among the surveillance organizations potentially excluded from these data are powerful technology companies whose profit model centers around mass data collection and, more broadly, any private entities that provide surveillance-related services and hardware that are not explicitly tied to specific US government surveillance programs (i.e., a company that manufactures and sells surveillance software or hardware to US law enforcement and security agencies for general usage). Despite such limitations, these data represent the best publicly available source of information on surveillance organizations and provide unprecedented insight into the network of organizations involved in US surveillance programs.

Like the data used to examine surveillance organizations, the data on surveillance infrastructures have been collected from robust publicly available data sources: the US Department Homeland Security (2021) fusion center database and Telegeography's (2021) undersea internet cable mapping data. These geographical infrastructure data were combined with the geographical data on surveillance organizations from the ICWatch database to create visual maps using Tableau software. The maps produced from these data (Figures 4.1 and 4.2) allow for further descriptive analyses of the physical arrangement of surveillance infrastructures in relation to the geographical location of surveillance organizations.

The relationship between surveillance infrastructures and organizations is complex and unpredictable. The rapid pace with which digital surveillance infrastructures have developed is perhaps only surpassed by the incredible ascent of surveillance organizations' power. It is thus impossible to understand the landscape of modern surveillance without disentangling the material interconnections between these two elements. Below, I examine two broad examples that evidence such materiality and their importance for understanding modern surveillance practices: 1) the geographies and physical arrangement of surveillance infrastructures and organizations and 2) the material reality and consequences of contemporary surveillance capitalism.

GEOGRAPHIES OF SURVEILLANCE ORGANIZATIONS AND INFRASTRUCTURES

In this section, I map the physical arrangements of surveillance organizations and infrastructures in relation to one another to illustrate the materiality of contemporary surveillance. As previously discussed, modern surveillance practices are almost entirely centered around monitoring and collecting digital communications data. Despite the abstract nature of surveillance data and some of the technologies used to collect and analyze them, surveillance practices are still reliant on material infrastructures to function. These physical infrastructures thus serve as bridges between the extensive network of digital technologies. If the dematerialization of contemporary surveillance were to occur as theorized by some surveillance scholars, the physical arrangement of surveillance organizations and infrastructures would be expected to diverge from one another. In other words, the mapping of surveillance infrastructures and organizations would be void of any clear relationship to one another. As previously noted, despite the black-boxed nature of modern surveillance, I contend that the physical realities of this network of organizations and infrastructure still play a significant role. To this end, the exercise of mapping these geographical arrangements presents a unique opportunity to illustrate that surveillance organizations and infrastructures remain tied to one another in material ways.

While the growth of Big Data technologies – software, algorithms, code, and cloud computing – have certainly played a significant role in allowing for and perpetuating modern surveillance practices, they would not exist in their current forms without the simultaneous advancements and growth when it comes to digital infrastructures. For instance, the mass collection of nearly five billion cell phone records by the NSA each day is only possible thanks to recent advancements in fiber optics and data storage technologies (Greenwald 2014). Borrowing a phrase from the late US Senator Ted Stevens, the Internet is quite literally "a series of tubes," with a complex set of infrastructure providing the physical connections that integrate and fuel modern digital life. In the decades since the first transatlantic fiber-optic telephone line was laid on the ocean floor in 1988, the number of such cables has multiplied and spread alongside demands for more extensive and faster connections. As of 2015, there were 343 cables active or under construction, totaling over half a million miles across every ocean and connecting every continent except Antarctica (Sohn 2015). The locations where these cables intersect, known as "chokepoints," have become primary spots for the NSA to tap into massive amounts of digital data from around the globe as they pass through the cables. Despite their importance for the functioning of modern life, like many infrastructures, these cables are largely invisible to the public. To this end, recent work by scholars and academics alike has attempted to bring greater visibility to these surveillance infrastructures. One notable example is the work of artist Trevor Paglen, which has brought considerable attention to the materiality of surveillance infrastructures. Paglen's impressive photography of surveillance sites, such as underwater cables and NSA bases, has brought greater visibility to previously-invisible infrastructures and physical locations of surveillance (Jobey 2015).

Figure 4.1 maps the geographical arrangement of surveillance organizations using data from the ICWatch database and undersea cable landing points from Telegeography's (2021) open database. Here, red circles represent private surveillance organizations, and blue circles represent governmental surveillance organizations. The empty black circles along the coastal areas of the US represent cable landing points, and the colorful lines that trail behind them represent the underwater path of such cables. As the map indicates, the physical arrangement of many of the undersea cable landing points aligns with the presence of clusters of surveillance organizations. As previously discussed, nearly all internet traffic travels through these cables and, consequently, through the US. The predominance and interconnectivity of such digital infrastructure in the US have made mass surveillance feasible and scalable with minimal effort; for instance, research by Andrew Clement (2014) on internet traffic routes found that the US government, specifically the NSA, could intercept and collect 99% of internet traffic by tapping only a small number of locations in the US. Of course, the tapping of these fiber-optic cables by US government intelligence agencies has been made possible in large part thanks to partnerships with private internet service providers, such as AT&T, who provided not only access to such data cables but also hardware and equipment to make the transfer and storage of it more efficient (Cayford, Van Gulijk, and van Gelder 2014). The physical ties between surveillance organizations and these infrastructures evidence the significance of the material relations for producing and enabling modern surveillance practices.

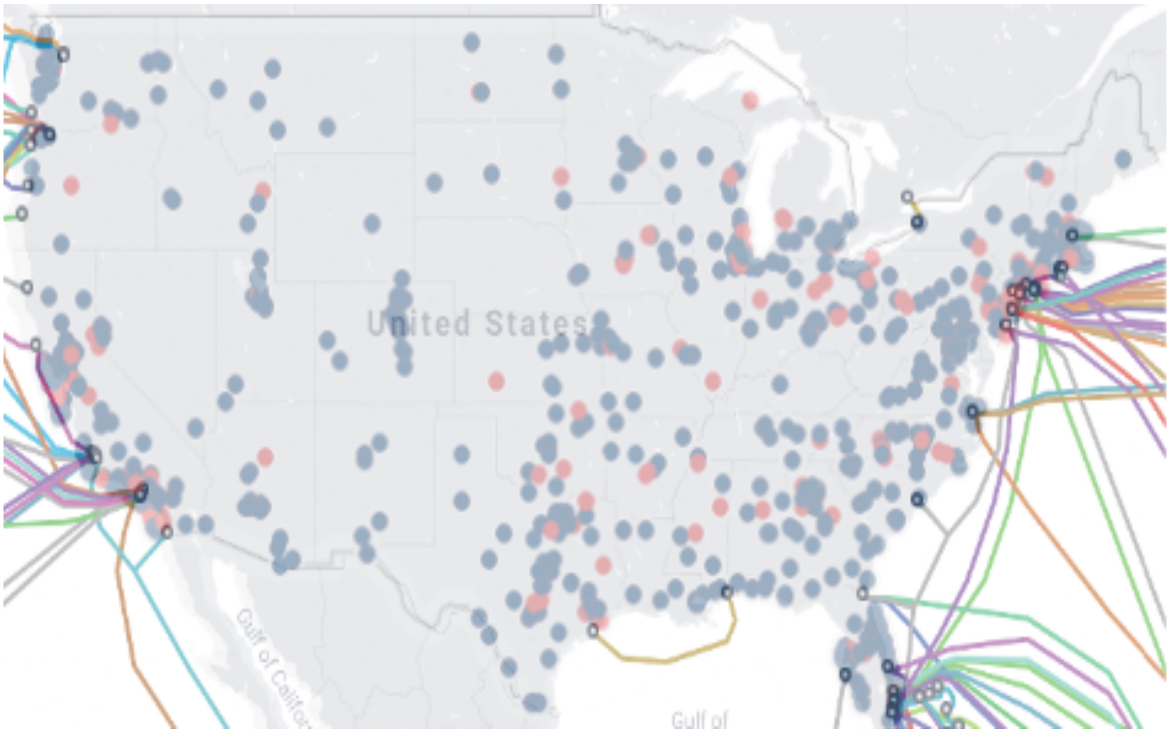

Figure 4.1: Map of Surveillance Organizations and Undersea Internet Cables To/From the United States.

The scaling of surveillance practices and, as illustrated above, the actors involved in such practices have required considerable investment in growing the physical structures needed to support them. US intelligence-gathering efforts are estimated to total over $70 billion each year (Federation of American Scientists 2014). In addition to the existing internet infrastructure, the massive effort (and capital) for modern surveillance operations has led to investments in developing physical structures whose sole purpose is to store and analyze data gathered for surveillance purposes. Some of these infrastructure sites, known as "fusion centers," were created to prioritize mass data collection, analysis, and sharing among government and private entities. As of 2010, at least 72 fusion centers were operating across the continental US (Monahan 2010). Fusion centers have become representative of modern surveillance's seemingly never-ending reach, moving from government records and private data brokers to the integration of "old" surveillance systems like closed-circuit TV cameras and license plate readers, and more recently, to the whole-sale data mining of social media and other forms of digital intelligence (McQuade 2019). Fusion centers are therefore essential objects of study that represent the ongoing materiality of surveillance despite the immaterial and digital nature of some contemporary surveillance practices and technologies.

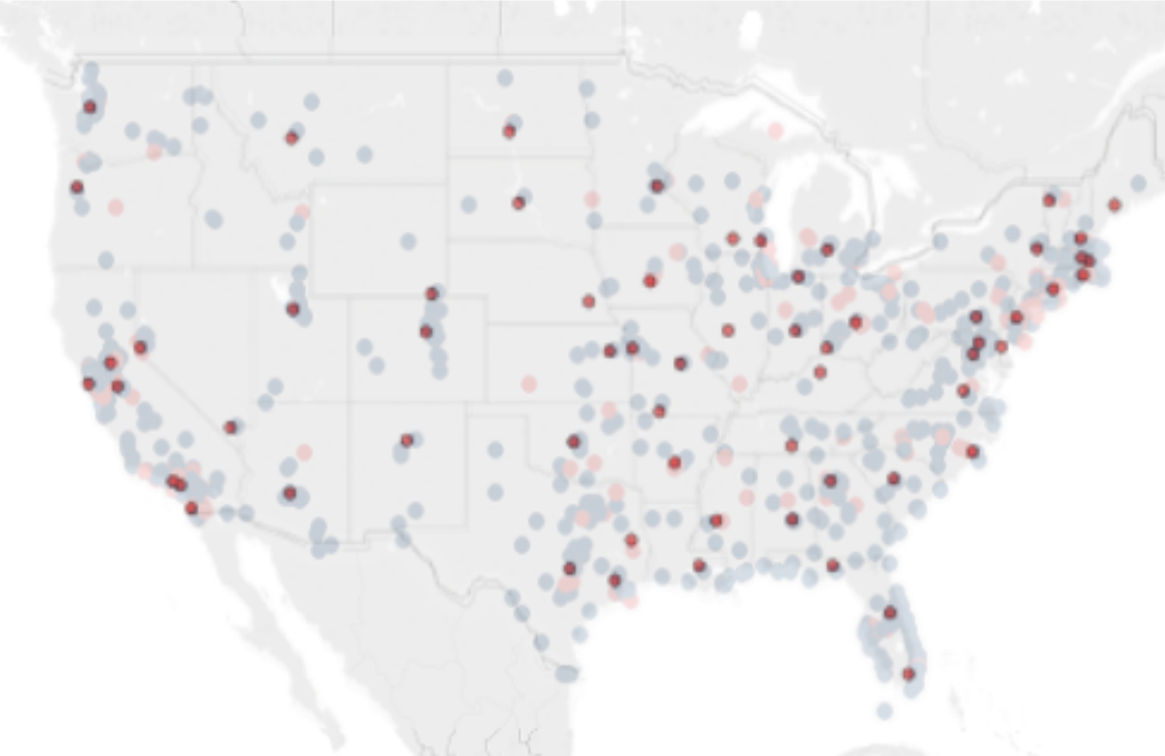

Figure 4.2: Map of Surveillance Organizations and Fusion Centers in the United States.

Figure 4.2, above, depicts the locations of fusion centers across the US. Once again, the locations of fusion centers were derived from publicly-available data from the Department of Homeland Security website (Department of Homeland Security 2021). Again, the light red circles on the map represent private surveillance organizations, and blue circles represent governmental surveillance organizations. The darker red circles on the map represent fusion centers. As noted above, fusion centers were created to conduct mass data collection, analysis, and intelligence-sharing between government and private entities. As with the map of surveillance organizations and undersea internet cables (Figure 4.1), fusion centers are scattered throughout the continental United States. A close examination of Figure 4.2 suggests, once again, that there is considerable overlap in the geographical arrangements of surveillance organizations and fusion centers. This is especially the case when examining the larger clusters of surveillance organizations in relation to the locations of fusion centers across the country. This map provides visual evidence of the geographical ties between surveillance organizations and infrastructures.

In sum, the exercise of mapping the geographies of these surveillance infrastructures in relation to those of surveillance organizations helps shed light on the material nature of surveillance and the linkages between these two crucial elements of modern surveillance. Despite the dematerialization of some aspects of contemporary surveillance practices and technologies, these maps provide descriptive visual evidence that the material relations between these two entities may remain an essential consideration for understanding modern surveillance. While these examples may not be enough to say definitively whether the geographical locations and physical arrangement of surveillance infrastructure and organizations are tied to one another, the geographical evidence serves as helpful starting points for tracing the material relations that underly modern surveillance practices.

THE MATERIAL REALITY AND CONSEQUENCES OF MODERN SURVEILLANCE (CAPITALISM)

Modern surveillance infrastructure is not simply confined to fusion centers. Private organizations have intensified their efforts to collect personal data and information on individuals in their capitalistic pursuit of profit. The growth of what Zuboff (2019) terms “surveillance capitalism,” a new economic logic and mutation of capitalism centered around the commodification of human behavior and data, has accelerated the rapid development of digital infrastructure used for surveillance purposes. Though their motivations may differ, mass data collection is at the intersection of the interests of both government and private surveillance organizations. Private corporations exploit mass surveillance to maximize profits through targeted advertisements and behavior manipulation, while governmental actors (presumably) do so to fulfill their national security agenda. Today, users are offered essential digital services for free, and then the data they produce is then monetized. Such practices are made possible due to the ongoing scaling of data infrastructure, especially around cloud storage and computing.

The largest market shares in the cloud data storage industry are held by three primary US-based services: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud. These digital data storage infrastructures have created the capacity needed to expand the reach and power of surveillance actors operating in both the government and private sectors (Landwehr, Borning, and Wulf 2021). Private companies are not alone when it comes to data storage centers, however, as the US government is building massive data centers of its own. In 2014, the NSA spent $1.7 billion to build a new data center in Utah. This data center is huge, spanning 1 million square feet (approximately 17 football fields), consuming 65 megawatts of power, and storing 20 terabytes of data per minute (Carroll 2013). Despite perceptions of “the cloud” and the various algorithmic technologies that rely upon it as an immaterial and abstract form of data storage and computing power, the material realities of such infrastructures and the organizations utilizing them are far from it.

The development of surveillance technologies and the infrastructure required to maintain them pose serious material consequences. One major consequence that is often overlooked in the surveillance studies literature are the material environmental implications of surveillance capitalism. The growing usage of digital data and technologies in the US has necessitated considerable investment in infrastructure to maintain such growth. Today, four of five of the world's largest data centers are located in the US (Forbes 2012). As indicated above, these data centers consume massive amounts of electricity and are, as a result, amongst the largest consumers of fossil fuels. As of 2020, it is estimated that data centers represent about 1% of global energy consumption, equivalent to the annual electricity usage of 20 million US homes (Masanet et al. 2020). Most data centers also require large, continuous supplies of water for their cooling systems, utilizing an increasingly precarious resource (Mosco 2017). Energy consumption for cloud storage pales in comparison to that of cloud computing, where some estimates put consumption above that of entire populous nation-states (Brevini 2020). Perhaps unsurprisingly, environmental regulations and laws in the US are currently ill-equipped to address such emissions (Story 2014). The entanglement between capitalistic economic logic and surveillance means that such practices embody and share the same sociomaterial realities.

While emerging and recently developed digital technologies may have created new, abstract modes of surveillance, to detach such elements from the materiality of surveillance risks overlooking crucial material aspects of this assemblage and, perhaps more importantly, its material consequences. Here, examining the sociomateriality of surveillance means linking the driving forces of capitalistic accumulation with the material infrastructures that emerged from them. Doing so illustrates how such materiality has shaped modern surveillance practices in ways that pose serious social, political, economic, and environmental implications. This is not to say that the abstract and material elements of surveillance should be ignored or detached from theoretical and empirical studies of surveillance altogether, however. Instead, this exercise of examining the materiality of contemporary surveillance serves as a reminder to surveillance scholars of the significance of the material realities of such practices and the material consequences they may produce. As shown here, the material consequences and implications of modern surveillance practices, especially those intertwined with capitalistic modes of accumulation and exploitation, should warrant greater attention to the materiality of surveillance.

DISCUSSION

The materiality of organizations and infrastructure has long been a topic of social science inquiry across various contexts (Bowker and Star 2000; Cooren 2020; Edwards 1997; Hughes 1993; Latour 1996; Schiller 2006; Schüll 2012; Scott and Orlikowski 2014). In the context of surveillance, the rapid development of digital technologies developed or co-opted for surveillance purposes has led some surveillance studies scholars to move towards models of surveillance that emphasize the role of more abstract, immaterial elements of contemporary surveillance practices (Bogard 2012). Drawing on materialist approaches to infrastructures (Parks 2015; Star 1999; Sterne 2013) and organizations (Orlikowski 2007), this paper examined the materiality of surveillance infrastructures and organizations to evidence the need for continued attention and emphasis on the material realities of contemporary surveillance.

To this end, this paper employed an analysis of two broad illustrations to assess such materiality and their importance for understanding modern surveillance practices in the US: 1) the geographies and physical arrangement of surveillance infrastructures and organizations and 2) material reality and consequences of modern surveillance. The first section of this analysis provided descriptive mappings of surveillance organizations and infrastructures, finding that the physical arrangement of these two crucial elements of surveillance appeared to be closely correlated. While some have theorized contemporary surveillance as becoming more abstract and immaterial, such material relations evidence the continuity among ongoing co-dependencies between surveillance actors and infrastructures. These maps also serve as sites of sousveillance by rendering these surveillance actors and infrastructures visible. Though unlikely to dismantle the surveillance apparatus, such contributions may contribute to broader public awareness that can disrupt traditional power relations of surveillance (Burke 2020; Mann et al. 2003).

The second section of the analysis draws on Zuboff's (2019) notion of surveillance capitalism to trace the materiality of surveillance in relation to capitalist logics and the emergence of new digital infrastructures. Through a discussion of the material realities and consequences of modern surveillance, the capitalistic logic of accumulation that has become intertwined with modern surveillance practices necessitate greater consideration and attention to the material elements and consequences of contemporary surveillance. In particular, the expansion of digital (surveillance) infrastructures and the resulting patterns of consumption and accumulation poses profound social, political, economic, and environmental implications. Theoretical approaches to surveillance that ignore or downplay the sociomaterial elements of surveillance risk also overlooking the material consequences of modern surveillance practices. The perception that surveillance technologies and digital technologies, in general, have become more immaterial and abstract only serves to reify existing power structures and further obfuscate harmful surveillance practices and the actors involved in carrying them out. It is thus crucial that surveillance scholars push back against such conceptualizations and fully consider the materiality of modern surveillance along with the material consequences of surveillance practices that have become entangled with capitalistic modes of power and accumulation in complex and problematic ways.

CHAPTER 5: CONCLUSION

Though often associated with today's institutions and widespread digital technologies, surveillance long pre-dates its modern conception. Early forms of surveillance, such as eavesdropping and the interception of physical communications, have been used for centuries (Locke 2010). Nonetheless, as exemplified by this dissertation research, modern forms of surveillance have transformed immensely from their earlier predecessors in terms of their nature, impact, and complexity. The rapid development of digital technologies, corporate and governmental infrastructures, and global interconnectivity has produced major societal shifts in power, identity, institutional practices, and interpersonal relations that have positioned surveillance as the dominant organizing practice of modernity (Lyon et al. 2012). In today's world, it can be challenging to identify a single aspect of social life that remains untouched by surveillance. Surveillance has become a part of the workplace (Ball 2009), global citizens are subject to mass surveillance programs (Bamford 2009; Greenwald 2014; Maass and Poitras 2014), schools are monitoring their students' social media activity (Burke and Bloss 2020), and even local law enforcement agencies in the US have shifted towards using mass surveillance and big data technologies for policing (Brayne 2017). Further, large corporations have also embraced surveillance as a capitalistic mode of operation, gathering massive amounts of behavioral, communications, and biometric data about consumers to pursue greater profits and power (Gates 2011; Zuboff 2019). As this dissertation research has shown, surveillance has expanded well beyond the confines of the national security and defense apparatuses to become an essential element of modern social life.

Alongside the expansion of modern surveillance practices, academic inquiry into such practices has also grown considerably in recent years. The emergence and growth of the surveillance studies subfield have produced an incredible multidisciplinary community of scholars and, along with it, considerable contributions to academic and public knowledge around these practices. As pointed out throughout this dissertation, the stakes of this research are incredibly high. The power structures embedded within and reified by modes of surveillance, regardless of who carries out such surveillance, pose serious implications for the social, political, economic, and environmental conditions of modern life. This chapter will thus conclude the dissertation by first summarizing the key high-level findings of each of the previous chapters. Next, I outline the broad academic contributions and societal implications of this research. I then conclude by discussing some of the limitations of this work and future directions for research in this area.

KEY FINDINGS

Overall, the findings of the dissertation provide insights into the nature and quality of modern surveillance on multiple levels. Chapter 2 of this dissertation demonstrated the digital sousveillance approach using network analytic methodologies. The analysis closely examined the structure of the network of public and private surveillance organizations from the 1970s to the 2000s. The results of these analyses indicated that surveillance has become increasingly privatized over this time span, as private organizations are, at an increasing rate, partnering with the US government to engage in mass surveillance. Further, such analyses demonstrated the utility of a digital sousveillance approach to conducting surveillance research through the co-optation of digital technologies typically used for surveillance to instead bring greater visibility and transparency to surveillance practices.

Chapter 3 of the dissertation built upon the methodologies and findings of Chapter 2 to further examine the network of surveillance organizations and, more specifically, the relationship between organizations' embeddedness within this network and economic outcomes. The results of these analyses suggest that while there is a strong relationship between surveillance organizations' embeddedness and economic capital as predicted, the directionality and degree of this relationship were conditional on organization type, ownership type, and industry. For instance, surveillance organizations falling under the local government, manufacturer of goods, private university, and public university typologies had stronger positive relationships between embeddedness and economic capital. Also, surveillance organizations that were US-owned, female-owned, and foreign-owned but located in the US had stronger positive relationships between embeddedness and economic capital than other ownership types. Such results indicate that organizational and institutional characteristics may play an important role in mediating the relationship between organizations' structural position and economic outcomes.

Chapter 4 grounds the earlier empirical analyses in a descriptive examination of the materiality of modern surveillance. The results of these analyses indicate that despite the theoretical turn in surveillance studies towards a focus on the abstract and immaterial elements of modern surveillance, the material relations underlying contemporary surveillance practices remain crucial to understanding such practices. By mapping the geographical arrangement of surveillance organizations and infrastructures, it was found that both entities remain closely tied to one another in material ways. The analyses of surveillance capitalism indicate the need for greater consideration of the material consequences of such practices, which I argue is best achieved through approaches to surveillance that focus more critical attention on the material elements of modern surveillance. In the following sections, I discuss the broad academic and societal significance of this dissertation research.

ACADEMIC CONTRIBUTIONS

This dissertation research builds on past social science research to contribute significantly to the academic disciplines and subdisciplines of sociology, surveillance studies, STS, and the broader public subject to modern surveillance practices. More specifically, this dissertation contributes to sociological studies of organizations, social networks, and science and technology. Chapter 2 contributes to the literature on organizational networks, with unique, longitudinal insights into the structure and nature of a large network of organizations. Also, Chapter 3 closely examines the relationship between organizations' network position and economic outcomes. This is notable as sociology has long been interested in how social structure impacts the distribution and obtainment of economic capital, especially in the organizational context (Granovetter 1985). This research adds to this literature by investigating how this relationship is conditional on specific organizational and institutional characteristics, bringing additional nuance and empirical support to long-standing theories in this area.

Chapters 2 and 3 also contribute to the study of social networks and organizational networks, specifically. The application of network methodologies to the study of surveillance is novel and, to my knowledge, has not yet been done within surveillance studies. Such approaches also align with the direction of recent theoretical work in surveillance studies that view surveillance as being made up of heterogeneous actors (Berndtsson and Stern 2011; Haggerty and Ericson 2000). Lastly, Chapter 4 contributes to the sociological study of science and technology by bringing together research in the organization studies and STS to examine the materiality of contemporary surveillance. This contribution is significant because surveillance research often focuses on either the relational or material aspects of contemporary surveillance practices, and rarely both. Chapter 4 also makes an important theoretical contribution to surveillance studies in highlighting the importance of materiality for conceptualizations of surveillance. This stands in contrast to the growing body of theoretical work in surveillance studies that places emphasis on immaterial and abstract elements of surveillance practices.

In alignment with growing calls for open forms of science more broadly, the use of digital data and computational methodologies in the social sciences (and especially surveillance studies) should come with transparency and accountability of its own. The extensive use of open sources of data in this research can serve as an example of the empirical utility of using sources and methods that are conducive to greater transparency and reproducibility. Further, more transparent science in the context of surveillance and other social science subfields may open up new doors for knowledge exchange and collaborations with important public stakeholders, including citizens, activists, and non-profit organizations. Digital sousveillance, as a methodological approach to studying surveillance, also aligns with such aspirations and could enable more transparent and reproducible surveillance research.

BROADER SOCIETAL SIGNIFICANCE

Among the most significant underlying motivations for surveillance studies as a transdisciplinary field of study is to go beyond conceptualizing and understanding surveillance at an academic level to inform and enable the mobilization of resistance to such practices more broadly. Because contemporary surveillance practices pose significant and pressing repercussions for society, especially as it relates to existing power structures, civil liberties, democracy, and inequality, the decision to undertake research in this area necessitates a critical awareness of the broader implications it may pose.

As previously noted, the underlying approach to this research, digital sousveillance, enables a critical methodological examination of surveillance practices and places the researcher in a position to resist and counteract the power hierarchies that such practices embody through the production of knowledge and making such practices, as well as the powerful actors engaging in them, more visible. Given the lengths that surveillance actors will go to remain hidden from the public eye, research that works to bring transparency to such actors and their practices can serve as influential acts alone and even bring about meaningful social and political change. The simple act of mapping can lead to a greater number of academic and public inquiries into the actors involved and potentially produce mechanisms of accountability for their actions. This is especially true in regard to policy, as legislation aimed at regulation of potentially problematic surveillance practices faces the challenge of identifying the actors involved and disentangling the black box of surveillance practices and technologies. To this end, this research contributes to the foundations of knowledge around surveillance actors and their practices. To my knowledge, this work is the first to meaningfully quantify the scale of the surveillance organizational network over the span of decades and in its more modern form. In an area of research as heavily guarded and secretive as surveillance, this kind of work can serve as crucial building blocks towards more knowledge, awareness, and accountability for surveillance actors.

LIMITATIONS

It is important to also briefly acknowledge some of the limitations of this research in terms of the data, methodologies, and generalizability of the findings. The main source of data for this study came from the ICWatch database originally developed by Transparency Toolkit. For reasons unknown, these data in their original form are now being hosted on WikiLeaks. As noted in Chapters 2 and 3, these data include over 31,000 organizations involved in surveillance programs. However, this is by no means an exhaustive dataset of all organizations involved in surveillance practices. Some types of surveillance organizations are likely to have been excluded from these data, including any organization engaging in surveillance outside of the confines of US government surveillance programs. Because these data were collected from LinkedIn, there is likely bias towards particular kinds of individuals who are more likely to have a social media presence. This bias is somewhat evident in the smaller data and sample sizes for earlier time periods compared to recent years. Further, this research examines surveillance in the US and these data are limited in scope to the US context. Thus, the results and findings from this research are not necessarily generalizable to surveillance in other global contexts. Because the surveillance apparatus in the US is, in some ways, unique in quantitative and qualitative ways caution should be exercised in broadly extrapolating this research to assemblages of surveillance organizations outside of the US.

FUTURE DIRECTIONS

Future research can build on the methodologies and findings of this dissertation research. Going forward, work in surveillance studies can employ digital sousveillance as an approach to studying surveillance. With the growth of digital data more generally, there is increasing opportunity to develop and analyze new sources of data relevant to the study of surveillance in various contexts. The dataset used in this research, originally derived from the ICWatch database, may serve as a useful starting point for surveillance scholars interested in such an approach. Although the surveillance studies subfield has traditionally leaned towards more qualitative methods, the growing accessibility of quantitative and computational methods to scholars in the social sciences and humanities may open new lines of inquiry as such methodologies become more common within these disciplines. As illustrated in Chapter 3, these data can serve as the foundation for a more robust dataset pertaining to surveillance organizations when combined with other open sources of data. In sociology, the findings and contributions of Chapter 3 serve as starting points for new lines of inquiry into the long-studied relationship between organizational embeddedness and economic outcomes. The conditionality of this relationship has been seldom explored and introduces the potential for future research to examine the complexities and dynamics of this relationship further. Lastly, the emergence of surveillance capitalism and the expansion of modern surveillance into nearly every sphere of our daily lives poses serious implications for the future of society on multiple fronts. More work is needed to continue to build on the foundations of this work and ensure the continued growth of knowledge, transparency, accessibility, and accountability around modern surveillance.

REFERENCES

Abrahamsen, Rita, and Michael C. Williams. 2009. "Security Beyond the State: Global Security Assemblages in International Politics." *International Political Sociology* 3(1):1–17.

Allmer, Thomas. 2011. "Critical Surveillance Studies in the Information Society." *TripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society* 9(2):566–92.

Andrejevic, Mark, and Kelly Gates. 2014. "Big Data Surveillance: Introduction." *Surveillance & Society* 12(2):185–96.

Ball, Kirstie. 2009. "Exposure: Exploring the Subject of Surveillance." *Information, Communication & Society* 12(5):639–57.

Ball, Kirstie, Ana Isabel Canhoto, Elizabeth Daniel, Sally Dibb, Maureen Meadows, and Keith Spiller. 2015. *The Private Security State?: Surveillance, Consumer Data and the War on Terror*. CBS Press.

Bamford, James. 2009. *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*. Anchor.

Barad, Karen. 2003. "Posthumanist Performativity: Toward An Understanding Of How Matter Comes To Matter." *Signs* 28:801–31.

Barnes-Mauthe, Michele, Steven Allen Gray, Shawn Arita, John Lynham, and PingSun Leung. 2015. "What Determines Social Capital in a Social–Ecological System? Insights From a Network Perspective." *Environmental Management* 55(2):392–410.

Baudrillard, Jean. 1994. *Simulacra and Simulation*. University of Michigan press.

Becker, Fred, and Valerie Patterson. 2005. "Public-Private Partnerships: Balancing Financial Returns, Risks, and Roles of the Partners." *Public Performance & Management Review* 29(2):125–44. doi: 10.1080/15309576.2005.11051866.

Berndtsson, Joakim, and Maria Stern. 2011. "Private Security and the Public–Private Divide: Contested Lines of Distinction and Modes of Governance in the Stockholm-Arlanda Security Assemblage." *International Political Sociology* 5(4):408–25.

Biddle, Sam. 2017. "How Peter Thiel's Palantir Helped the NSA Spy on the Whole World." *The Intercept*. Retrieved February 2, 2019 (https://theintercept.com/2017/02/22/how-peter-thiels-palantir-helped-the-nsa-spy-on-the-whole-world/).

Bleiker, Roland. 2014. “Visual Assemblages: From Causality to Conditions of Possibility.” Pp. 75–81 in *Reassembling International Theory: Assemblage Thinking and International Relations*, edited by M. Acuto and S. Curtis. London: Palgrave Macmillan UK.

Bogard, William. 2012. “Simulation and Post-Panopticism.” Pp. 3–37 in *Routledge Handbook of Surveillance Studies*. Routledge London.

Bonacich, Phillip. 2007. “Some Unique Properties of Eigenvector Centrality.” *Social Networks* 29(4):555–64.

Bowker, Geoffrey C., Karen Baker, Florence Millerand, and David Ribes. 2009. “Toward Information Infrastructure Studies: Ways of Knowing in a Networked Environment.” Pp. 97–117 in *International Handbook of Internet Research*. Springer.

Bowker, Geoffrey C., and Susan Leigh Star. 2000. *Sorting Things Out: Classification and Its Consequences*. MIT press.

Boyd, Danah, and Kate Crawford. 2012. “Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon.” *Information, Communication & Society* 15(5):662–79.

Boyne, Roy. 2000. “Post-Panopticism.” *Economy and Society* 29(2):285–307.

Brambor, Thomas, William Roberts Clark, and Matt Golder. 2006. “Understanding Interaction Models: Improving Empirical Analyses.” *Political Analysis* 63–82.

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

Brevini, Benedetta. 2020. “Black Boxes, Not Green: Mythologizing Artificial Intelligence and Omitting the Environment.” *Big Data & Society* 7(2):2053951720935141. doi: 10.1177/2053951720935141.

Brunjes, Benjamin M., and J. Edward Kellough. 2018. “Representative Bureaucracy and Government Contracting: A Further Examination of Evidence from Federal Agencies.” *Journal of Public Administration Research and Theory* 28(4):519–34. doi: 10.1093/jopart/muy022.

Buchanan, Ian. 2015. “Assemblage Theory and Its Discontents.” *Deleuze Studies* 9(3):382–92.

Bueger, Christian. 2014. “Thinking Assemblages Methodologically: Some Rules of Thumb.” Pp. 58–66 in *Reassembling International Theory: Assemblage Thinking and International Relations*, edited by M. Acuto and S. Curtis. London: Palgrave Macmillan UK.

Burke, Colin. 2020. "Digital Sousveillance: A Network Analysis of the US Surveillant Assemblage." *Surveillance & Society* 18(1):74–89. doi: 10.24908/ss.v18i1.12714.

Burke, Colin, and Cinnamon Bloss. 2020. "Social Media Surveillance in Schools: Rethinking Public Health Interventions in the Digital Age." *Journal of Medical Internet Research* 22(11):e22612. doi: 10.2196/22612.

Burt, Ronald S. 1997. "The Contingent Value of Social Capital." *Administrative Science Quarterly* 339–65.

Carroll, Rory. 2013. "Welcome to Utah, the NSA's Desert Home for Eavesdropping on America." *The Guardian*. Retrieved February 15, 2022 (https://www.theguardian.com/world/2013/jun/14/nsa-utah-data-facility).

Cayford, M., C. Van Gulijk, and PHAJM van Gelder. 2014. "All Swept Up: An Initial Classification of NSA Surveillance Technology." *Safety and Reliability: Methodology and Applications* 643–50.

Cheney-Lippold, John. 2017. *We Are Data: Algorithms and the Making of Our Digital Selves*. NYU Press.

Clement, Andrew. 2014. "NSA Surveillance: Exploring the Geographies of Internet Interception." *IConference 2014 Proceedings*.

Collier, Stephen J., and Aihwa Ong. 2005. "Global Assemblages, Anthropological Problems." Pp. 3–21 in *Global Assemblages: Technology, Politics, and Ethics as Anthropological Problems*, edited by Stephen J. Collier and Aihwa Ong. New York: Wiley-Blackwell.

Confessore, Nicholas, and Matthew Rosenberg. 2018. "Spy Contractor's Idea Helped Cambridge Analytica Harvest Facebook Data." *The New York Times*, March 28.

Coole, Diana, and Samantha Frost. 2010. "Introducing the New Materialisms." *New Materialisms: Ontology, Agency, and Politics* 1–43.

Cooren, François. 2020. "Beyond Entanglement:(Socio-)Materiality and Organization Studies." *Organization Theory* 1(3):2631787720954444.

Crampton, Jeremy W., Susan M. Roberts, and Ate Poorthuis. 2014. "The New Political Economy of Geographical Intelligence." *Annals of the Association of American Geographers* 104(1):196–214.

Dahlström, Carl, Mihály Fazekas, and David E. Lewis. 2020. "Partisan Procurement: Contracting with the United States Federal Government, 2003–2015." *American Journal of Political Science*.

Dandeker, Christopher. 1990. *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day*. Polity.

Deleuze, Gilles, and Felix Guattari. 1987. *A Thousand Plateaus*. Minneapolis: University of Minnesota Press.

Department of Homeland Security. 2021. "Fusion Center Locations and Contact Information."

Donohue, Laura K. 2016. *The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age*. Oxford University Press.

Dreiling, Michael, and Derek Darves. 2011. "Corporate Unity in American Trade Policy: A Network Analysis of Corporate-Dyad Political Action." *American Journal of Sociology* 116(5):1514–63.

Edwards, Paul N. 1997. *The Closed World: Computers and the Politics of Discourse in Cold War America*. MIT Press.

Edwards, Paul N. 2003. "Infrastructure and Modernity: Force, Time, and Social Organization in the History Of." P. 185 in *Modernity and Technology*. Cambridge, MA: MIT Press.

Edwards, Paul N., Geoffrey C. Bowker, Steven J. Jackson, and Robin Williams. 2009. "Introduction: An Agenda for Infrastructure Studies." *Journal of the Association for Information Systems* 10(5):364–74.

Esposti, Sara Degli. 2014. "When Big Data Meets Dataveillance: The Hidden Side of Analytics." *Surveillance & Society* 12(2):209–25.

Eubanks, Virginia. 2018. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press.

Federation of American Scientists. 2014. "Intelligence Budget Data."

Fernandez, Sergio, Deanna Malatesta, and Craig R. Smith. 2013. "Race, Gender, and Government Contracting: Different Explanations or New Prospects for Theory?" *Public Administration Review* 73(1):109–20. doi: 10.1111/j.1540-6210.2012.02684.x.

Forbes. 2012. "The 5 Largest Data Centers in the World." Retrieved February 1, 2022 (https://www.forbes.com/pictures/54f4e712da47a54de8245358/the-5-largest-data-center/?sh=74db73aa4e36).

Foucault, Michel. 1977. *Discipline and Punish: The Birth of the Prison*. Vintage.

Fox, Nick J., and Pam Alldred. 2015. "New Materialist Social Inquiry: Designs, Methods and the Research-Assemblage." *International Journal of Social Research Methodology* 18(4):399–414.

Fyfe, Nicholas R., and Jon Bannister. 1996. “City Watching: Closed Circuit Television Surveillance in Public Spaces.” *Area* 28(1):37–46.

Gates, Kelly. 2011. *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. Vol. 2. NYU Press.

Giddens, Anthony. 1986. “The Nation-State and Violence.” *Capital & Class* 10(2):216–20.

Government Accountability Office. 2019. “A Snapshot: Government Wide Contracting.” Retrieved December 17, 2020 (https://www.gao.gov/assets/700/699330.pdf).

Granovetter, Mark. 1985. “Economic Action and Social Structure: The Problem of Embeddedness.” *American Journal of Sociology* 91(3):481–510.

Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*. Macmillan.

Greenwald, Glenn, and Ewen MacAskill. 2013. “NSA Prism Program Taps in to User Data of Apple, Google and Others.” *The Guardian*, June 7.

Haggerty, Kevin D. 2006. “Tear Down the Walls: On Demolishing the Panopticon.” Pp. 37–59 in *Theorizing surveillance*. Willan.

Haggerty, Kevin D., and Richard V. Ericson. 2000. “The Surveillant Assemblage.” *The British Journal of Sociology* 51(4):605–22.

Haggerty, Kevin D., and Amber Gazso. 2005. “Seeing beyond the Ruins: Surveillance as a Response to Terrorist Threats.” *The Canadian Journal of Sociology* 30(2):169–87.

Hardy, Cynthia, and Robyn Thomas. 2015. “Discourse in a Material World.” *Journal of Management Studies* 52(5):680–96.

Harris, Mark. 2017. “How Peter Thiel’s Secretive Data Company Pushed Into Policing | Backchannel.” *Wired*, August 9.

Hayes, Ben. 2012. “The Surveillance-Industrial Complex.” Pp. 167–75 in *Routledge Handbook of Surveillance Studies*, edited by Kirstie Ball, Kevin D. Haggerty, and David Lyon. Routledge.

Hier, Sean P. 2003. “Probing the Surveillant Assemblage: On the Dialectics of Surveillance Practices as Processes of Social Control.” *Surveillance & Society* 1(3):399–411.

Hughes, Thomas Parke. 1993. *Networks of Power: Electrification in Western Society, 1880-1930*. JHU Press.

Ingram, Paul, and Peter W. Roberts. 2000. “Friendships Among Competitors in the Sydney Hotel Industry.” *American Journal of Sociology* 106(2):387–423.

Introna, Lucas D., and Amy Gibbons. 2009. “Networks and Resistance: Investigating Online Advocacy Networks as a Modality for Resisting State Surveillance.” *Surveillance & Society* 6(3):233–58.

Jobey, Liz. 2015. “Trevor Paglen: What Lies Beneath.” *The Financial Times*, December, 9–11.

Kling, Rob, and Walt Scacchi. 1982. “The Web of Computing: Computer Technology as Social Organization.” *Advances in Computers* 21:1–90.

Kumaraguru, Ponnurangam, and Lome Faith Cranor. 2005. “A Survey of Westin’s Studies.” *Institute for Software Research International*.

Lakon, Cynthia M., Dionne C. Godette, and John R. Hipp. 2008. “Network-Based Approaches for Measuring Social Capital.” Pp. 63–81 in *Social Capital and Health*. Springer.

Landwehr, Marvin, Alan Borning, and Volker Wulf. 2021. “Problems With Surveillance Sapitalism and Possible Alternatives For IT Infrastructure.” *Information, Communication & Society* 1–16.

Latour, Bruno. 1996. *Aramis, or the Love of Technology*. Harvard University Press.

Latour, Bruno. 2005. *Reassembling the Social: An Introduction To Actor-Network-Theory*. Oxford University Press.

Lee, Charlotte P., Paul Dourish, and Gloria Mark. 2006. “The Human Infrastructure of Cyberinfrastructure.” Pp. 483–92 in *Proceedings of the 2006 20th Anniversary Conference on Computer Supported Cooperative Work*. ACM.

Lee, Charlotte P., and Kjeld Schmidt. 2017. “A Bridge Too Far?” *Critical Remarks on the Concept of Infrastructure’in CSCW and IS* 177–218.

Legal Information Institute. n.d. “Government Contracts.” *LII / Legal Information Institute*. Retrieved December 17, 2020 (https://www.law.cornell.edu/wex/government_contracts).

Lewis, Kevin. 2015. “Three Fallacies of Digital Footprints.” *Big Data & Society* 2.

Lindgren, Karl-Oskar. 2010. “Dyadic Regression in the Presence of Heteroscedasticity—An Assessment of Alternative Approaches.” *Social Networks* 32(4):279–89.

Lisle, Debbie. 2014. “Energizing the International.” Pp. 67–74 in *Reassembling International Theory: Assemblage Thinking and International Relations*, edited by M. Acuto and S. Curtis. London: Palgrave Macmillan UK.

Locke, John L. 2010. *Eavesdropping: An Intimate History*. OUP Oxford.

Lyon, David. 1992. "The New Surveillance: Electronic Technologies and the Maximum Security Society." *Crime, Law and Social Change* 18(1):159–75.

Lyon, David. 2001. *Surveillance Society: Monitoring Everyday Life*. McGraw-Hill Education (UK).

Lyon, David. 2014. "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique." *Big Data & Society* 1(2):1–13.

Lyon, David, Kevin D. Haggerty, and Kirstie Ball. 2012. "Introducing Surveillance Studies." *Routledge Handbook of Surveillance Studies* 1(12):1988.

Maass, Peter, and Laura Poitras. 2014. "Core Secrets: NSA Saboteurs in China and Germany." *The Intercept*. Retrieved September 22, 2018 (https://theintercept.com/2014/10/10/core-secrets/).

Mann, Steve, and Joseph Ferenbok. 2013. "New Media and the Power Politics of Sousveillance in a Surveillance-Dominated World." *Surveillance & Society* 11(1/2):18.

Mann, Steve, Jason Nolan, and Barry Wellman. 2003. "Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments." *Surveillance & Society* 1(3):331–55.

Marcus, George E., and Erkan Saka. 2006. "Assemblage." *Theory, Culture & Society* 23(2–3):101–6.

Marx, Gary T. 2015. "Surveillance Studies." *International Encyclopedia of the Social & Behavioral Sciences* 23(2):733–41.

Masanet, Eric, Arman Shehabi, Nuoa Lei, Sarah Smith, and Jonathan Koomey. 2020. "Recalibrating Global Data Center Energy-Use Estimates." *Science* 367(6481):984–86.

Matzner, Tobias. 2016. "Beyond Data as Representation: The Performativity of Big Data in Surveillance." *Surveillance & Society* 14(2):197–210.

Mazmanian, Melissa, Marisa Cohn, and Paul Dourish. 2014. "Dynamic Reconfiguration in Planetary Exploration." *Mis Quarterly* 38(3):831–48.

McQuade, Brendan. 2019. *Pacifying the Homeland: Intelligence Fusion and Mass Supervision*. Univ of California Press.

Mizruchi, Mark S., and Linda Brewster Stearns. 2001. "Getting Deals Done: The Use of Social Networks in Bank Decision-Making." *American Sociological Review* 647–71.

Mizruchi, Mark S., Linda Brewster Stearns, and Christopher Marquis. 2006. "The Conditional Nature of Embeddedness: A Study of Borrowing by Large US Firms, 1973–1994." *American Sociological Review* 71(2):310–33.

Mol, Annemarie. 2003. *The Body Multiple*. Duke University Press.

Monahan, Torin. 2010. "The Future of Security? Surveillance Operations at Homeland Security Fusion Centers." *Social Justice* 37(2/3 (120-121)):84–98.

Moore, Spencer, Eugenia Eng, and Mark Daniel. 2003. "International NGOs and the Role of Network Centrality in Humanitarian Aid Operations: A Case Study of Coordination During the 2000 Mozambique Floods." *Disasters* 27(4):305–18.

Mosco, Vincent. 2017. "The Next Internet." Pp. 95–107 in *Carbon Capitalism and Communication: Confronting Climate Crisis*, edited by B. Brevini and G. Murdock. Cham: Springer International Publishing.

Murakami Wood, David. 2013. "What Is Global Surveillance? Towards a Relational Political Economy of the Global Surveillant Assemblage." *Geoforum* 49:317–26.

Murphy, Maria Helen. 2014. "The Pendulum Effect: Comparisons between the Snowden Revelations and the Church Committee. What Are the Potential Implications for Europe?" *Information & Communications Technology Law* 23(3):192–219.

Noble, Safiya Umoja. 2018. *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU Press.

Orlikowski, Wanda J. 2007. "Sociomaterial Practices: Exploring Technology at Work." *Organization Studies* 28(9):1435–48.

Ortiz de Mandojana, Natalia, and Juan Alberto Aragon-Correa. 2015. "Boards and Sustainability: The Contingent Influence of Director Interlocks on Corporate Environmental Performance." *Business Strategy and the Environment* 24(6):499–517.

Parks, Lisa. 2015. "Stuff You Can Kick: Toward a Theory of Media Infrastructures." Pp. 355–73 in *Between Humanities and the Digital*. Cambridge, MA: MIT Press.

Parks, Lisa, and Nicole Starosielski. 2015. *Signal Traffic: Critical Studies of Media Infrastructures*. University of Illinois Press.

Poster, Mark. 1990. "Foucault and Data Bases." *Discourse* 12(2):110–27.

Praescient Analytics. 2019. "Solutions." *Praescient Analytics*. Retrieved February 2, 2019 (https://praescientanalytics.com/solutions).

Raley, Rita. 2013. "Dataveillance and Countervailance." Pp. 121–46 in *Raw Data is an Oxymoron*. Cambridge, MA: MIT Press.

Raynes-Goldie, Kate. 2010. "Aliases, Creeping, and Wall Cleaning: Understanding Privacy in the Age of Facebook." *First Monday* 15(1).

Richards, Neil M. 2012. "The Dangers of Surveillance." *Harvard Law Review* 126:1934.

Sandvig, Christian. 2013. "The Internet as Infrastructure." in *The Oxford Handbook of Internet Studies*, edited by Dutton, William H.

Sassen, Saskia. 2006. *Territory, Authority, Rights: From Medieval to Global Assemblages*. Cambridge University Press.

Schiller, Dan. 2006. *How to Think About Information*. University of Illinois Press.

Schüll, Natasha Dow. 2012. *Addiction By Design: Machine Gambling In Las Vegas*. Princeton University Press.

Schwarz, Frederick AO, and Aziz Z. Huq. 2008. *Unchecked and Unbalanced: Presidential Power in a Time of Terror*. The New Press.

Scott, Susan V., and Wanda J. Orlikowski. 2014. "Entanglements in Practice: Performing Anonymity Through Social Media." *MIS Quarterly* 38(3):873–94.

Shorrock, Tim. 2016. "5 Corporations Now Dominate Our Privatized Intelligence Industry." September 8.

Simon, Bart. 2005. "The Return of Panopticism: Supervision, Subjection and The New Surveillance." *Surveillance & Society* 3(1).

Smith, Craig R., and Sergio Fernandez. 2010. "Equity in Federal Contracting: Examining the Link between Minority Representation and Federal Procurement Decisions." *Public Administration Review* 70(1):87–96. doi: 10.1111/j.1540-6210.2009.02113.x.

Sohn, Tim. 2015. "Trevor Paglen Plumbs The Internet." *The New Yorker*.

Star, Susan Leigh. 1999. "The Ethnography of Infrastructure." *American Behavioral Scientist* 43(3):377–91.

Star, Susan Leigh, and Karen Ruhleder. 1994. "Steps Towards an Ecology of Infrastructure: Complex Problems in Design and Access for Large-Scale Collaborative Systems." Pp. 253–64 in *Proceedings of the 1994 ACM Conference on Computer Supported Cooperative Work*. ACM.

Stefani, Silvana, and Anna Torriero. 2013. "Formal and Informal Networks in Organizations." Pp. 61–77 in *Advanced Dynamic Modeling of Economic and Social Systems*, edited by A. N. Proto, M. Squillante, and J. Kacprzyk. Berlin, Heidelberg: Springer Berlin Heidelberg.

Sterne, Jonathan. 2013. "'What Do We Want?''Materiality!''When Do We Want It?''Now!'" *Media Technologies: Essays on Communication, Materiality, and Society* 119–28.

Story, Jasmine N. 2014. "Cloud Computing and the NSA: The Carbon Footprint of the Secret Servers." *Journal of Environmental and Public Health Law* 9(1):33–65.

Suchman, Lucy A. 2007. *Human-Machine Reconfigurations: Plans and Situated Actions*. Cambridge University Press.

Telegeography. 2021. "Submarine Cable Map."

Transparency Toolkit. n.d. "ICWatch." *ICWatch*. Retrieved January 10, 2019 (https://icwatch.wikileaks.org/).

US Small Business Administration. 2019a. "FY 2020 Goaling Guidelines." 22.

US Small Business Administration. 2019b. "Table of Size Standards." *Table of Size Standards*. Retrieved January 2, 2021 (https://www.sba.gov/document/support--table-size-standards).

usa.gov. n.d. "How to Become a Federal Contractor." Retrieved December 17, 2020 (https://www.usa.gov/become-government-contractor).

Uzzi, Brian. 1999. "Embeddedness in the Making of Financial Capital: How Social Relations and Networks Benefit Firms Seeking Financing." *American Sociological Review* 481–505.

van der Vlist, Fernando N. 2017. "Counter-Mapping Surveillance: A Critical Cartography of Mass Surveillance Technology After Snowden." *Surveillance & Society* 15(1):137–57.

Volz, Dustin. 2022. "Secret CIA Bulk Surveillance Program Includes Some Americans' Records, Senators Say." *The Wall Street Journal*, February 10.

Wakefield, Alison. 2002. "The Public Surveillance Functions of Private Security." *Surveillance & Society* 2(4):529–45.

Wasserman, Stanley, and Katherine Faust. 1994. *Social Network Analysis: Methods and Applications*. Vol. 8. Cambridge University Press.

Waters, Stephenson. 2018. "The Effects of Mass Surveillance on Journalists' Relations with Confidential Sources: A Constant Comparative Study." *Digital Journalism* 6(10):1294–1313.

White, Halbert. 1980. "A Heteroskedasticity-Consistent Covariance Matrix Estimator and a Direct Test for Heteroskedasticity." *Econometrica* 48(4):817–38. doi: 10.2307/1912934.

Wonders, Brooke J., Frederic I. Solop, and Nancy A. Wonders. 2012. “Information Sampling and Linking: Reality Hunger and the Digital Knowledge Commons.” *Contemporary Social Science* 7(3):247–62.

Woodman, Spencer. 2017. “Palantir and Trump’s Deportation Machine – The Intercept.” Retrieved February 2, 2019 (https://theintercept.com/2017/03/02/palantir-provides-the-engine-for-donald-trumps-deportation-machine/).

Zarit, Matthew. 2018. “Lost in Translation: How Bureaucratic Hierarchies Limit Presidential Control Over Distributive Policymaking in US Federal Agencies.”

Zeileis, Achim. 2004. “Econometric Computing with HC and HAC Covariance Matrix Estimators.” *Journal of Statistical Software* 1(10).

Zuboff, Shoshana. 2019. *The Age Of Surveillance Capitalism: The Fight For The Future At The New Frontier Of Power*. New York: Profile Books.