

UC Irvine

UC Irvine Electronic Theses and Dissertations

Title

The Role of Corporate and Government Surveillance in Shifting Journalistic Information Security Practices

Permalink

<https://escholarship.org/uc/item/9p22j7q3>

Author

Shelton, Martin

Publication Date

2015

Copyright Information

This work is made available under the terms of a Creative Commons Attribution-ShareAlike License, available at <https://creativecommons.org/licenses/by-sa/4.0/>

Peer reviewed|Thesis/dissertation

UNIVERSITY OF CALIFORNIA,
IRVINE

The Role of Corporate and Government Surveillance in Shifting Journalistic Information
Security Practices

DISSERTATION

submitted in partial satisfaction of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

in Information and Computer Science

by

Martin L. Shelton

Dissertation Committee:
Professor Bonnie A. Nardi, Chair
Professor Judith S. Olson
Professor Victoria Bernal

2015

© 2015 Martin Shelton
This document is distributed under a Creative Commons
Attribution-ShareAlike 4.0 International License.

TABLE OF CONTENTS

	Page
LIST OF FIGURES	v
ACKNOWLEDGMENTS	vi
CURRICULUM VITAE	viii
ABSTRACT OF THE DISSERTATION	ix
SECTION 1: Introduction and Context	1
CHAPTER 1: The Impulse for Information Security in Investigative Journalism	2
1.1 Motivations	6
1.2 Research Scope	9
CHAPTER 2: Literature Review	12
2.1 Journalistic Ideologies	12
2.1.1 Investigative Routines and Ideologies	15
2.2 Panoptic Enforcement of Journalism	17
2.3 Watching the Watchdogs	21
2.4 The Decentralization and Normalization of Surveillance	27
SECTION 2: Findings	30
CHAPTER 3: Methods	31
3.1 Gathering Surveillance News	31
3.2 Interview Recruitment	32
3.3 Interview Structure	35

	3.4 Limitations	36
	3.5 Analysis	37
	3.6 Maintaining Confidentiality with At-Risk Populations	37
CHAPTER 4:	Legal and Technical Protections for Journalists	40
	4.1 Journalism, Surveillance, and the Law	40
	4.2 Government Whistleblowers and Leakers	53
	4.2.1 Key Espionage Cases	55
	4.3 Surveillance Across Borders	58
	4.4 Methods to Keep Sources Confidential	61
	4.5 Threat Modeling and Security Tools	63
CHAPTER 5:	Findings	73
	5.1 About the Journalists	73
	5.2 Attribution and Nonattribution in Reporting	74
	5.3 Threat Modeling	80
	5.4 Information Security Practices and Challenges	82
	5.4.1 Adoption, Concerns, and Challenges with Email Encryption	83
	5.4.2 Successes and Compromises in Instant Messaging	87
	5.4.3 Phones and Mobile Devices	89
	5.4.4 Malicious Software and End Point Security	91
	5.4.5 Avoiding Electronic Records	95
	5.4.6 Why Not Use Encryption?	99

5.4.7 Other Security Considerations	101
5.5 Secrecy and Invisible Surveillance	102
5.6 Outside of Work	103
5.7 Technology Companies and Surveillance in Journalism	105
5.8 American Journalism in Global Context	108
SECTION 3: Synthesis	113
CHAPTER 6: Discussion: Key Factors for Resisting Surveillance	114
6.1 Selective Security Approaches in Investigative Journalism	114
6.1.1 Awareness of Surveillance and its Conditions	116
6.1.2 Motivation for Security Approaches	118
6.1.3 Costs of Action	120
6.2 Acts of Resistance	124
CHAPTER 7: Conclusion	130
REFERENCES	135

LIST OF FIGURES

		Page
Figure 1	An example of a plaintext message converted into an encrypted PGP message.	66
Figure 2	Internal NSA slides detailing the collection and indexing of unencrypted Web traffic.	70
Figure 3	NSA Tailored Access Operations implanting “beacons” into computing equipment.	94

ACKNOWLEDGMENTS

I came to journalism to conduct research, but found the embrace of a warm community of reporters and press advocates. I consider this dissertation a collective, community-driven undertaking. It gave me a place to collect my thoughts alongside the insights of countless others. I'm thankful to numerous groups and individuals for their contributions to this research.

I want to thank the many journalists and press advocates who generously shared their time with me. Their fearless work to bring timely and accurate information to the public is foundational to our democracy. During my time with the Pew Research Center and throughout this work, I learned that a regular stream of deadlines can prevent journalists from having much downtime (much less a moment alone with their thoughts). The reporters spoke with me to share their “war stories,” and sometimes they did so while running between meetings. I spoke with press advocates, digital security specialists, and whistleblower lawyers, all of whom were equally generous with their time. I truly appreciate that so many remarkable individuals took the time out of their overbooked schedules to bring this research to life. Their passion for exposing truth, especially where it is obscured, inspired me to continue working for the press through research.

I'm grateful to my two wonderful co-advisors, Bonnie Nardi and Judith Olson, who have helped me develop as a researcher and as a person. During my time at the Department of Informatics at the University of California, Irvine, they have been my mothers away from home. I also want to thank Victoria Bernal for taking so many opportunities within and beyond our coursework to foster critical conversations about the role of surveillance in our democracy. I wish to thank my peers in the Department of Informatics for their critical feedback, insights, and friendship. I particularly wish to thank my cohort (and informal moral support network), the incoming Informatics PhD class of 2011.

I would like to recognize the Pew Research Center's Internet and Journalism Projects, my peers in Pew's data analytics laboratory, and Claudia Deane, who lobbied for us to join Pew as “big data” interns before the laboratory took flight. During my time at Pew, I consulted on the development of surveys to understand the privacy and security behaviors and perceptions of investigative journalists and ordinary Americans. The work with Pew Research was foundational to this research; it inspired me to focus on the intersection between digital policy and journalism.

Google's Privacy Research and Design group also deserves my thanks. In the summer of 2015, alongside a remarkable team—Anna Turner, Katie O'Leary, Dr. Sunny Consolvo, and Dr. Tara Matthews—I helped to conduct a study examining the privacy and security concerns and strategies of non-Western journalists and activists. This research provided important context around the privacy and security concerns and practices of U.S. investigative journalists. My friends and colleagues at Google helped me to tell clear stories about my research, and in so doing, to understand the research more intimately.

I want to thank my family, Marty, Paula, and Jonathan, for their support and encouragement throughout my PhD and my intellectual development more broadly. Finally, I'd like to thank my partner, Soraya, for her apparently infinite patience, thoughtful editing, and unflagging moral

support, and for accompanying me on countless trips to coffeehouses as I've developed this project.

CURRICULUM VITAE

Martin L. Shelton

- 2011 B.S. Psychology (Social Psychology), Santa Clara University
- 2011-14 Research Assistant, Technology, Design, & Research Laboratory
Research Assistant, Hana Research Laboratory
- 2012 User Research Intern, Twitter Inc.
- 2014 M.S. in Information & Computer Science (Informatics),
University of California, Irvine
- 2014 Data Analytics Intern, Pew Research Center Internet & Journalism Projects
- 2015 Privacy User Research Intern, Google Inc. Privacy Research & Design
- 2015 Ph.D. in Information & Computer Science (Informatics),
University of California, Irvine

FIELD OF STUDY

Human-Computer Interaction

PUBLICATIONS

- Shelton, M. L., Rainie, L., Madden, M., Anderson, M., Duggan, M., Perrin, A., & Page, D. (2015). Americans' privacy strategies post-Snowden. Pew Research Center Internet Project.
- Shelton, M. L., Lo, K., & Nardi, B. (2015). Online media forums as separate social lives: A qualitative study of disclosure within and beyond reddit. In Proc. iConference, 2015.
- Wang, Y., Echenique, A., Shelton, M. L., & Mark, G. (2013). A comparative evaluation of multiple chat stream interfaces for information-intensive environments. In Proc. CHI, 2013.
- Burger, J. M. & Shelton, M. L. (2011). Changing everyday health behaviors through descriptive norm manipulations. *Social Influence*, 6, 69-77.

ABSTRACT OF THE DISSERTATION

The Role of Corporate and Government Surveillance in Shifting Journalistic Information Security Practices

By

Martin L. Shelton

Doctor of Philosophy in Information & Computer Science

University of California, Irvine, 2015

Professor Bonnie A. Nardi, Chair

Digital technologies have fundamentally altered how journalists communicate with their sources, enabling them to exchange information through social media as well as video, audio, and text chat. Simultaneously, journalists are increasingly concerned with corporate and government surveillance as a threat to their ability to speak with sources in confidence and to conduct basic reporting. In response, some U.S. journalists are learning information security techniques as well as nontechnical approaches to source protection and slowing surveillance. I conducted thirty interviews with journalists and press advocates to learn about their information security practices and their perceptions of the impediments that government and corporate surveillance impose on their ability to complete their work. I found that most of the time, journalists had routine sources who did not require strict confidentiality. However, journalists expressed deep concerns regarding the confidentiality of their sources when working on sensitive stories and when their sources place themselves at risk. While I found the journalists shared widespread concerns about surveillance, they also had diverse and inconsistent approaches to their digital security. When conducting sensitive work, some journalists shared experiences about speaking with their sources

over encrypted channels, avoiding cell phones, or avoiding commercial phone and Web services that could be subpoenaed for their user data. To minimize their electronic records and for the sake of convenience, many of the journalists have been meeting sensitive sources in person whenever possible. However, unless absolutely necessary, many journalists preferred to speak with sources through the most convenient communication channels—for example, text messages and phone calls—even when they were concerned about issues of confidentiality. Even in stereotypically sensitive reporting (e.g., national security), the journalists would often forgo comprehensive security measures to speak with their sources. I argue that the security approaches often compete with journalists' other interests, such as communicating with sources and working with colleagues to publish within strict timelines.

Section 1. Introduction and Context

Chapter 1

Introduction—The Impulse for Information Security in Investigative Journalism

The American tradition of investigative journalism emerged from cyclical tides of political upheaval as old as the European colonies (Armao, 2000; Aucoin, 2006). American investigative reporters have been concerned with publicizing information in the public interest, especially where politically important truths are obscured (de Burgh, 2000; Ettema & Glasser, 1998). In the late 17th century, the tradition began with exposés revealing acts of transgression by the British Crown (Armao, 2000; Aucoin, 2006). The dissemination of news, journalistic professionalization, and reporting routines have evolved tremendously, particularly in the late 19th and early 20th centuries, lending authority and power to journalistic institutions (C. Anderson, 2008). With traditional readers turning to broadcast television and magazines and with journalists pushing for greater workplace inclusivity, both newsroom economics and the civil rights movements of the 1960s and 1970s catalyzed the spread of investigative reporting. During the 1960s, a new wave of investigative reporting emerged where journalists reported on the actions and motivations of people embedded in powerful institutions (e.g., Armao, 2000; Downie & Schudson, 2009). For example, Bob Woodward and Carl Bernstein's reporting on the Watergate scandal is often credited as the symbolic introduction of modern investigative reporting (Armao, 2000; Ettema & Glasser, 1998). They were able to conduct their work solely through their own persistence, caution, and the assistance of a network of human sources—individuals with timely knowledge—to help them unearth the facts in their reporting. In certain instances, sources require confidentiality to speak about facts in a news story without restraint. Woodward and Bernstein developed elaborate systems to covertly speak with then-unnamed sources, notably their most famous FBI informant Mark Felt, better known by the pseudonym *Deep Throat* (O'Connor, 2005).

In recent decades, journalists have come to rely on digital technologies to locate information for stories, to communicate with sources, and to publish their work (Ettema & Glasser, 1998; Weinberg, 1996). Particularly in national security and foreign affairs reporting, current research suggests that journalists attempt to protect their confidential sources by taking security measures against surveillance and data breaches. In so doing, they must consider a variety of actors, including telecommunications providers, information technology companies, and government institutions (Human Rights Watch & ACLU, 2014; McGregor, Charters, & Holliday, 2015; Pew Research Center, 2015).

In this dissertation, I explore how corporate and government electronic surveillance affects the work of investigative journalism in the United States, with attention to how journalists manage their information security. This examination of journalistic security practices will serve as a powerful foundation from which to explore the role of the free press, civic engagement, and digital technology in American democracy.

Since the recent emergence of countless disclosures of U.S. intelligence activities, journalists who investigate corporate and government activities have been among the most vocal opponents of electronic surveillance. To protect their sources, journalists have resorted to elaborate measures—avoiding online communications and meeting their sources in person, arranging meetings with disposable “burner” phones instead of their personal phones, and enhancing their communication security through the use of sophisticated encryption software (Human Rights Watch & ACLU, 2014; Pew Research Center, 2015). Increasingly, news organizations have sought out information security instruction with security specialists, including “boot camps” and multi-week trainings (Henrichsen, Betz, & Lisosky, 2015; Walker & Waters, 2015). Previous research attributes the heightened attention to information security practices to

multiple contemporary political factors, including the Obama Justice Department's aggressive stance toward journalists (Human Rights Watch & ACLU, 2014), as well as Edward Snowden's disclosures of National Security Agency surveillance (FDR Group, 2013; Human Rights Watch & ACLU, 2014; Pew Research Center, 2015). Yet, the field of investigative journalism has been facing information security challenges for decades (Armao, 2000; Ettema & Glasser, 1998). Exemplified by Woodward and Bernstein's reporting on the Watergate scandal, investigative journalists have long understood the seemingly extreme efforts that are necessary to keep sources confidential. Thus, it is crucial to consider the relatively recent NSA disclosures in a broader historical context by understanding how journalistic information security has operated in decades past. Simultaneously, in an environment of pervasive government surveillance over phone and Internet activity, previous research suggests that source protection (when a journalist refuses to publicly identify a source by name) is more challenging than ever before (Human Rights Watch & ACLU, 2014; Pew Research Center, 2015).

With special attention to information security practices, I explore the impact of corporate and government electronic surveillance on work in journalism over several months of investigation. I spent hundreds of hours reading news and reports on national security, personal information security, and legal challenges in courts, as well as following journalism and security conferences—the only way to keep abreast of the torrent of news surrounding U.S. surveillance. I also spoke with journalists as well as electronic policy and press advocates to learn about their experiences and perspectives on journalistic information security practices.

The interdisciplinary field of surveillance studies strongly influenced my analysis. In particular, I leverage prior surveillance studies research to explore the role of corporate institutions in contemporary surveillance (Andrejevic, 2002; Bogard, 2006; Haggerty & Ericson,

2000; Lyon, 2014) and orienting surveillance theories to examine the impact of contemporary U.S. intelligence practices (Lyon, 2014). The ongoing NSA disclosures have also attracted the attention of advocacy and research organizations that conduct empirical research. A growing body of research focuses on how ordinary citizens alter their behavior in response to government surveillance (Hampton et al., 2015; Madden, 2014; Marthews & Tucker, 2014; Shelton et al., 2015). A smaller constituency of empirical work examines the role of information security practices in journalism (McGregor et al., 2015; Pew Research Center, 2015). Most related work emerges from advocacy organizations, including PEN America (FDR Group, 2013, 2015), UNESCO (Henrichsen et al., 2015), and the American Civil Liberties Union and Human Rights Watch (2014).

In prior research, government surveillance had been a central concern—particularly in the context of journalism that critically investigates the activities of authorities (e.g., FDR Group, 2013; Human Rights Watch & ACLU, 2014). However, the government is ultimately one of many actors conducting electronic surveillance of journalists. Indeed, the government relies on networks of companies that can be legally compelled to share data about their customers, and in other cases, that willingly share data with the government (e.g., Angwin et al., 2015). Surveillance should therefore be understood as a collective activity involving many groups and conflicting interests, rather than one cohesive party (Haggerty, 2006; Haggerty & Ericson, 2000; Schneier, 2015). I pay particular attention to governments and private companies due to the scope of their surveillance capacities.

Much of the existing literature is inspired by, and structures itself around, how journalists and ordinary citizens respond to government surveillance. Yet, previous literature tends to overlook the crucial role the private sector plays in contemporary surveillance practices. I intend

to address this gap in the literature to understand how government and corporate actors influence the work of investigative journalism.

In the following section, I argue that examining the impact of government and corporate surveillance on journalism requires further academic attention. I follow with a summary of my intended research scope, and I conclude this chapter with a brief outline of the work.

1.1 Motivations

I examine journalists, as opposed to any other group, because of their distinctive security approaches. Much existing literature examines how the general public perceives U.S. surveillance, yet suggests that ordinary Americans have made relatively modest security changes in response to the NSA revelations (Marthews & Tucker, 2014; Shelton et al., 2015). Instead, specific groups, including investigative journalists and law professionals, are changing their information security habits in order to protect communications with confidential sources and clients (FDR Group, 2013; Human Rights Watch & ACLU, 2014; Pew Research Center, 2015).

The NSA disclosures have inspired scholars to examine how entire populations perceive surveillance and how electronic monitoring influences behavior on the Internet. In general, these studies point to people withholding certain forms of information in various electronic communication services. Pew Research (Hampton et al., 2015) found that 86% of Americans were willing to have an in-person conversation about the government's electronic surveillance programs, whereas only 42% were willing to speak about the same topic on social media sites like Facebook or Twitter. However, when researchers measure online self-censorship, the effect is subtler. For example, Marthews and Tucker (2014) found that Google searches including sensitive terms (according to the Department of Homeland Security's "government sensitive" list) diminished by 2% in the months immediately following the NSA revelations, while

comparatively less sensitive search terms rose overall. In other words, surveillance appears to be associated with modest trends of online self-censorship among ordinary Americans.

Americans share concerns over electronic surveillance practices, but the concern has been met with relatively small changes in security habits (Madden, 2014; Shelton et al., 2015). A Pew Research survey (Shelton et al., 2015) found widespread concern over electronic surveillance, but comparatively small numbers of Americans say they are altering their electronic privacy habits in their use of email (18%), search engines (17%), social media (15%), cell phones (15%), text messages (13%), mobile apps (13%), and landline phones (9%). An exceedingly small number of survey respondents reported using sophisticated encryption tools to scramble their electronic communications, thus making them illegible to potential eavesdroppers. Indeed, at least a third of American adults have not heard about encryption tools that can be used to enhance their privacy in email communications and Web traffic (Shelton et al., 2015). While little direct observational research exists, current studies point to modest trends of self-censorship and withholding information in electronic communications among ordinary citizens.

Since the NSA disclosures, policy and advocacy groups including the American Civil Liberties Union (ACLU) and Human Rights Watch (HRW) have released reports on the impact of government electronic surveillance on U.S. journalists (Human Rights Watch & ACLU, 2014). One respondent in the ACLU and HRW report suggests that reporters in intelligence, followed by reporters covering the Department of Justice, terrorism, the military, and national security, were the most likely to be plagued by increasingly “skittish” sources. A separate Pew Research report similarly suggests that investigative reporters covering government, national security and foreign affairs are more likely than other groups of journalists to make substantive changes in their work practices and connections with sources since the Snowden disclosures

(Pew Research Center, 2015). For example, many investigative journalists anonymize traces of their investigative research and encrypt their communications and Web traffic through sophisticated software. Some investigative reporters communicate with sources with disposable “burner” phones in order to make their calls more difficult to trace (Human Rights Watch & ACLU, 2014). Some forgo technical solutions, deliberately avoiding phones and other communication technologies, and instead speak with their sources in person. Many of the reporters suggest that the measures are warranted to protect sources, yet these reporters feel that they should not be forced to do so. As one journalist described in the ACLU and HRW report, “I don’t want the government to force me to act like a spy. I’m not a spy; I’m a journalist.” A survey by PEN America and the Farkas Duffett Research Group (2013) suggests that self-censorship in electronic communications is another common response among journalists. PEN found that journalists and non-fiction writers are increasingly self-censoring in their electronic communications for fear that surveillance might cause them future troubles. For example, 28% of respondents have curtailed or avoided social media activities, and 24% have avoided certain topics of conversation over the phone or email. Survey participants described difficulties conducting research on various topics because they feared how their search terms on sensitive topics might be interpreted. Roughly 93% of journalism professionals reported being “very concerned” about government efforts to compel journalists to reveal sources of classified information. At the time of this work, with few exceptions, research addressing the role of electronic surveillance in journalism emerged largely from journalism and human rights advocacy organizations. The research provided readers with an understanding of the most dramatic impacts of surveillance on journalists, as well as directions for future study.

1.2 Research Scope

Examining the influence of electronic surveillance on investigative journalism requires both speaking with press advocates who understand the broad trends in journalism, and learning from reporters themselves. I spoke with investigative journalists in particular, because of their deliberate involvement in issues of information security. Previous work describes how investigative journalists perceive and respond to national intelligence surveillance, specifically in reporting on the Department of Justice, terrorism, the military, and national security (Human Rights Watch & ACLU, 2014; Pew Research Center, 2015). By now, it is well established that some journalists resist surveillance through the use of security tools, face-to-face meetings, and creative uses of consumer technology to complicate the analysis of their electronic records (Human Rights Watch & ACLU, 2014; Pew Research Center, 2015; Walker & Waters, 2015). Some crucial questions have not been clearly addressed in previous literature:

1. When, and under what conditions, do journalists deliberately engage in countersurveillance practices?
2. To what extent do reporters outside of stereotypically sensitive journalistic beats (e.g., national security) see surveillance as a hindrance in their work?
3. What roles do telecommunications and information technology companies play in journalistic information security practices?

I expand on existing research by exploring how journalists attempt to resist surveillance through the selective use of security practices, and by exploring the role of technology companies in government surveillance. I structured my interviews with investigative journalists and press advocates around four themes:

1. How is their work challenged by corporate and government surveillance?

2. What are they doing about it? What technical and non-technical solutions do they need to employ to continue collecting information and reporting?
3. How do they understand the trade-off between the government's role in attempting to keep Americans safe and their need to conduct meaningful investigative work?
4. How do journalists perceive the potential changes in their work habits?

My goal, then, is not to examine information security tools or practices. In the end, the security practices themselves will change. I am more concerned with *how*, and most importantly, *why* journalists choose to use security tools and practices.

In this work I focus primarily on electronic surveillance in the United States and how it impacts American journalists. However, U.S. surveillance cannot be disentangled from legal and technical surveillance capacities around the world (Bigo, 2006). I occasionally draw on stories of foreign journalists, as any meaningful discussion of U.S. foreign intelligence capabilities must include surveillance across borders. Indeed, the proliferation of surveillance technologies around the globe increasingly mirrors U.S. surveillance capabilities. Private companies now sell commercial spying software to governments that might otherwise lack the expertise to conduct offensive surveillance of journalists and activists, as is the case in Ethiopia, Bahrain, and Morocco (Crete-Nishihata et al., 2014; Human Rights Watch, 2014b; Marczak, Guarnieri, Scott-Railton, & Marquis-Boire, 2014; Marquis-Boire, Marczak, Guarnieri, & Scott-Railton, 2013). Surveillance capacities in the Western world are mobilized as commercial products for governments in volatile regions, some of which explicitly target journalists in both digital and physical attacks. Some of my interviewees have worked as, or alongside, international journalists. Their stories contextualize Western surveillance practices. In many regions, activists and journalists face violent attacks or imprisonment for their adversarial reporting, whereas in

the United States, journalists and their sources usually face legal discipline. While I focus on American investigative journalism, I provide diverse perspectives in this research by interviewing journalists and advocates across a spectrum of journalistic beats and work in press advocacy.

In the following chapters, I discuss the changes in practices among journalists. Many journalists have strong motivations, both practical and principled, to resist surveillance of their personal data and communications. In chapter two, I explore previous literature on research describing journalistic ideologies and practices in relation to theories of surveillance. In particular, I explore Foucault's (1977) concept of the panopticon, and Haggerty and Ericson's (2000) concept of the *surveillant assemblage*. I conclude the section with an outline of recent research that explores journalism and surveillance. Chapter three lays out this study's methods for learning about information security practices among journalists by examining news, reports, and conferences, and by learning from journalists themselves. Chapter four describes historical and current developments in how journalists connect with sources and how they protect their communications. In chapter five, I explore the stories of the journalists and press advocates to understand their motivations and practical responses for managing information security. My findings lead to a broader discussion on the evolving role of information security practices among journalists.

Chapter 2

Literature Review

Multiple arenas of scholarship serve as powerful toolboxes for considering the intersection between surveillance and journalism. Transparency and surveillance play conflicting roles in contemporary newsrooms, where journalists simultaneously seek to expose information in the public interest and withhold specific types of information from publication. To explore this paradox, I rely on the field of surveillance studies, which itself draws on a multitude of scholarly disciplines.

Few studies have explored the role of information security practices and surveillance countermeasures in contemporary journalism. Often citing the National Security Agency disclosures as their catalyst, a small number of studies have begun to explore journalistic security in greater depth (e.g., FDR Group, 2013, 2015; Human Rights Watch & ACLU, 2014; Pew Research Center, 2015). I explore these studies in detail, placing theories of surveillance and journalism studies together in conversation. For the purposes here, I focus on journalism in American news institutions. My goal is not an exhaustive canvassing of surveillance studies and journalism studies, but rather, to contextualize investigative journalism in an evolving environment of corporate and government surveillance.

2.1 Journalistic Ideologies

The practice of journalism involves gathering, scrutinizing, and presenting the news for an audience (Deuze, 2005; Tuchman, 1973; Zelizer, 1993). Journalists are steeped in these newsmaking routines, while simultaneously engaged in “routinizing” unexpected events for their audiences through regular analysis and publication (Tuchman, 1973). To the extent that journalists gather, analyze, and broadcast information to the public, the many fields and subfields of journalistic practice can be understood to overlap in their routines and ideologies (Deuze,

2005; Hanitzsch, 2007).

The late 19th and early 20th centuries represent an introduction to contemporary journalism, characterized by the rapid development of professional norms, formalized pedagogies, and standards of ethics (Bivins, 2014; Davis, 2010; de Burgh, 2000; Deuze, 2005; Krause, 2011). Specific details differ among individual news organizations, but in general, Western news organizations usually develop their own codes of ethics detailing standards of journalistic integrity, information quality, public service, timeliness, and attribution among sources (Bivins, 2014; Deuze, 2005; Hafez, 2002). Previous work suggests that journalists often disagree on the need for formalized codes of ethics (Hanitzsch, 2007), and indeed, journalistic standards are not constituted through their professed ethics guidelines alone. In some cases journalists overtly reject guidelines in favor of individualistic standards of ethics (Keeble, 2008, pp. 6-8). As in any profession, journalists also informally share stories and personal experiences about ethical ideals and lapses (Wyatt & Clasen, 2014).

Both official and informal discourses among journalists collectively give rise to, and reflect, journalistic ideologies with specific characteristics. For example, in a cross-national study of first-year journalism students in 22 countries, Splichal and Sparks (1994) found that journalism students across the world shared a desire for autonomy and independence in their reporting practices. Similarly, in a survey of nearly 2,000 professional journalists from 18 countries, Hanitzsch and colleagues found that independence, non-involvement in stories, publicizing political information, and monitoring the government are all considered essential roles of journalism around the globe (Hanitzsch et al., 2011). Hanitzsch (2009) suggests that the journalistic ideals of objectivity and impartiality dominate news organizations around the world, arguing for a “transfer of ideology” from Western nations to the East, as demonstrated through

occupational routines. Journalistic values of intellectual and editorial independence, a “watchdog” role over powerful institutions, and a strict adherence to fact-based reporting characterize the work of journalists in an increasingly globalized ideology (p. 413).

In an analysis of multiple cross-national surveys exploring journalistic values and standards, Deuze (2005) argues that journalists largely agreed on a small set of ideological values, despite their substantial differences in geopolitical and social climates. The ideology of journalism, Deuze suggests, is the collective process of including and excluding accepted ideas about the profession. According to Deuze, “Ideology is seen here as an (intellectual) process over time, through which the sum of ideas and views—notably on social and political issues—of a particular group is shaped, but also as a process by which other ideas and views are excluded or marginalized.” Deuze (2005) argues that journalists strive (1) to work in service to the public, (2) to be objective, impartial, or neutral, (3) to be autonomous, or independent in their reporting, (4) to be quick and responsive in reporting, and (5) to uphold ethics and standards of legitimacy.

Depending on their specific context, Zelizer (1993) argues, reporters act on elements of journalistic ideologies in distinct ways. For example, despite the apparent global convergence of journalistic ideologies, journalists’ employers will have an inevitable and profound influence on their reporting (Haan, Landman, & Boyles, 2014; Wyatt & Clasen, 2014). A news organization can provide substantial legal, technical, and editorial support to journalists. Moreover, funding profoundly impacts what kinds of work can be conducted. For example, Armao (2000) suggests that news organizations with corporate owners sometimes downplay investigative reporting, which can be quite expensive and may attract “lone wolves” who may not fit neatly into their corporate newsroom culture. Those owners may instead reward “team players who support the company.” (p. 44) The newsroom’s governance has a clear influence on the work done within

journalistic institutions.

The newsroom, of course, is only one of many configurations of news institutions. For example, journalists work in traditional newsrooms, but may also work as independent journalists who write stories for multiple newsrooms, or may work with small organizations that sell their news to larger publishers. The boundaries of professional journalism are further complicated by blogging and social media, allowing new genres of “citizen journalism,” where ordinary people participate in creating and publishing the news outside of traditional news organizations (Singer, 2010). Journalists continue to grapple with the role of online news production in established journalistic practices, suggesting that professional journalism is distinguished not only by original reporting (Mitchelstein & Boczkowski, 2009; Singer, 2010), but by an enduring commitment to journalism as an occupational identity. As Wyatt and Clasen (2014) put it so well, “What do these newsroom-enabled relationships yield? First is a sense of solidarity and shared purpose. Newsroom colleagues are comrades—brothers- and sisters-in-arms. They are people who share the same moral commitments and who, through those commitments, have taken up the identity ‘journalist.’” (p. 251) In other words, journalism should not be understood through journalists’ behaviors alone, but also their ideological identification with the profession.

2.1.1 Investigative Routines and Ideologies

Routine work in investigative journalism is distinct from other areas of journalism. Whereas most journalism typically requires work with sanctioned information sources, investigative reporters focus on digging up information that is obscured. Sometimes “obscured” information can be understood as secret or privileged, but it may also be publicly available and unexplored. In practice, their work requires investigative journalists to comb through documentary evidence

(e.g., public records) and to learn from sources outside of the “usual suspects” (Armao, 2000; Ettema & Glasser, 1998; Weinberg, 1996). Furthermore, most types of journalism seek to publish as quickly as possible, whereas investigative work often requires long-term examination, sometimes over the course of months or years (Ettema & Glasser, 1998).

Investigative work is often more expensive than other types of journalism. Investigations require substantial investment by the news organization and may generate fewer advertising dollars than the news organization could collect by publishing short articles. Furthermore, investigative reporters are often digging up information that outside parties may not want publicized, including the government, private organizations, and lone individuals (Armao, 2000; Ettema & Glasser, 1998; Weinberg, 1996). In part, investigative work often surfaces critiques of the powerful. Armao (2000) argues that business leaders of news organizations sometimes fear how investigative reporting can affect a newsroom’s advertising potential. In an environment of enormous cutbacks and corporate ownership of journalism organizations, some corporate owners do not favor investigative reporting (Armao, 2000). Bernt and Greenwald (2000) sum up the problem accordingly: “the corporate goals of maximizing profit and maintaining the status quo or managing change may be incompatible with either the watchdog or guard-dog mission of journalism to monitor the establishment” (p. 51).

There are reporters who investigate, and then there are investigative reporters. Their practices at times overlap, yet they can be distinct in routines and genres of inquiry. In subtle respects, investigative journalists also have unique ideological orientations, while retaining commitments to institutional accountability and the publication of information in the public interest (Armao, 2000; Ettema & Glasser, 1998).

2.2 Panoptic Enforcement of Journalism

While journalists act as watchdogs to hold powerful institutions accountable, journalists' audiences hold reporters to account in turn. Journalistic ideologies introduce conflicts between the need for near-absolute publicity enabled through reporting, and the need for selective confidentiality. I explore these conflicts through Michel Foucault's (1977) concept of panopticism, highlighting fundamental paradoxes of transparency in journalism.

Foucault (1977) examined how power is exercised through surveillance using the metaphor of Jeremy Bentham's architectural design of a prison, the panopticon. For Foucault, the panopticon represents "a diagram of a mechanism of power reduced to its ideal form" (Foucault, 1977, p. 205), elevating the prison to an embodiment of power. Bentham's panopticon exposed the prison's inhabitants to a single, centralized watchtower shielded from reciprocal view. From the center of the prison, a guard may watch any prisoner without being seen in turn. In effect, the architecture of the panopticon yields self-disciplining inmates who must assume they are being watched at all times, whether or not someone is in the watchtower.

Surveillance studies often—in fact, almost unavoidably—draw on Foucault's panoptic metaphor to examine surveillance and power (Simon, 2005). However, a chorus of scholars describe how the panopticon is ill-fitted to contemporary concepts of surveillance (e.g., Bossewitch & Sinnreich, 2013; Haggerty, 2006; Simon, 2005) that are characterized by automated data-gathering, aggregation, and analytical methods, as well as the globalization of surveillance by governments and corporate institutions (Bigo, 2006; Lyon, 2014).

In Foucault's classic concept of the panopticon, the few watch the many, imposing clear power asymmetries between the watcher and the watched (Brunton & Nissenbaum, 2013). In the "top-down" relationship Foucault envisioned, power is exercised through the act of monitoring

others. However, more recently, scholars have adapted Foucault's model to describe alternative configurations of surveillance. The oppressive power asymmetry introduced by panopticism is often at odds with people's desire to broadcast themselves. People voluntarily engage in mutual surveillance of one another through online dating (Andrejevic & Gates, 2014) and within social media websites (Albrechtslund, 2008; Marwick, 2012). Andrejevic compares hierarchical marketing practices of data collection to what he calls "lateral" surveillance in the context of online dating, where users are encouraged to inspect one another and share information about each other (Andrejevic, 2002; Andrejevic & Gates, 2014). In some situations, broadcasting information about oneself is desirable. Drawing on social media, Albrechtslund (2008) calls surveillance a "mutual, empowering and subjectivity-building practice," arguing for surveillance as a fundamental part of ordinary social life.

Often, people voluntarily subject themselves to surveillance. Rettberg (2014) describes how modern surveillance is often marked by the desire for visibility to others, but also suggests that information technology can be a lens through which people see themselves by learning about their own biometrics and by contemplating themselves through their own social media activity. As she argues, "We don't think too much about our machine audiences. We are too busy learning more about ourselves and each other by taking selfies, writing blogs, talking together on Facebook or Tumblr." (p. 88) The oppressive walls of the panopticon live at odds with the reality where, in routine life, people selectively seek publicity (Albrechtslund, 2008; Marwick, 2012; Rettberg, 2014).

Not unlike people who benefit from broadcasting themselves on social media, news organizations benefit from a large audience. Mass media organizations prize their viewership and, as a business imperative, need their viewership in order to survive (Mathiesen, 1997). By

deriving its power from the attention of its audience, journalism inverts the power relationship of Foucault's panoptic model, and yet such an inversion also highlights the audience's power (C. Anderson, 2008). When journalists place the news in a public setting, they open their work to near-absolute scrutiny, with the potential to damage their own professional standing and threaten the perceived legitimacy of their work (Allen, 2008; Deuze, 2005). Simultaneously, by providing credible and accurate information in the public interest, journalists seek a sense of legitimacy in the eyes of the public (Franklin & Carlson, 2011; Reich, 2011a, 2011b). Anderson (2008) described a reporter's sense of legitimacy as "journalistic authority." Journalistic authority is the cultural power that allows journalists to give meaning to their work as "accurate, truthful, and of political importance" (C. Anderson, 2008, p. 250). In other words, journalistic authority is derived from the news audience.

In maintaining journalistic authority, journalists both publicize and withhold information as they seek to publish primarily relevant and necessary parts of a story (Allen, 2008). Where information is newsworthy, they may still feel compelled to withhold information (e.g., national security secrets). In some cases, journalists actively avoid publishing certain items, such as the names of anonymous sources (Shoemaker & Reese, 1991). Allen (2008) described the challenge for journalists of discerning what information should be published, as well as concerns with maintaining the trust of their readership. For example, Allen describes the "pseudo-event"—an event contrived explicitly for press coverage. While journalists can simply cover the event without acknowledging its scripted nature, they may report transparently by sharing the staged nature of the pseudo-event with their audience. According to Allen, "Transparency as journalistic practice becomes a way for journalists to describe the constructed reality of pseudo-events without making judgments about the legitimacy of the story and separating themselves from

responsibility for the deceptive nature of the story. Or put another way: journalists know that what they are reporting is deceptive, but they are not responsible for that deception as long as they report the fact that they know it is deceptive.” Allen points out that such practices represent calculated acts of selective transparency.

Calculated transparency leads journalists to engage in what Habermas (1991) called “strategic” communication. Allen suggests that transparency can be reduced to a rhetorical tool to enhance journalistic credibility and accuracy. In his words, “Following Habermas, pseudo-events are a form of strategic action that require more from journalists than admitting the fact that they are being manipulated. They require an independent assessment by journalists about the validity and truth-claims contained in those events.” While journalists intend to promote informed political decision-making and take the responsibility quite seriously, they simultaneously do so in selective and instrumental fashions (Allen, 2008; Wyatt & Clasen, 2014).

Allen’s (2008) work suggests that journalists have a responsibility to conduct accurate reporting and simultaneously mobilize fact-based reporting as a shield from scrutiny. In effect, fact-finding becomes a tool. Indeed, the principle of dispassionate fact-finding gives birth to a journalistic cliché: “If your mother says she loves you, check it out” (Hamilton & Krimsky, 1996, p. 11). Based on their own ideological commitments (Deuze, 2005; Hanitzsch, 2007; Hanitzsch et al., 2011) and a pragmatic interest in maintaining legitimacy (Allen, 2008), reporters need to be skeptical of information they wish to publish. In Allen’s view, journalists should either withhold unreliable information, or report their doubts—both as an ethical imperative and to stand up to scrutiny of their work.

One key custom for lending legitimacy to journalistic work is the practice of finding and

quoting statements from sources that appear credible (Carlson, 2011b; Franklin & Carlson, 2011). Journalists have long relied on official, routinized sources to surface original reporting (Gans, 1979; Reich, 2011a; Sigal, 1973). These sources typically come from positions of authority—government officials, organizational spokespeople, and senior employees. Reporting requires the quick turnover of stories, and time pressures profoundly influence how journalists work with their sources. Indeed, journalists rank source credibility as the primary factor in source selection, followed by time pressure (Powers & Fico, 1994). Reliable, authoritative sources are seen as highly valuable because they can lend legitimacy to reporting (Hallin, Manoff, & Weddle, 1993; Reich, 2011a).

Previous research suggests that journalists repeatedly reach out to sources who reliably provide timely and accurate information. In his seminal study of *CBS Evening News*, *NBC Nightly News*, *Newsweek*, and *Time*, Gans (1979) found that journalists valued sources with specific characteristics. Journalists most value sources who convey the most information in the least amount of time, are reliably available, and appear trustworthy, authoritative, and articulate. These sources can be seen to lend authority to the news, while simultaneously deflecting criticism from the journalist to the source (Carlson, 2011b). As Shoemaker and Reese argued, “Attributing statements to sources is a key element of the objective ritual. It protects against accusations that they have been manipulated” (p. 108). The maintenance of audience credibility is of crucial importance, upheld by providing evidence in all aspects of published work. In other words, transparency is mobilized as an object of journalistic legitimacy (Allen, 2008).

2.3 Watching the Watchdogs

Wielding the power of the pen, news organizations act as overseers for powerful institutions. However, they don’t typically use the pen to police themselves or other journalistic institutions,

and indeed, previous literature suggests that they may also be resistant to such practices (Hamilton & Krinsky, 1996). As Hamilton and Krinsky (1996) argued, “Journalists take great pride in their role as watchdogs fearlessly guarding the commonweal. Yet, when it comes time to consider how *they* should be watched, they protest” (p. 133, emphasis original). Journalistic institutions have a few strategies for holding themselves publicly accountable. For example, journalists print and highlight corrections to their writing, and may publish extended letters-to-the-editor (Hamilton & Krinsky, 1996). However, these acts of transparency are self-motivated, serving to maintain trust with readership. In contrast, Hamilton and Krinsky suggest that journalists detest being policed by others outside the newsroom.

Electronic surveillance represents a key example of journalistic resistance to monitoring. In recent years, researchers have begun to examine how journalists perceive government surveillance, and how it affects their work. In particular, the literature suggests that American journalists are concerned that U.S. surveillance practices will reveal their sources and methods (Human Rights Watch & ACLU, 2014; Pew Research Center, 2015). For the moment, a relatively small number of related studies exist. Among the few current empirical studies, the Pew Research Center conducted a survey of nearly 700 investigative journalism professionals to understand their information security practices in the months following the Snowden disclosures (Pew Research Center, 2015). Additionally, the Tow Center for Digital Journalism at Columbia University is perhaps the foremost institution examining the digital security practices in American journalism. Tow Center fellows Walker and Waters (2015) conducted a study on the effectiveness of digital security pedagogies in journalism school (j-school) classrooms. In partnership with researchers at the University of Washington, the Tow Center also examined how journalists based in France and the U.S. manage their digital security (McGregor et al.,

2015). Nearly all other studies in this arena come from advocacy groups, including the American Civil Liberties Union and Human Rights Watch (2014), UNESCO (Henrichsen et al., 2015), and PEN America (FDR Group, 2013, 2015).

The Pew Research Center (2015) found that investigative journalists share widespread concerns about government surveillance, and some changed their information security practices in the months following the Snowden disclosures. According to Pew, 80% of investigative reporters believed that being a journalist increases the chance of their their data being collected by the government, and some 64% believed the U.S. government has collected information about their personal online or phone communications. Roughly half who belong to a news organization believed their news organization was not doing enough to protect them and their sources.

At the time of data collection in December 2014, only 27% of the journalists in Pew's (2015) survey reported that they have spent at least "some time" recently (over the past 12 months) researching how to improve their digital security. Journalists covering stereotypically sensitive reporting beats, including government, national security, and foreign affairs, appeared significantly more likely than other journalists to view electronic surveillance as a serious issue in their work. Journalists covering sensitive beats said that they have changed how they store sensitive documents (58%) compared to other journalists (46%), and have changed how they communicate with their colleagues (39%) more than other journalists as well (26%). They were also more likely than other journalists to adopt a variety of sophisticated security tools and techniques. Journalists covering sensitive beats were more likely than other journalists to report turning off their electronic devices when meeting sources in person, using email encryption, communicating through fake online profiles (e.g., in their email), and using voice encryption when speaking with sources. They were also more likely to say that it has become harder to find

sources to speak on the record (18%) than others (10%).

Following the NSA disclosures, Human Rights Watch and the American Civil Liberties Union released a joint report examining how journalists have been addressing surveillance in their work, suggesting that reporters must go through difficult lengths to protect the confidentiality of sources (Human Rights Watch & ACLU, 2014). In the report, journalists expressed frustration with government surveillance, arguing that sources are increasingly reluctant to come forward with information in the public interest. In turn, the journalists took pains to protect the confidentiality of their sources. To diminish risk, investigative journalists working with sensitive sources would provide security guidance for sources and leave misleading information for potential investigators. When connecting to a source, they may opt to use sophisticated encryption software on their phones and in their online conversations. They make calls from disposable “burner” phones and public pay phones, as well as leaving their cell phones elsewhere as they meet sources in person. As *ProPublica* editor-in-chief Stephen Engelberg suggested in the report’s press release (Human Rights Watch, 2014a), “I think anybody who is a good reporter now has to think about how do you contact somebody without leaving an electronic trail of crumbs behind you that directs potential investigators to your source.”

Digital security approaches are often time-consuming or inconvenient for journalists. For example, many journalists reported that they taught themselves to use encryption tools, and that the software is often poorly designed and difficult to use. However, in a study with 15 journalists based in the U.S. and France, McGregor and colleagues (2015) also found that journalists use ad hoc approaches that fall outside the scope of traditional security techniques. For example, the researchers described an instance where a reporter called his source’s previous assistant and left

a message with a false name. When the assistant passed on the message, the source would know to contact the journalist. McGregor and her colleagues argue that these ad hoc approaches indicate that some journalists (and/or their sources) sometimes feel uncomfortable with traditional security technology.

With journalists teaching themselves to manage their digital security, newsrooms and journalism organizations increasingly invest in security training. In their own research conducting security training, Walker and Waters (2015) found that a series of short workshops resulted in better retention and less confusion around security concepts than introductory sessions or multi-day “boot camp” events. They suggest that digital security programs are not meeting the practical needs of newsrooms, nor are current interventions meeting the needs of journalism schools, which often lack a systematic curriculum for teaching information security (Walker & Waters, 2015). Furthermore, when journalists do have training sessions, they often leave out significant aspects of security knowledge. For example, such training often does not include operational security—techniques for assessing critical information that should be withheld from an adversary (Henrichsen et al., 2015). The concepts can be challenging for participants, and security boot camps and short-term sessions commonly fail to focus on the specific needs of the participants (Walker & Waters, 2015).

To avoid endangering themselves or their sources, a small number of journalists opt not to pursue stories, and in some cases, may self-censor in the course of their research (Human Rights Watch & ACLU, 2014; Pew Research Center, 2015). For example, in the ACLU and Human Rights Watch report, a senior national security and intelligence journalist at McClatchy suggested, “Protecting a source is paramount for me. If I can't report a story without keeping a source safe, I'm not going to report the story” (Human Rights Watch, 2014a). Journalists who

judge themselves incapable of protecting a source's anonymity in the face of legitimate threats when reporting a story may choose not to pursue the story at all, signaling that surveillance necessarily discourages the publication of certain stories.

Previous research provides conflicting results about the role of electronic surveillance in self-censorship among journalists. Shortly after the Snowden disclosures, a survey by PEN America and the Farkas Duffett Research Group (FDR Group, 2013) found that journalists and non-fiction writers increasingly self-censored in their electronic communications for fear that surveillance might cause them future troubles. Some 28% of respondents reported they have curtailed or avoided social media activities, and 24% have avoided certain topics in phone or email conversations. Survey participants described difficulties conducting research on various topics because they feared how sensitive search terms would be interpreted. Roughly 93% of journalism professionals reported being "very concerned" about government efforts to compel journalists to reveal sources of classified information.

In early 2015, the Pew Research Center Journalism Project released a report detailing how investigative journalists perceive and respond to government surveillance (Pew Research Center, 2015). Unlike PEN America, Pew found that investigative journalists largely continued to pursue stories, and few (13%) chose not to reach out to sources due to concerns related to surveillance. Even fewer (3%) decided not to pursue certain stories in response to surveillance. In other words, there has been mixed support for the claim that surveillance leads U.S. journalists to censor themselves.

Journalists' problems of surveillance fundamentally overlap with those of ordinary citizens, because both groups often use the same technologies. However, journalists may have greater need for surveillance countermeasures. For the moment, research examining the

relationship between journalists and information security practices has tended to position surveillance as a preemptive law enforcement or government activity (FDR Group, 2013; Human Rights Watch & ACLU, 2014; Pew Research Center, 2015). While the literature has focused on government actors, theories of surveillance increasingly have highlighted a decentralized assemblage of non-state actors that enable government surveillance.

2.4 The Decentralization and Normalization of Surveillance

To understand basic processes of electronic monitoring, surveillance studies scholars are moving beyond the centralized notion of the panopticon. As Haggerty and Ericson argue (Haggerty, 2006; Haggerty & Ericson, 2000), panopticism must not be understood through the metaphor of a single identifiable watchman at the center of the prison. Gilles Deleuze and Felix Guattari (1988) offer an alternative metaphor inspired by rhizomes—plants growing like weeds at the surface level, but with interconnected systems of roots below the ground. Drawing on Deleuze and Guattari’s rhizomic metaphor, Haggerty and Ericson (2000) reimagined the panopticon through the concept of *assemblages* that may include a broad range of actors that conduct surveillance while interconnected in ambiguous fashions.

Through the collection, aggregation, and analysis of disparate sources in the exchange of data, Haggerty and Ericson argue that contemporary surveillance transforms people into digital representations composed of data. In their words, “A great deal of surveillance is directed toward the human body. The observed body is of a distinctively hybrid composition. First it is broken down by being abstracted from its territorial setting. It is then reassembled in different settings through a series of data flows. The result is a decorporealized body, a ‘data double’ of pure virtuality.” In modern surveillance systems, “data doubles” (Haggerty & Ericson, 2000; Los, 2006) are collections of computerized information about people, represented through

standardized data formats across various contexts. Being in contact with a greater number of institutions leads to the reproduction of data doubles, exemplified by monitoring of health records, financial transactions, travel information, communications information, legal records, and so on (Haggerty, 2006; Lyon, 2014). All of these genres of surveillance should be understood as deeply entangled through potential and actual exchanges of commercial, legal and technical information.” In other words, practices of “big data” aggregation in contemporary surveillance should be seen as a collective process with many actors (Lyon, 2014).

Nissenbaum (1997, 1999) argued that computational indexing and analysis enables disparate public records to be easily linked. Computation heightens the visibility of arrest records, birth and death records, marriage records, zoning and property records, and so on. Through their convergence, scattered data sources are organized and available to ordinary people through search engines and public records tools. For example, data convergence serves information technology companies that increasingly rely on advertising. Facebook purchases consumer data from data brokers including Doubleclick, First Impression, and OpenX to improve targeted advertisements for its users (Lunden, 2013). Facebook also purchases consumer loyalty card data to learn about the efficacy of their ads. By aggregating consumer purchase history and ad data, they check whether consumers actually bought in-store products after seeing an advertisement on the social network platform (Beckett, 2014). The collection, aggregation, and analysis of data introduce novel economic opportunities, often in contexts that are opaque or unanticipated to the subject of surveillance (Lyon, 2014). As Haggerty and Ericson’s (2000) analysis suggests, the interconnections between institutions conducting surveillance are often rendered invisible in contemporary systems of surveillance.

Since the September 11th attacks in 2001, the United States has dramatically expanded its

intelligence capacities to aid in counter-terrorism (Lyon, 2003). Masco (2014) argues that American political discourses position electronic surveillance as a strategic asset to preempt and combat terrorism, elevating online activities to a setting for existential crisis. Simultaneously, well before the September 11th attacks, surveillance scholars understood the potential for the decentralization and normalization of anticipatory surveillance practices. For example, Marx (1988) predicted the normalization of surveillance, suggesting that for law enforcement, future surveillance would become more preemptive than reactive. The presumption of “innocent until proven guilty,” he argues, is turned on its head in computational surveillance systems that gather data about individuals by default. The growth of computing in modern surveillance enables automated monitoring of massive populations without suspicion (Clarke, 1988). Modern surveillance is further characterized by the collection and storage of data (Clarke, 1988; Lyon, 2014). Simply to participate in public life requires the passive and active archival of people’s daily activities. Through the reappropriation and analysis of consumer data, contemporary U.S. surveillance transforms electronic records of ordinary citizens into objects of preemptive law enforcement and terror prevention (Masco, 2014).

In an environment where surveillance is ubiquitous, normalized, and has far-reaching political consequences, journalism is only one of many contexts where surveillance takes place. However, for many journalists, surveillance is not a remote abstraction but directly affects their work (Human Rights Watch & ACLU, 2014). In section two, I describe my methods for examining information security practices within journalism, and finally, I extract and discuss my findings.

Section 2. Findings

Chapter 3

Methods

In this chapter, I detail the methods used in my study of information security practices in investigative journalism. Between March 2014 and June 2015, I monitored ongoing developments in electronic surveillance and journalism through a wide range of information resources. I spent hundreds of hours learning about journalism and surveillance in the news, through information security and journalism conferences, technical reports, and reports on surveillance policy, and by speaking with journalists and press advocates themselves. Press advocates work with organizations that provide policy, legal, and technical support for journalists. I analyzed my interviews with journalists in relation to the ongoing news surrounding U.S. and global electronic surveillance.

3.1 Gathering Surveillance News

As a consequence of gathering interviews and information resources while developing this work, new developments in electronic surveillance news prompted regular iteration on my analysis. I therefore looked for persistent trends in electronic surveillance news involving journalists, particularly investigative journalists.

I gathered resources by following a wide range of traditional news organizations, as well as blogs and the websites of digital rights and press advocacy organizations. Those advocacy organizations included the Electronic Frontier Foundation, Freedom of the Press Foundation, the Open Technology Institute, and numerous others. I also closely monitored the news from publicly available online accounts of U.S. intelligence agencies, including the National Security Agency and the Office of the Director of National Intelligence (ODNI). For example, the ODNI uses social media sites (e.g., Tumblr: <http://icontherecord.tumblr.com/>) to publicize its transparency reports. Finally, I used Twitter to surface countless related articles each day shared

by digital rights activists, press freedom advocates, information security specialists, news professionals, news organizations, and think tanks.

With so many information resources, it may be unsurprising that the research required reading dozens of news articles nearly every day. Interviews with journalists were crucial to filtering analytically relevant information about electronic surveillance and information security practices, and to understanding conflicting perspectives about journalistic information security.

3.2 Interview Recruitment

I conducted semi-structured interviews with two types of participants with distinct perspectives: journalists and press advocates. In particular, journalists spoke about information security in their personal work, while press advocates shared trends they have observed in their work with journalists. I believe the high-level perspective of the press advocates closely complemented “ground level” activities of journalists themselves. I anonymized all interviews by default. Due to legal concerns, one reporter requested that I not identify them or their organization by name in the research. Barring few exceptions when I obtained explicit permission to quote participants by name, I refer to participants with pseudonyms.

In the formative stages of this research, I attempted unsuccessfully to recruit reporters involved in an investigative journalism organization called Investigative Reporters and Editors, Inc. (IRE). IRE advocates for high-quality investigative reporting and the rights of journalists. Among other information resources, IRE offers a listserv called IRE-L—a large electronic mailing list for exchanging information, resources, and advice between investigative journalists. For three weeks, I sent regular recruitment messages to IRE-L. While the recruitment emails did lead to informative discussions with journalists, some of whom I remain in correspondence with, the recruitment tactic failed to attract formal interviews.

Following the failed attempts with IRE-L, I instead reached out to reporters and advocates individually. I contacted members of dozens of news and advocacy organizations over the course of eight months between October 2014 and May 2015. I sent a scripted email with a personalized invitation to participate in the research to journalists' professional, publicly available email addresses. To focus on journalism organizations that examine national affairs, I primarily targeted national and international news organizations (e.g., the *New York Times*), as opposed to organizations that focus on local news. I also met and recruited reporters at journalism conferences. Whenever I was familiar with their reporting or advocacy, I was sure to acknowledge their work in my recruitment emails. The personalized emails were much more successful than my previous recruitment attempts.

A total of 20 journalists and 10 advocates agreed to participate in formal interviews for the research. Two of the advocates also identified themselves as journalists. The reporters come from news organizations including the *Washington Post*, the *New York Times*, the *Los Angeles Times*, the *Intercept*, *ProPublica*, the *Guardian*, *Wired*, *Fusion*, the *Daily Dot*, *Vice*, and the *Verge*. The interview participants included four independent journalists, at least six journalists who wrote with multiple organizations, and two retired reporters. Four journalists worked in academia, including two investigative reporters who are supported by academic fellowships, and two college professors, one of whom was retired from journalism while the other still reported actively.

The journalists worked across a variety of different beats, reporting on criminal justice, the Justice Department, national security, information security, business, and local topics in multiple cities across the United States. Many did not identify themselves with a specific beat, but instead focused on a variety of topics. Likewise, some reporters focus on specific regions

rather than bounded topics. They had a wide range of experience, including young fledgling journalists as well as senior reporters and executives. The group as a whole was highly decorated, including at least five Pulitzer Prizes and countless other awards among them.

I also spoke with press advocates and technologists whose organizations provide information and train journalists to use information security tools and techniques. The advocates come from multiple organizations, including the Electronic Frontier Foundation, the Freedom of the Press Foundation, the Committee to Protect Journalists, and the Open Technology Institute. The advocates were consistently well informed and were spread across various levels of seniority within their organizations. My interviews with advocates included technical analysts, legal and policy analysts, and executives.

Interviews lasted between 15 minutes and two and a half hours. All but one participant granted permission to record their interviews using a computer or portable recording device. I did not record or transcribe four interviews voluntarily, either due to privacy concerns with sensitive materials or to allow participants to speak more freely. I stored interview transcriptions on encrypted drives, and I backed up the encrypted drives using SpiderOak, a privacy-protecting cloud storage service.

My participants had tight schedules. Some journalists replied to invitations with suggestions for alternative interviewees because they did not have the time to participate. The journalists and advocates were routinely juggling events, and on several occasions had to reschedule to focus on an unanticipated news story. The reporters were beholden to the fast-paced news cycle, and nearly every interviewee was remarkably busy. Many regularly attended a variety of conferences, press events, and speaking events in between their reporting, investigations, and advocacy work. It was important not to misuse their time. It became

incredibly valuable for me to remember current events and history related to surveillance and journalistic security, allowing lengthy stories to become shorthand during the interviews. Because some interviewees had restrictive schedules, I attempted to accommodate their availability and condensed the interview questions as necessary.

Finally, I invited participants to speak with me using their preferred communication channels. I prepared encrypted text messaging applications, as well as encrypted audio and video chat tools. In the end, most of my interviewees preferred to speak using their landline office phone or a personal cell phone. I conducted two interviews through Skype and two interviews using Google Hangout. I also conducted three interviews using RedPhone, a mobile application for encrypted phone calls on Android, as well as one interview through encrypted email. Finally, I conducted two interviews on Jitsi Meet, a browser-based encrypted video chat application.

3.3 Interview Structure

I asked questions to better understand how journalists and press advocates perceive the impact of surveillance on their work, as well as details about their security habits. The semi-structured interviews examined three overarching questions with journalists: (1) What (if any) challenges are introduced into their work routine by electronic surveillance? (2) Are they doing anything to address surveillance? If so, what are they doing? (3) How do journalists perceive the potential changes in their work habits? I explored the same themes with press advocates by asking parallel questions about their work with journalists and trends they have observed. The journalists often spoke about their personal work and their colleagues' work. In contrast, many press advocates worked with journalists across diverse organizations (and were sometimes journalists themselves). Advocates offered observations of the reporters they have worked with.

I asked reporters about their personal work routines and occupational history, as well as

how their work fits into their broader organizations. I also asked how often their work involves connecting with sources. If they did work with sources, I asked how often their sources required confidentiality. I also asked about how they typically connected with their sources (e.g., over email), including strategies for source protection. My early questionnaire included questions to gauge participants' awareness of electronic surveillance, but it quickly became apparent that nearly all interviewees were well informed, and these questions rarely surfaced. I asked participants about their perspectives on U.S. surveillance programs, as well as whether they observed changes in their own organizations and in their personal work. Finally, I asked participants about the role of consumer information technologies in their workplace, and their concerns about the role of consumer technology in electronic surveillance. These specific questions helped me to understand how journalists and advocates conducted their work. I concluded each interview by inviting participants to ask questions. I asked interviewees if they were open to answering follow-up questions, to which everyone agreed. I followed up with roughly half of the participants at various points in the months following their interviews. I also asked participants to recommend others they thought I should speak with.

3.4 Limitations

Reaching out to journalists individually proved much more successful than recruitment through IRE-L, but there are clear challenges with my recruitment approach. One limitation to my recruitment strategy is that some journalists did not feel well informed enough about the topic to address it, or seemed to have qualms about sharing their concerns about surveillance. For example, a few potential interviewees declined to participate, noting that they wanted to help but did not know a lot about information security. I told the journalists that I wanted a range of perspectives for the research, but despite this reassurance, few who expressed reluctance

subsequently volunteered to participate in interviews. It is also possible that some of the journalists felt uncomfortable publicizing their views on electronic surveillance and would not speak about it unless they had a history of doing so on other occasions. Many of the journalists I interviewed have already spoken publicly on electronic surveillance issues, either in their own reporting or in previous interviews. It is therefore likely that this research overrepresents journalists who are knowledgeable about information security and who work in stereotypically sensitive reporting beats (e.g., national security). Nonetheless, the recruitment approach outlined here was successful for gathering a range of perspectives on journalistic information security, marked by many levels of familiarity with digital security, and conflicting visions of best practices.

3.5 Analysis

I analyzed my interviews using a grounded theory approach (Glaser & Strauss, 1967; Muller, 2014). I created an initial series of codes from my preliminary understanding of the conversations that focused on journalists' general perceptions about electronic surveillance and specific information security practices in their work. I repeatedly returned to these themes with branching subcategories of behaviors and perceptions. Through several iterations of coding, I identified trends in the journalists' information security habits and their motivations for using their particular approaches. I explore these findings through representative quotes from the journalists and press advocates.

3.6 Maintaining Confidentiality with At-Risk Populations

While confidentiality is a regular challenge in social science research, scholars must confront distinct issues with confidentiality while working with at-risk populations with serious privacy and security challenges. At-risk groups may face surveillance, physical and digital threats, or

undesired scrutiny of their work. Participation in research may ultimately be benign, but can also represent an unnecessary burden for at-risk groups. While most journalists were happy to participate in the research and to answer my questions, some were cautious about my intentions and the aims of this study. I've found it important to (1) build trusting relationships, (2) be selective about the information I publish, and (3) be careful about the data I collect and retain. I briefly outline issues that researchers should consider when working with at-risk groups.

First, to conduct research with at-risk populations, researchers must build trust and openness with participants. For populations that are cautious about electronic recordkeeping, participants may not feel safe or comfortable speaking openly. I deliberately withheld identifying information from my analysis, as well as security techniques that journalists preferred not to publish. The promise of anonymity and responsible disclosure of their information is profoundly important for enabling a sense of openness with participants. For example, I spoke with a handful of journalists who asked for assurances that I would destroy my interview recordings after I transcribed and anonymized the transcripts. I found that many participants were more comfortable speaking when they felt confident that their identity wouldn't be revealed through negligence or in publication.

Researchers have long confronted ethical challenges concerning when to withhold information about study participants from publication. Researchers must confront the potential that their publications could endanger participants, and must take appropriate precautions. For example, international activists may seriously endanger themselves by being identified in research. Correspondingly, these dangers lead participants to self-censor, or to decline to speak about certain topics regarding their methods and sources. Given the subject of the work, it is likely that many journalists preferred not to participate in the research altogether. The tensions

surrounding confidentiality and publicity represent serious challenges for researchers. For researchers to discern how to publish responsibly, research with sensitive populations requires intimate understanding of participants' situations, and in some cases, feedback directly from the participant. For example, I checked with certain journalists when I was unsure whether I should publish on sensitive topics about their sources. I usually found reassurance in my publication choices. Occasionally, I found that participants preferred to keep certain topics "off the record."

Beyond ethical decisions, researchers who work with populations under surveillance must also become vigilant stewards of participant data. In this research, I explore how companies can be easily subpoenaed to hand over user data, including the data of researchers. For that reason, it is vital to encrypt remote and local storage of interview data. Researchers should also be prepared to delete electronic records of their conversations with participants, including emails, text messages, and to the extent possible, phone records. Finally, researchers should be flexible with communication technologies and prepared to speak to participants however they feel most comfortable, including encrypted channels.

For research that involves populations under surveillance, issues of trust and openness, research ethics, and data stewardship intersect. With these constraints in mind, I first explore the legal and technical protections afforded to journalists and share the combined insights of my participants.

Chapter 4

Legal and Technical Protections for Journalists

“If you grant source anonymity, how do you actually guarantee that pledge if everything can be looked at by the government?”

– Former *New York Times* Executive Editor, Jill Abramson (*Journalism After Snowden*, 2014)

As digital communications are increasingly central to professional, social, and civic life, information security is a serious issue as investigative journalists connect with sources and research sensitive topics. Reporters must consider practical responses for keeping electronic records out of the hands of third parties, including direct interception by governments, companies, hackers, and others (Human Rights Watch & ACLU, 2014). To examine recent developments in journalistic information security, I introduce the legal and technical protections afforded to journalists, as well as the changing landscape of source protection in light of the ongoing revelations of government surveillance. I then explore key examples within the investigative journalism community involving American journalists and their sources, with a comparative analysis of journalism in non-Western countries. Finally, I describe challenges in maintaining source confidentiality, and conclude this section with an examination of modern information security techniques and tools.

4.1 Journalism, Surveillance, and the Law

Knowledgeable journalists who work with sensitive sources may reasonably assume that their communications are being gathered. They have good reasons to believe so; there exist well-documented cases when government surveillance authorities have been used against U.S. journalism institutions. In one of the most famous instances, the Associated Press (AP) had its phone records seized by federal investigators in 2013 as part of a leak investigation (Savage & Kaufman, 2013). Without notice to the AP itself, the Justice Department ordered phone

companies serving the AP to turn over phone records, including landline and cell phone data, over the course of two months. Because of the duration and the lack of notification about the collection, the AP expressed concern that the records would compromise information about its confidential sources (Savage & Kaufman, 2013). The telephone record seizure and several high-profile court cases highlight the limits of protections for U.S. journalists' communications. In turn, journalists with serious concerns about the safety of their sources take unilateral precautions to protect their sources. One might ask about the legal support for these surveillance practices.

U.S. surveillance laws are remarkably complex. As a consequence, I highlight only the legal context most central to law enforcement investigations that may directly involve journalists and whistleblowers. However, some of the law is also unclear to the general public. In the interest of maintaining the intelligence community's strategic advantage over adversaries, some U.S. surveillance programs rely on secretive interpretations of the law that can be hidden from the public. I therefore discuss related law as well as legal ambiguities. To explore these ambiguities, I highlight stories of whistleblowers who have spoken out against, or directly exposed, U.S. government and corporate surveillance where it has been obscured.

In the United States, privacy laws are built on the foundation of the Fourth Amendment and have always been strongly influenced by advances in technology. The right to privacy was first defined by British common law as, "only the physical interference of life and property," a standard that is increasingly complicated when property is represented by immaterial data. In the late 1800s, Samuel Warren and (later, Supreme Court Justice) Louis Brandeis wrote one of the most influential essays in American legal scholarship. "*The Right to Privacy*" (Warren & Brandeis, 1890) examined privacy in the context of then-emergent printing press and photographic technologies during the industrial revolution. As opposed to older, unwieldy

cameras, the handheld camera quickly emerged as an inexpensive consumer product that could be used to create spur-of-the-moment images. These technologies, they argued, require a new understanding of privacy beyond physical encroachment:

Now that modern devices afford abundant opportunities for the perpetration of such wrongs without any participation by the injured party, the protection granted by the law must be placed upon a broader foundation. (Warren & Brandeis, 1890)

Harkening back to British incursions on American households, Warren and Brandeis argued that the right to be let alone, as established in the Fourth Amendment, should be considered well beyond physical incursion. They argued for the legal recognition of information about “the private life, habits, acts, and relations of an individual,” particularly in light of the growth of the printing press and camera technologies. More than a century later, Warren and Brandeis have proven prescient in an environment of widespread digital consumer technologies with far-reaching privacy implications for both citizens and the press.

First Amendment press protections have been developed through hundreds of years of court decisions on press freedom, and have been particularly well supported in the 20th century (Youm, 2009). The U.S. Supreme Court case *Near v. Minnesota* (283 U.S. 697, 1931) held that “prior restraint”—preemptive government censorship of publications—is unconstitutional, except in highly constrained circumstances. *Near* and numerous previous cases have allowed newsrooms to publish even extraordinarily sensitive information when deemed in the public interest, including classified government documents. In a landmark 1971 case, the U.S. Supreme Court held that the *New York Times* and *Washington Post* were free from prior restraint in their publication of the Pentagon Papers (*New York Times Co. v. United States*, 403 U.S. 713). The freedom from prior restraint allows American journalists to operate with relative autonomy.

While the government cannot unilaterally prevent news organizations from publishing

information, the U.S. officials can levy serious punishments for doing so. The government can take punitive action against government employees who share information with reporters. Those government employees can be held criminally liable for sharing national security secrets without authorization (Policinski, 2014, p. 68). The government may demand that reporters disclose information about their sources in such cases, but most states recognize a reporter's privilege to withhold confidential information, including information about their sources under "shield laws." As of 2014, 40 of the states and the District of Columbia have shield statutes, while at the federal level no such protections exist (Reporters Committee for Freedom of the Press, 2014). A reporter's privilege is not absolute. In *Branzburg v. Hayes* (408 U.S. 665, 1972), the Supreme Court held that "the First Amendment does not protect a reporter's right to conceal criminal conduct by refusing to answer a grand jury's questions, and consequently the First Amendment does not establish an unqualified reporter's privilege, at least not in the context of a grand jury investigation." (Lerner & Bar-Nissim, 2014) While the law does not prevent journalists from taking the stand, an alternative norm emerged in courts—prosecutors side-step the testimony of reporters (Carlson, 2011, pp. 8-9). Instead of seeking reporter testimony, increasingly, prosecutors seek data that can demonstrate their claims.

Electronic records (e.g., phone call metadata) provide sufficient evidence to link a journalist to a source. U.S. agencies generally have the authority to compel corporate entities (e.g., phone companies) to give electronic records to the government, including information about electronic communications under multiple authorities. The government does not need to ask a journalist to disclose information about confidential sources if the government can instead obtain a subpoena for the records, and deliver the subpoena to the company that manages the relevant records. In other cases, the government collects information with potential intelligence

value preemptively—that is, without demonstrating evidence of criminal wrongdoing and obtaining a warrant for specific investigations from a court judge. Furthermore, in “bulk collection” programs, the government interprets legal standards for “relevance” quite broadly, enabling the collection of data about countless Americans with no ties to criminal wrongdoing.

For the moment, surveillance laws that involve business records are built on foundations introduced in the 1960s and 1970s. The 1967 U.S. Supreme Court case, *Katz v. United States* (389 U.S. 347), examined the legal definition of a “search” of information. The court established the “reasonable expectation of privacy” test to determine whether certain types of information should be protected under the Fourth Amendment. However, in the criminal case *Smith v. Maryland* (442 U.S. 735, 1979), the Supreme Court reaffirmed that law enforcement could intercept call records without a warrant because the caller forgoes any reasonable expectation of privacy by providing communications records to a third party—the phone company. The principle that people have no reasonable expectation of privacy when they route information through an outside party is now known as the “third party doctrine,” a concept that has become the cornerstone for modern interpretation of Fourth Amendment protections for consumer data in courts (e.g., Kerr, 2012; Newell, 2013; Newell & Tennis, 2013). Courts have generally held that customers forfeit Fourth Amendment privacy protections when sharing information with a business.

Despite the considerable changes in American life introduced by the proliferation of information and communication technologies, citizens continue to live with legal vestiges that suggest Americans have no expectation of privacy when their digital communications are supported by a business or other third parties. When browsing the Web, nearly all information that a user accesses or provides will be housed on a third party server. Because a person may

assume that their data will be private when using the Internet, when sending an email or conducting a Web search, for example, scholars have argued that these laws may be inappropriate for modern consumer technologies (Kerr, 2012; Nissenbaum, 1997, 2004).

The government has broad authority for investigating potential criminal activities and internal leaks. In the United States, law enforcement and the government have three primary categories (Lerner & Bar-Nissim, 2014) of legal tools at their disposal to investigate whistleblowing and leak cases:

- 1) Law enforcement can compel recipients of leaked information to disclose information through a traditional subpoena or search warrant.
- 2) Surveillance in an ongoing investigation can be conducted through specific laws, such as the Electronic Communications Privacy Act of 1986 (ECPA), an amendment to the older Wiretap Act. ECPA requires court authorization to intercept wire, oral, or electronic communications.
- 3) Authorities may retrieve information from third parties related to leaks through a subpoena, search warrant, or a court order as authorized by specific laws (e.g., the Stored Communications Act).

While their interpretation is the subject of perennial debate among practitioners and legal scholars, the First and Fourth Amendments generally serve to constrain surveillance of Americans. Separate laws govern the collection of foreign intelligence data.

In practice, foreign intelligence data can involve Americans quite often. The Foreign Intelligence Surveillance Act of 1978 (FISA) outlines procedures for U.S. federal intelligence agencies to gather electronic records related to foreign targets. Under FISA, the government established the Foreign Intelligence Surveillance Court (FISC) to oversee federal intelligence

and law enforcement communities, including the NSA and the FBI, intending to curb decades of Cold War-era spying on American civil rights leaders and ordinary citizens. A FISC judge must approve a warrant to request data related to Americans as part of foreign intelligence surveillance. That is, the intended role of the FISC is to provide authorization for electronic surveillance through court orders. However, between its first full year of operation in 1979 through 2014, the Court received over 35,000 requests for warrants and rejected only 12 (Electronic Privacy Information Center, 2014). In other words, the court has almost never rejected a request for a court order from the intelligence community. Due to the sensitive nature of its work, the FISC does not disclose its deliberations publicly. In a strict sense, U.S. intelligence activities are authorized. Simultaneously, authorization for intelligence activities takes place with little public oversight, and the FISC is unambiguously one-sided in its deliberations.

Shortly after the attacks on the World Trade Center in 2001, the U.S. government immediately began removing long-held intelligence constraints under rules governed by the FISC (Office of the Director of National Intelligence, 2013, 2014). The intelligence powers of the NSA dramatically expanded under the Bush and Obama administrations to include an unprecedented volume of personal data belonging to Americans, compounded by the widespread adoption of computing technology on the consumer and enterprise level. Intelligence agencies governed by the Department of Defense, notably the NSA, were granted formal authority to target communications (e.g., phone and Web activity) of people known to be in the United States as part of counter-terrorism efforts. In 2001, the program was authorized as the “Terrorist Surveillance Program,” and with similar legal support, the program was renewed under the FISA Amendments Act of 2008. Compared to earlier laws, the government’s legal and technical

surveillance authorities developed rapidly, without public coverage or debate.

In the decade following September 11th, 2001, hints of government surveillance activity surfaced in courts but the authorization for those programs was unclear to the public. For example, an AT&T technician named Mark Klein found evidence that the NSA was gathering Web traffic in warrantless, bulk surveillance over AT&T's fiber optic cables. Klein provided documentation supporting his claims to the Electronic Frontier Foundation, showing that the NSA tapped the company's fiber optic cables to copy traffic passing through a hidden room in Klein's San Francisco AT&T offices (Electronic Frontier Foundation, 2015a). Furthermore, Klein said that similar rooms exist in AT&T facilities around the country. Although it is not clear how the government used its access in practice, as far back as 2001 the government had access to physical checkpoints for global Web traffic (Kravets, 2009, 2013). With Klein's evidence in tow, the EFF brought suits against AT&T and the government in multiple cases (Electronic Frontier Foundation, 2015a), including *Hepting vs. AT&T* (2006) and notably, *Jewel v. NSA* (2008). *Jewel* asserted that the government was conducting broad surveillance of so-called "UPSTREAM" Internet traffic—effectively everything that a person can do on the Web. Concerned with revealing national security secrets, the government has asserted a state secrets privilege in *Jewel* and countless other cases, persuading courts to remove classified and privileged evidence.

For some in the intelligence community, it became abundantly clear that reform would not take place within the courts. A growing chorus of NSA whistleblowers, including Thomas Drake, William Binney, Kirk Wiebe and Edward Loomis, among others, worked within the established channels for intelligence whistleblowers to highlight potential legal issues as well as inefficient programs (Harris, 2012; Shane, 2010). For example, an NSA senior executive named Thomas Drake and his whistleblower colleagues worked with the NSA and Pentagon Offices of

the Inspector General (OIGs) to highlight mismanagement of costly and ineffective programs. Although Drake moved through official channels, the OIG later reported Drake to the FBI as part of an unrelated criminal leak investigation (Devine & Katz, 2014). “Drake and his whistleblowing partners all faced FBI raids at gunpoint in which their homes were ransacked, property seized, and families terrorized” (p. 104). Drake spoke to a reporter with the *Baltimore Sun* about misconduct within the NSA but maintains that he did not share classified information. The government indicted Drake under the Espionage Act for 10 different charges, for which Drake faced up to 35 years in prison (Nakashima, 2010; Shane, 2011). Drake pleaded guilty to a much smaller misdemeanor and served no jail time (Shane, 2011). He went bankrupt in the process and lost his job and his wife (Devine & Katz, 2014). Drake’s story provided an example to later intelligence whistleblowers.

In later testimony to the European Parliament, Edward Snowden recounted the story of Drake and his colleagues (Peterson, 2014). Snowden first worked through official channels to raise concerns about the legality and efficacy of certain NSA activities, but officials did not respond to his concerns. In private, he spoke with co-workers about his anxieties. “The first were well-meaning but hushed warnings not to ‘rock the boat,’ for fear of the sort of retaliation that befell former NSA whistleblowers like Wiebe, Binney, and Drake” (Peterson, 2014). In other words, in the case of Drake and his colleagues, the official whistleblowing channels appeared ineffective at promoting change, and in fact, appeared to instigate a backlash within the ranks of the intelligence community.

In June 2013, news organizations began to publish a stream of stories detailing the U.S. intelligence community’s global surveillance infrastructure based on internal documents that Snowden relayed to news organizations. The earliest reports by the *Guardian* and the

Washington Post detailed the NSA's technical capabilities to intercept electronic communications. The disclosures detailed the inner-workings of dozens of intelligence programs such as PRISM, a program that authorized the NSA to access users' personal data stored by the largest American technology companies, including Google, Apple, Facebook and Microsoft (Gellman & Poitras, 2013; Greenwald & MacAskill, 2013). A parallel program named MUSCULAR allowed the intelligence community to unilaterally access Google's and Yahoo's user data by hijacking the unencrypted information flowing between their data centers (Gellman & Soltani, 2013). The documents also reveal the bulk collection of American and foreign phone metadata (Devereaux, Greenwald, & Poitras, 2014; Gordon & Mendoza, 2014; Savage & Wyatt, 2013), political and technical efforts to subvert encryption for mobile and Web communications (Ball, Borger, & Greenwald, 2013; R. Gallagher, 2014; Larson, Perlroth, & Shane, 2013; Scahill & Begley, 2014), the stockpiling of unpatched computing vulnerabilities (Fung, 2013; R. Gallagher, 2014), and the pervasive collection of Web traffic around the globe (Greenwald, 2013a).

Not long after Snowden's disclosures of NSA activities, whistleblowers began to crop up in other areas of the government, revealing further U.S. surveillance authorities. In a 2014 *Washington Post* editorial, a State Department whistleblower named John Napier Tye described one of the chief intelligence authorities, an Executive Order signed by President Reagan in the early 1980s. Executive Order 12333 authorizes intelligence agencies to gather the content of Americans' electronic communications—for example, the content of emails—even if the U.S. person is suspected of no wrongdoing (Tye, 2014b). Under the Executive Order, the data may be retained for no more than five years. While a court order is normally required to directly target an American for surveillance, a court order is not necessary if an American's communications

are collected “incidentally” when investigating data housed outside of the United States. In other words, the intelligence community is authorized to look for the foreign targets, which may include data about Americans in the process.

In practice, it is quite difficult to discern the “nationality” of data. When the government was armed with its newfound surveillance authorities in the early 1980s, intelligence officials probably could not have foreseen the globalization of the Internet and the explosion of mobile telecommunications across international boundaries. Today’s Web and mobile technologies muddy the distinction between American and foreign data, where a single person’s data can be sitting in multiple countries simultaneously. For example, multinational companies like Google host content (e.g., a user’s emails) that traverses U.S. borders and resides on Google’s servers in numerous countries. In those countries, American data can look quite similar to foreign data.

The Reagan-era Executive Order introduces a “legal loophole that can be stretched very wide,” according to the State Department whistleblower John Napier Tye. In a separate talk, he elaborated with an example:

They could have just a single legitimate foreign target. So, one person overseas, who is using all of these services—Gmail, Hotmail, Twitter, OkCupid, whatever it is. And they don’t just go and take that one person’s data. They take all of the data from all of those services, for all of the users. So you could, in theory—and it’s not that far from this—have just a single foreign target and then collect three or four billion people’s data. And all of the rest of that, those three or four billion people, would be incidental collection. (Tye, 2014a)

A second program provides a hodgepodge of more specific U.S. surveillance authorities. Under section 702 of the Foreign Intelligence Surveillance Amendments Act, the government is authorized to collect virtually everything that a user does through physical taps on the fiber optic cables that transmit data across the Web. The intelligence community has called this capability “upstream” surveillance (Timberg, 2013). The same authorities allow the government to monitor

the phone calls of U.S. and international targets, as well as to conduct targeted surveillance with the legal compliance of large information technology companies through the PRISM program.

Finally, on the heels of the September 11th attacks, U.S. intelligence authorities collected virtually all American telephone call records under section 215 of the USA Patriot Act. The law is quite open-ended, authorizing the collection of “tangible things” related to an ongoing counter-terror investigation. Tangible things could include “books, records, papers, documents, and other items,” as well as a wide range of consumer data. The FBI has used the Patriot Act to gather “large collections” of Americans’ business records as part of terror and espionage investigations (Ackerman, 2015). These records may contain information about ordinary citizens, for example, medical records and tax information. Importantly, the Patriot Act enabled the NSA to collect Americans’ phone metadata in bulk, including conversational participants and the time and duration of Americans’ calls (Gordon & Mendoza, 2014; Greenwald, 2013b).

Privacy and civil liberties groups found the government’s activities troubling because of the unprecedented scale of their phone metadata collection. By chaining calls in multiple “hops” from the original target, the government intended to construct networks of potential terror suspects. However, people call not only relevant actors, but also countless extraneous civilians, businesses, and organizations with no connection to a terror investigation. In other words, the Patriot Act inevitably connects call records of legitimate suspects to unrelated, innocent civilians.

At the time of this research, nearly two years after the ongoing government intelligence leaks began, the laws governing electronic surveillance in the United States faced minimal legal challenge. Federal intelligence and law enforcement groups under the Obama administration argued that the programs are crucial for safeguarding national security. For example, FBI director James Comey and senior intelligence officials—ex-NSA director Michael Hayden, and

Director of National Intelligence James Clapper—advocated for surveillance powers in the interest of preempting terrorist and criminal activities.

At the time of this research, most of the intelligence programs described here faced few serious legal challenges in courts and in congress. The Patriot Act is the single exception.

Section 215 of the Patriot Act, the provision authorizing bulk collection of Americans' phone metadata, became the target of government-appointed review groups following Edward Snowden's disclosures. In January 2014, the White House-appointed Privacy and Civil Liberties Oversight Board released an independent report recommending that the Obama Administration abolish the bulk telephone record program, citing its minimal role in preventing criminal threats while collecting "billions of records per day with full knowledge that virtually all of them are irrelevant" (p. 73, Privacy and Civil Liberties Oversight Board, 2014). At most, it is possible that the program may have been useful in one investigation—a case where it was nonetheless unclear that the phone records were necessary (Schwartz, 2015).

In early 2014, the Obama Administration signaled that it would constrain the scope of the phone metadata program (Office of the Press Secretary, 2014a, 2014b), and in early 2015, the intelligence community announced that it would no longer request authorization for the program (Office of the Director of National Intelligence, 2015). In May 2015, a federal appeals court ruled that the Patriot Act did not, in fact, authorize bulk phone metadata collection, suggesting the program was illegal (Savage & Weisman, 2015). In other words, an Executive-appointed review group found the program ineffective, the intelligence community deemed the program unnecessary, and courts deemed the program illegal. In June 2015, the U.S. congress finally discontinued the bulk phone metadata program, marking the first time that surveillance authorities had been weakened since the foundation of the Foreign Intelligence Surveillance

Court in 1978. While advocacy organizations such as the Electronic Frontier Foundation touted the event as a victory (e.g., Jaycox & Kayyali, 2015), other forms of surveillance authorization faced no serious challenges in courts or on the congressional level. In the end, the far-reaching surveillance laws have seen modest reform.

4.2 Government Whistleblowers and Leakers

Several court cases and seizures of journalist data demonstrate the limits of legal protections for journalists' communications. Protections for members of the press, however, differ in countries around the world. In an increasingly networked world, with journalists connecting to sources outside of their own countries, source protection plays out quite differently in many regions. I highlight examples of the legal protections of journalists within the United States, as well as the legal vulnerability of their sources.

Source protection directly relies on individual journalists to manage their communications and personal relationships (Carlson, 2011a; Powers & Fico, 1994; Reich, 2011a). For example, journalists who work on national security issues have long worked with government sources (Hallin et al., 1993). Those sources may prefer to speak confidentially when sharing their misgivings about government activities with a reporter. Peter Maass, a reporter with the *Intercept*, describes the relationship accordingly (Maass, 2015a):

There is a time-honored way in government for mid-level experts to convey their worries that high-level officials are misguided—they talk to reporters to raise an alarm outside the walls of whichever department they work for. This is why confidential conversations in Washington seem to take place in parks and restaurants and store aisles as much as they do in actual offices. These conversations can serve as a check on the official statements that portray prevailing policies as wise and successful, even when they are not.

According to Hencke (2000), journalists often prefer to work with a network of moles who can provide different types of information to help understand the contours and details of a story.

When sources wish to speak off-the-record or remain anonymous when sharing information with a reporter, the journalist usually takes those requests quite seriously (Keeble, 2008).

A source can put him- or herself at legal risk by disclosing sensitive information in violation of binding agreements as an employee (e.g., non-disclosure agreements), or as a citizen in violation of the law. While a thorough treatment of the history of legal cases for leakers and whistleblowers warrants its own volume, for the purposes outlined here, I offer a narrow window into cases involving high-profile leaks. Some of the most high-profile cases against leakers and whistleblowers who share information with journalists have been pursued under the Espionage Act of 1917, a World War I era law that was intended to help prevent the delivery of privileged national defense information to foreign adversaries. The broad law made sharing information that interfered with U.S. military operations (or aided enemies) punishable by death or imprisonment for up to 30 years (Edgar & Schmidt, 1973; Lerner & Bar-Nissim, 2014). Yet, instead of foreign adversaries, in recent decades the law has also been used to pursue criminal cases against U.S. government leakers and whistleblowers who share privileged information with journalists and the public (Rafsky, 2013, 2014). Perhaps the most famous Espionage Act case involved Daniel Ellsberg and Anthony Russo in their publications detailing the Pentagon Papers in the early 1970s, revealing decades of covert American political and military influence over the development of South Vietnam's government amid Western fears of communism.

In recent years, the Obama administration's Justice Department has used the Espionage Act in an unprecedented crackdown on unauthorized information leaks that allegedly harm national security (Rafsky, 2013, 2014). At the same time, many leaks are entirely sanctioned by the government, problematizing the narrative that leaks are a danger to national security. As a matter of routine, U.S. agencies allow sanctioned leaks of classified information to the press. For

example, in a critique of the government's strategy to crack down on whistleblowers, Maass argued (2015b):

Classified information is regularly leaked by government officials who want to make themselves or the government look good. Such "authorized leaks" are rarely prosecuted. For instance, an array of highly classified information about the killing of Osama bin Laden—which made the Obama administration look resolute and militarily effective—was leaked to the press and no one was punished in connection with the leaks.

In other words, the Espionage Act and parallel laws have been used to punish leaks quite selectively. For national security reporters and journalists who routinely work with sensitive sources, cases involving the Espionage Act became the subjects of profound scrutiny (e.g., Wemple, 2014). Out of journalists' concern for their own ability to connect with sources, the Espionage Act cases have come to represent the most serious risks faced by potential leakers and whistleblowers. I briefly outline a few recent cases involving the Espionage Act.

4.2.1 Key Espionage Cases

In 2006, *New York Times* reporter James Risen published *State of War*, a book detailing covert government activities in wars overseas. In one chapter of the book, Risen revealed a Clinton-era Central Intelligence Agency plan to sabotage Iran's nuclear development program by providing it with faulty blueprints. However, their plan backfired, in fact accelerating the program's development when the blueprint's flaws were noticed and corrected.

In 2008 and 2010, Risen was subpoenaed to testify on the case and reveal his sources for the book chapter, and he refused through a long series of court appeals. Finally the Supreme Court rejected his appeal in June 2014 (Liptak, 2014; Savage, 2010), opening Risen to potential time in jail for refusing to reveal his sources. In early 2015, Risen's legal battle finally came to an end when the Justice Department decided to cease pursuing Risen's testimony against his alleged source (Apuzzo, 2015a). However, they did not need his testimony to convict the

purported source—an ex-CIA agent named Jeffrey Sterling. The government intercepted emails between Risen and Sterling, who was later charged and convicted under the Espionage Act (Apuzzo, 2015b). Government agencies cite national security concerns in response to sensitive government leaks in cases relating to foreign military and intelligence operations. The Committee to Protect Journalists (Rafsky, 2013, 2014) documented the Obama administration’s trend of charging numerous leak cases similarly, prosecuting more leakers and whistleblowers under the Espionage Act than all previous administrations combined (Wemple, 2014). As a journalist, Risen had considerable legal protection, but his alleged source did not. While his sentence was significantly shorter than the 19-to-24 year prison sentence that government prosecutors initially envisioned, Jeffrey Sterling will still serve three and a half years in federal prison (Maass, 2015b).

James Rosen, the chief Washington correspondent for Fox News (with a remarkably similar name to Risen), in 2009 reported how U.S. intelligence learned that North Korea planned to escalate its nuclear program in response to sanctions by the United Nations. In response, the Justice Department began an investigation of Rosen in 2010, tracing email exchanges and phone call records between Rosen and Stephen Jin-Woo Kim, a State Department analyst. The Department named Rosen a “criminal co-conspirator” in a case against Kim, yet the government employee did not have the protections that Rosen enjoyed as a member of the press.

At the time, Rosen’s report was widely panned as unsurprising in light of North Korea’s posturing on nuclear sanctions. When the government took Kim to court, *Mother Jones* published an article describing the case, titled “How the World’s Dullest Story Became the Target of a Massive Leak Investigation” (Drum, 2013) while Jon Stewart ridiculed the case on the *Daily Show*, revealing the headline of Rosen’s article to the audience. “That’s it?” Stewart

asked. “That’s the leak they needed to quash? North Korea to answer sanctions with more nuclear tests? North Korea answers everything with more nuclear! They have a nuclear-test-based economy!”

While the story may not have shocked the general public, the Obama Administration pursued the case against Kim aggressively. Kim’s family exchanged nearly all of their assets to pay for his legal defense. For Kim’s family, the case became all-consuming. Kim’s sister set up a legal defense fund, enlisting help from friends and supporters. Kim’s wife and young son left him, returning to relatives in South Korea. He became depressed, and in his own words in a profile by the *Intercept*, “Every single day, I thought about killing myself.” (Maass, 2015a) Kim was later indicted and charged under the Espionage Act.

Rosen spoke with government employees regularly—indeed, the practice is commonplace for investigative journalists covering the Department of Justice, national security, and other areas with access to potentially classified information. Rosen’s and Risen’s cases have both sparked enduring conversations in the journalism community about the extraordinary difficulties faced by sources who speak with journalists, particularly when involved in government positions with access to privileged information. The Obama administration has aggressively pushed to prosecute government leakers and whistleblowers and makes regular use of targeted digital surveillance as part of investigations of journalists’ communications with whistleblowers.

It is important to emphasize that many leaks, including espionage cases, take place outside of traditional journalistic outlets. In one important case, Chelsea (formerly Bradley) Manning was sentenced to 35 years in prison for leaking a cache of U.S. military and State Department documents to the document-sharing website WikiLeaks in early 2010. The

documents included video recordings depicting U.S. military airstrikes on civilians in the Afghani village of Granai in 2009, and the 2007 bombings of Iraqi civilians in Baghdad during the wars in Iraq and Afghanistan (Savage, 2013; Tate, 2013). Manning was exposed through chat logs with a confidant who later testified against her. Traditional journalistic outlets certainly have no monopoly on leaks, and indeed, Web platforms democratize publishing opportunities for would-be leakers and whistleblowers. Nonetheless, journalists are clearly intertwined with sensitive disclosures of U.S. military and intelligence activities as well as less stereotypically sensitive areas of reporting.

4.3 Surveillance Across Borders

While controversies surrounding press rights in the United States abound, American journalists have considerable legal protections and independence compared to most of the world. For comparison, Reporters Without Borders produces an annual *World Press Freedom* index that ranks government support for journalism in 180 countries on six measures: pluralism of opinions represented, media independence, degree of self-censorship, effectiveness of legislative frameworks, institutional transparency, and support for news infrastructure (Reporters Without Borders, 2014). Following the Snowden disclosures, the U.S. fell from rank 33 in 2013 to 46 in 2014, and fell further to 49 in 2015 (Reporters Without Borders, 2015) due to the growing number of cases against journalists pursued by the Justice Department. The report attributed the descent in ranks to legal reprisal against Edward Snowden and Chelsea Manning, as well as the arrests of at least 15 journalists covering the protests of law enforcement violence in Ferguson, Missouri in 2015. The index ranked many Western European countries well above the United States, with Finland, the Netherlands, and Norway consistently ahead of other nations. Conversely, a few countries with tightly controlled state media —Turkmenistan, North Korea,

and Eritrea—routinely score at the bottom of the index.

The Committee to Protect Journalists found that in 2014, China imprisoned the highest number of journalists in the world (44), followed by Iran (30). Their numbers combined account for roughly one third of the world's jailed journalists (Committee to Protect Journalists, 2014a). In some countries ranking low on the Press Freedom Index, sources and journalists risk physical attacks or risk being killed. The CPJ also produces an annual report detailing the number of unsolved murders of journalists in countries around the world (Committee to Protect Journalists, 2014b). Their work suggests that journalists are most likely to be victims of an unresolved murder in the Middle East and North Africa, as well as in Central and South America.

Government pressure on journalists is further compounded by the growth of consumer surveillance technology. Under authoritarian regimes, journalists are being targeted in local and state law enforcement attacks that make use of commercially available surveillance products. Researchers at the University of Toronto's Citizen Lab (Marquis-Boire et al., 2013) examined the emergence of the global commercial surveillance industry. A handful of companies sell their hacking technology to countries and law enforcement groups that otherwise lack the technical expertise to develop sophisticated exploits to break into remote computers. In 2013, commercial surveillance tools enabled governments and law enforcement to monitor Skype calls and cell phone calls, and to spy on a target through the target's computer webcam or microphone, complete with dedicated customer service support. Marquis-Boire and his colleagues (2013) argued that the market for commercial surveillance software is dominated by very few companies, notably Gamma International, Vupen Security, and Hacking Team. The companies describe their tools as a solution for monitoring criminals and terrorists. However, Citizen Lab found that the intrusion software has been used to conduct remote surveillance of Moroccan

journalists and London-based Bahraini activists—people who do not appear obviously related to terrorist groups (Marquis-Boire et al., 2013).

Commercial surveillance tools are used by an unknown number of governments. Due to the secrecy of the vendors, the software is rarely caught in action. However, Citizen Lab showed that Gamma International’s FinFisher software relayed data about targets back to servers in 25 countries around the world. Citizen Lab’s work highlighted the role of commercial surveillance software in several countries, notably Ethiopia (Marczak et al., 2014), Bahrain, and the United Arab Emirates (Marquis-Boire et al., 2013) where the tools are used to monitor human rights activists, dissidents, and journalists.

Western journalists are not necessarily safer than foreign journalists from digital attacks coordinated by outside countries. In an analysis of documents released by Edward Snowden, on January 19th, 2015, the *Guardian* reported that in the month of November 2009, the British Global Communications Headquarters (GCHQ) intercepted over 70,000 emails including some from addresses at the *BBC*, *Reuters*, the *Guardian*, the *New York Times*, *Le Monde*, the *Sun*, *NBC* and the *Washington Post*. The agency intercepted the emails through taps on fiber optic cables as part of a training exercise. The GCHQ subsequently shared the emails on its intranet. The *Guardian* suggested there were no indications of whether journalists were intentionally targeted. Their report revealed that the GCHQ compares the information security threat posed by investigative journalists as comparable to “terrorists” and “hackers.” The internal documents read, “journalists and reporters representing all types of news media represent a potential threat to security,” going on to say:

Of specific concern are ‘investigative journalists’ who specialize in defense-related exposés either for profit or what they deem to be of the public interest. All classes of journalists and reporters may try either a formal approach or an informal approach, possibly with off-duty personnel, in their attempts to gain official information to which they

are not entitled.

The GCHQ is a close ally of the United States' intelligence community, but that does not appear to prevent the agency from conducting surveillance exercises that include American journalists. It is unclear whether the GCHQ targeted journalists' communications or whether the emails were gathered incidentally. The GCHQ story suggests that American journalists have strong constitutional protections as a matter of policy, but in practice, the barriers to data breaches are limited. The story further demonstrates that there is little to stop a capable foreign country from intercepting journalists' electronic communications, given sufficient knowledge and resources.

By now, we have outlined the serious legal threats that journalists face in their reporting. To be sure, American journalists have considerable legal protections, and it is important to maintain perspective about American press freedom by considering the conditions for journalists in non-Western countries. American journalists and their sources face serious legal harassment. In volatile regions, however, journalists and their sources may face physical violence or death for their activities, particularly in climates of tightly controlled news media. Acknowledging the legal limits for source protection, U.S. journalists cannot rely on the law alone to speak with their sources in confidence. Journalists also use technology to protect their sources.

4.4 Methods to Keep Sources Confidential

Electronic records increasingly document information about locations and personal interests, and identifying information about communications. In the aggregate, that data can be used to determine information about sources and to infer the future actions of journalists. In their personal lives, journalists face many challenges that mirror those of ordinary citizens. However, as their work and personal lives depend on networked technology, they necessarily leave an enormous volume of electronic records. Phone calls, text messages, cell phone tower

connections, GPS, emails, social media, and Web messaging platforms all leave records that can be used against sources. The growing centrality of Web communications complicates the nature of source protection by introducing technical challenges for journalists. They may use encryption to scramble their communications, may avoid using electronic communications, and when appropriate, may manipulate their electronic records to provide misleading information (Human Rights Watch & ACLU, 2014; Pew Research Center, 2015).

On November 7th, 2014, the Freedom of the Press Foundation and Open Technology Institute held a *News Organizations and Digital Security* conference. At the conference, several prominent reporters spoke at length on the evolving landscape of source protection (Real-World Encryption Problems, 2014). The reporters included Dana Priest, Julia Angwin, and James Risen, as well as Chris Soghoian, a senior technologist with the ACLU. Priest, a seasoned journalist with the *Washington Post*, suggested that younger reporters have become accustomed to using Web technology to speak with sources but should not become dependent on these tools because a sensitive source may not trust the software or feel comfortable using it. Many sources will be concerned that encryption will make them appear suspicious, and are otherwise unfamiliar with the tools. Angwin, a reporter with *ProPublica*, joked that asking unfamiliar sources to use encryption is “like asking for sex on the first date,” to illustrate how encryption can be jarring for sources. “The problem is that if you ask on the fourth date, it’s too late. There’s already a digital trail.” *New York Times* reporter James Risen joked along similar lines, “If you’re trying to develop a source, and if you say it would really be good to have encrypted conversations because what we’re going to do is very dangerous to you, that’s not very good advertising.”

To avoid relying on Web communications, Dana Priest stressed the need for reporters to

be imaginative in their security techniques, recounting how she has hidden her phone activities by visiting businesses to call sources, with a list of contacts in tow. In her experience, a source may also feel more comfortable if he or she is not the only person being contacted. She suggests producing many data trails by contacting several potential sources for a single topic or piece of information. However, at the close of the panel, the reporters unanimously agreed that meeting in person is still the best way to exchange sensitive information with sources. Meeting in person, they agreed, enables reporters and sources to speak in confidence, and allows journalists to verify the legitimacy of a source.

The security benefits of meeting in person only work if the source and journalist also avoid being connected through their electronic records. Knowledgeable and security-minded journalists may exploit their data trail to provide misleading information. For example, journalists may leave their personal cell phones at home, or with a friend while meeting a sensitive source to provide a false data trail. Even if a source is identified in their communications with a journalist, it can still be valuable to provide misleading electronic records. Some journalists will use an innocuous “cover story” to arrange meetings in public places, stating false motives for the meeting in their communications.

Journalists have a variety of tricks for securing their communications with sources and managing their personal data. Security specialists also recommend and provide training for standardized security methods.

4.5 Threat Modeling and Security Tools

Journalism organizations promote information security education through extended training on information security tools and techniques (Henrichsen et al., 2015; Walker & Waters, 2015). Additionally, press freedom, human rights, and electronic policy advocacy groups have been

powerful contributors to media outreach, information campaigns, and research on the challenges that electronic surveillance creates for journalists and civilians. These advocacy organizations also promote education by providing detailed guides and training on digital security for journalists. For example, Micah Lee, a technologist who was then at the Freedom of the Press Foundation, wrote a thirty-page security article called *Encryption Works* (Freedom of the Press Foundation, 2013). Similar information security guides for journalists and ordinary users have since been published by the Electronic Frontier Foundation (2015b) and the Committee to Protect Journalists (2012), among others, all of which detail similar encryption methods commonly used among security-conscious journalists.

Information security specialists recommend that journalists consider how to tailor their defenses against anticipated “attackers”—a practice called threat modeling. Threat modeling requires that users imagine their potential adversaries (for example, a lone hacker or a foreign government), their capabilities, and the type of data under threat. They must consider the potential risk to their data, and prioritize countermeasures accordingly. Depending on the type of attacker and their intentions, the journalist can develop a tailored response. For example, if an adversary is an ordinary hacker looking to break into an email account, using two-factor authentication and a lengthy passphrase are likely appropriate, assuming no obvious vulnerabilities exist within the email system itself. If an adversary is a person’s employer, avoiding their electronic infrastructure (e.g., corporate phone and email services) is a wise choice. However, if the adversary is a government, ordinary measures are less likely to be effective. The adversary may have extraordinary legal authority to request user data from the email provider, or more advanced capacities to break into systems than ordinary hackers. Users can obstruct meaningful data collection through the use of encryption or anonymity software, or

through creating “noise” by making random queries or contacting random people to obfuscate their activities. Finally, users must also be aware of potential attacks that use technical exploits that could compromise their personal machine: if a user’s machine is compromised, services accessible by that machine may also be compromised.

I spoke with journalists whose personal computers, and those of their newsrooms, have been compromised because they opened documents containing malware. In the United States, this mistake might expose a journalist’s communications with sources or their personal research, opening the journalist or their sources to legal scrutiny, or opening the news organization to potential digital attacks. Yet, such attacks are a global phenomenon, unbound by the laws of any particular country or locale. Well-documented instances include Chinese attacks on the *Washington Post* and countless other news organizations (Perlroth, 2013). In many regions, journalists are targeted for malware attacks using commercially available hacking software sold by Western countries. Well-documented cases of governments breaking into journalists’ computing systems include Bahrain (Marquis-Boire et al., 2013), Egypt (Kimball, 2015) and Ethiopia (Marczak et al., 2014; Marquis-Boire et al., 2013). Envisioning the capabilities of a government, or even ordinary hackers, is increasingly difficult in a globalized environment of largely invisible technical infrastructure and, in some cases, technical vulnerability to so-called “cyber-threats.”

Security specialists often recommend open source software that can be scrutinized by independent developers, as opposed to proprietary software (e.g., Windows), because they may not trust proprietary systems that aren’t publicly audited for security vulnerabilities or deliberate tampering. Security guides for journalists often recommend a small number of open source tools, including PGP, OTR, Tor, and Tails:

- PGP—PGP stands for Pretty Good Privacy, an encryption protocol developed by Phil Zimmermann in 1991 as a response to emerging government surveillance in the early 1990s. The protocol uses a combination of algorithms to allow users to scramble their email messages before they traverse the Web from the sender to recipient. PGP then allows participants in conversation to decrypt the scrambled email on their personal device in readable plaintext.

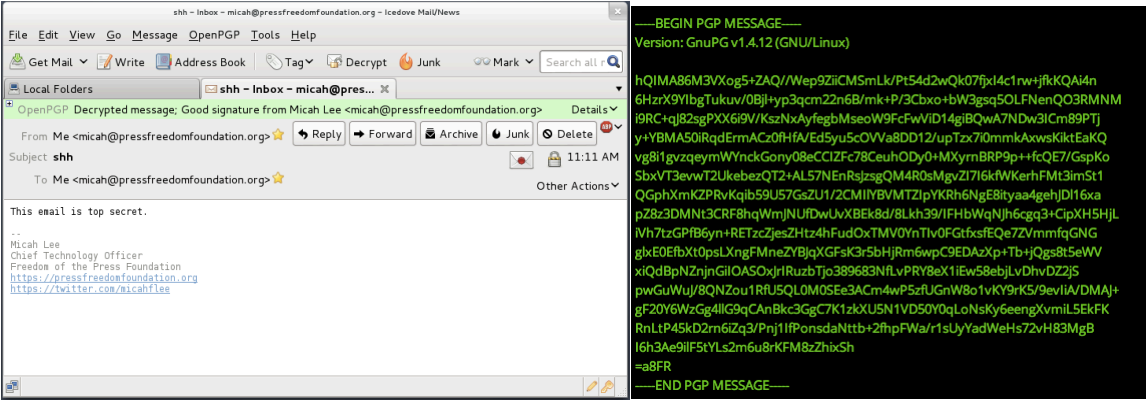


Figure 1. An example of a plaintext message (left) converted into an encrypted PGP message (right). Source: *Encryption Works* (Freedom of the Press Foundation, 2013)

Users have two sets of encryption keys: a “public key”—a long string of randomly generated text that can be shared with anyone—and a “private key” that is password-protected. To send encrypted email, PGP combines the sender’s private key with the recipient’s public key in its scrambling algorithm. The recipient uses their own password-protected private key to decrypt the message. This method of encryption and decryption using publicly available keys is called *public-key cryptography*, a method used in an enormous number of modern software products. Users typically manage their collection of other users’ public keys with key management tools (e.g., GPGTools’ Keychain Access). Users can also retrieve one another’s keys using directories, much like a phone book (e.g., MIT’s key server: <https://pgp.mit.edu>).

PGP achieved widespread adoption among privacy-minded Web users in the early 1990s,

when U.S. agencies, particularly the NSA, pushed to limit public access to cryptography. Despite the privacy advantages of the software, it is notoriously challenging to use, and is frequently held among security specialists and journalists alike as the prime illustration of difficulties with encryption. While PGP successfully scrambles the content of an email, it does not obscure the names of senders and receivers; a user's email metadata is still available to third parties, including the email provider itself. For more than 20 years, it has nonetheless remained a popular standard for email encryption.

- OTR—OTR stands for Off-the-Record messaging, generally considered a simple tool for encrypting instant messages over Google Hangout, Facebook, and AOL Instant Messenger, among other popular chat clients. Security-minded users often prefer to use an open source chat protocol called XMPP (or Jabber) to support their OTR messaging. XMPP users can encrypt their instant messages so that they are only readable by the intended recipient.
- Tor—The Onion Router, allows users to connect to the Internet anonymously by encrypting traffic and bouncing it between Tor clients around the world before it is delivered to its destination (e.g., a website). In doing so, the original source (as revealed by an IP address) of the traffic is obscured to adversaries. Tor is also a popular tool for anonymizing traffic through a conventional Firefox-based browser, enabling users to easily mask their Web activities.
- Tails—The Amnesiac Incognito Live System is an open-source Debian-based operating system developed to secure and anonymize the user's computing activity, including activity over the Web. Tails includes a suite of security-enhancing tools, including PGP and OTR, and routes all Web traffic through the Tor network. Tails can be launched from a USB flash drive or compact disk, as opposed to the user's hard drive. It is designed to “forget” the

user's activity when they are done using the system; Tails erases all traces of user activity on the operating system immediately after shutdown.

In short, PGP or OTR allow users to speak with one another without compromising the content of their communications, while Tor provides multiple layers of encryption for Web traffic. Tails offers a temporary operating system, enabling users to avoid proprietary operating systems while accessing a large suite of security tools, including PGP, OTR and Tor. With the appropriate threat model and knowledge of their limitations, a user can leverage these tools to obscure their activities to most adversaries. Unfortunately, many of these tools are still difficult to use and understand, allowing users to leak their data by mistake.

Open source projects serve as alternatives to proprietary software operated primarily by corporate entities. Open source projects increasingly tackle usability issues with encryption tools in order to make the tools more accessible to ordinary users, and have made enormous strides toward accessibility for encrypted text messages (e.g., Signal, TextSecure) and encrypted phone calls (e.g., Signal, RedPhone) for the most popular smartphone platforms. An open source Web chat tool called Cryptocat, delivered as a browser extension, has attracted attention among security-conscious users for its simple design and ease of deployment within standard Web browsers.

Securing communications is necessary because data can be intercepted in transit—as data moves between servers when a user requests information from the Web. However, data can also be intercepted from devices. For that reason, data resting on a journalist's computer or mobile device may also require protection. Their data are typically stored on hard drives that can be read by anyone with access to the computer, unless the hard drive is encrypted.

Popular operating systems offer hard drive encryption. For example, Windows Business

includes BitLocker, while Apple offers device encryption through FileVault, enabling users to secure their hard drives. While journalists are key beneficiaries, technology companies recognize the value of device encryption for ordinary users and are enabling these security features in their devices as well. For instance, Google and Apple announced plans to encrypt Android phones and iPhones by default (Kravets, 2014; Timberg, 2014).

Law enforcement officials have been vocal about the potential danger of pervasive encryption, warning that criminals will be empowered if police and federal investigators are unable to decrypt devices. For example, FBI head James Comey speaks regularly about the dangers of phone encryption, arguing that a phone may contain valuable data for investigations, including call histories and text messages as well as access to Web communications increasingly embedded into phones via email and social media applications (Reilly & Sledge, 2014). In criminal investigations, mobile phones are a goldmine for personal data because owners may carry them everywhere, broadcasting information about their location and personal associations.

It is somewhat misleading to suggest that encrypting a phone will prevent law enforcement officials from doing their work, because the data are not simply held on personal devices. Rather, user data is also stored remotely, for example, through cloud storage and through phone records held by telecommunications companies. Telecommunications companies are compelled to provide federal investigators and police departments with phone records if they can provide a warrant. For example, if Verizon is served with a subpoena in a criminal investigation, it may be compelled to turn over the user's call history, text messages, and location history.

The NSA disclosures demonstrated what security-minded technologists have known for decades: Unencrypted website connections can be easily analyzed by network eavesdroppers.

Traditionally, with the exception of financial institutions and for protecting login credentials, traffic between users and websites has not been secured, in significant part because Web traffic has often relied on HTTP (see Figure 2, below). In particular, HTTP is an unsecured protocol for routing Web traffic to its destination (e.g., <http://nytimes.com>). With HTTP, third parties can intercept a person's unsecured Web traffic. Two common cryptographic standards, Secure Sockets Layer (SSL) and Transport Layer Security (TLS) enable a website to transmit data between a user's computer and the website in an envelope of encryption.

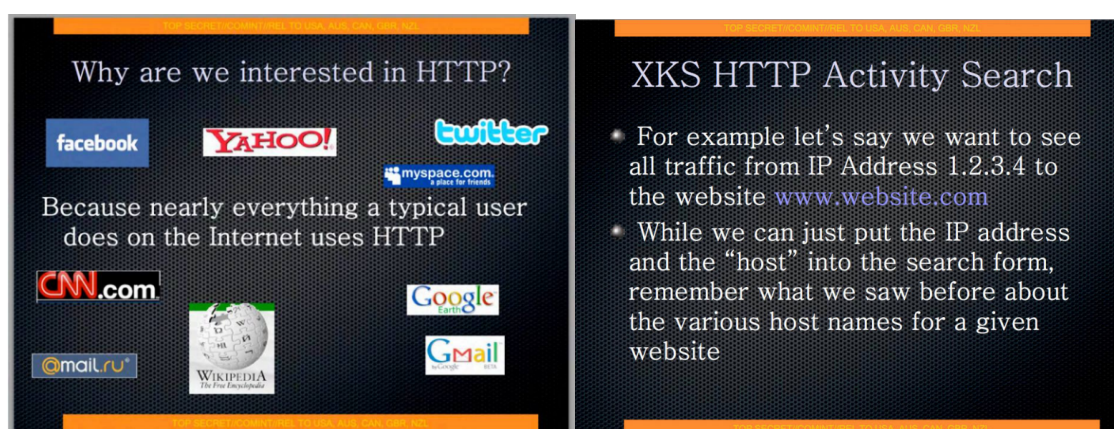


Figure 2. Internal NSA slides detailing the collection and indexing of unencrypted Web traffic.

In months immediately following the Snowden disclosures, Web companies quickly began to adopt SSL/TLS encryption by default—for example, Yahoo (Bonforte, 2014) and Facebook (Cohen, 2013)—to protect their customers' communications. In August 2014, Google announced that it will give preference to websites using encryption in its search service (Bahajji & Illyes, 2014). Web encryption has also seen an enormous jump in adoption spurred by Internet companies, for example, Cloudflare (Eckersley & Schoen, 2014; Prince, 2014), which began to offer encryption services for free in 2014. For ordinary users the primary difference in their experience of an encrypted connection to a website is that the URL will include HTTPS ("HTTP Secure") instead of HTTP. In other words, <http://nytimes.com> will simply become <https://nytimes.com>. The *New York Times* challenged major news organizations to adopt

encryption by default before the close of 2015 (Konigsburg, Pant, & Kvochko, 2014), arguing for its value in cryptographically authenticating the delivery of its own content and allowing users to browse the *Times* privately. In September 2014, the Freedom of the Press Foundation similarly urged news organizations to adopt HTTPS by default (K. Gallagher, 2014).

The proliferation of encrypted communication software coincides with the development and adoption of novel security tools to support the news. SecureDrop, an open-source project currently managed by the Freedom of the Press Foundation, allows sources to securely and anonymously deliver documents to news organizations. News organizations including the *Guardian*, the *Washington Post*, *ProPublica*, the *Intercept*, and others support SecureDrop, facilitating the anonymous transfer of documents between whistleblowers and news organizations. SecureDrop requires users to connect through the Tor anonymity network before they can upload documents. The journalist must, in turn, download the documents on one computer connected to the Internet, and use USB flash drives to transfer and decrypt the data on a secondary computer that does not connect to the Internet. The elaborate encryption, transfer, and decryption scheme offers a relatively high level of security for both journalists and sources, enabling them to receive sensitive documents from anyone in the world.

It is insufficient for journalists to manage security on their own. Rather, sources also take security measures. Through tools like SecureDrop and a small but growing contingent of online guides for leaking documents to journalists (e.g., Lee, 2015a), the process of leaking is increasingly streamlined. Simple guides describe how users can bypass the pitfalls of using anonymity tools to leak documents, and possible mistakes that could identify the leaker. For example, SecureDrop users should “clean” identifying metadata attached to their documents before sending them through Tor.

Anonymity and encryption tools supplement information-gathering activities for a small number of news organizations and cannot replace the traditional work of connecting with sources and gathering information for a story. In my interviews with investigative journalists and press advocates, I found that both encryption and anonymization software are being quickly adopted by many journalists. However, they have complex motivations that align with their behaviors in unexpected ways. In the next chapter, I finally explore the journalists' motivations for adopting information security technologies, and stories about how they conduct their work in the face of digital security threats.

Chapter 5

Findings

Security guides recommend that journalists use data obfuscation and encryption techniques to help manage source protection. These security guides do not reflect what investigative journalists appear to do in practice. The journalists with whom I spoke presented a variety of conflicts with the use of these information security approaches in the context of electronic surveillance. I found that security tools and techniques both enable and foreclose opportunities to connect with others. I first describe the basic contours of the journalists' work, with attention to how they consider threat modeling and their corresponding information security practices. Finally, I examine the relationship between corporate and government surveillance, and how it impacts the work of journalism in the United States and around the world.

5.1 About the Journalists

I spoke with journalists and press advocates about experiences related to their own information security and the trends they observed within American journalism more broadly. Journalists and press advocates described information security quite differently. Advocates tended to speak in general terms, often describing the broad trends they have witnessed within news organizations and the challenges faced by journalists, whereas journalists were more likely to describe their personal stories.

The journalists worked within a range of organizational structures. While most of the journalists I spoke with were involved in traditional corporate newsrooms that sell news to the public as a product, some were freelancers working with multiple organizations and others were involved in commercial newswire agencies. Unlike traditional news organizations, newswires (e.g., BusinessWire, PR Web, ABN Newswire) primarily focus on selling news to larger media companies (e.g., the Associated Press, Agence France-Presse) that redistribute their news on a

broader scale. Unlike a traditional newsroom focused on expertise of a specific topic or beat, a wire offers regional expertise.

One of the major challenges with asking journalists about information security practices is that many journalists prefer to obscure their methods for protecting sources. In turn, nearly everyone who routinely communicates with confidential sources was cautious about the details they included in our interviews and occasionally took certain disclosures off the record. Much of the time they focused on previously published information, or events of the past, rather than the present. As one of the press advocates who I will call “Michael” told me:

Journalists don't like talking about their specific situations [about their relationships] with sources. At [a recent security conference], there were a lot of people talking about hypotheticals, and in the past, things that have happened to them.

Clearly, most participants withheld information. Only those with a history of speaking publicly on topics related to information security and surveillance spoke without reservation. In one prominent example, I spoke with Glenn Greenwald, whose commentary I will share throughout this chapter. Altogether, the journalists and press advocates offered novel stories about their own experiences and observations in newsrooms and in their personal lives. Their diverse perspectives represent a composite of approaches for managing information security.

5.2 Attribution and Nonattribution in Reporting

For most of the journalists I spoke with, an ordinary day involves conducting research by speaking with sources and reading background for a story as well as actively writing stories. Every journalist routinely worked with sources. Depending on the nature of their organization, journalistic beat, and the specific story, journalists may involve sources in the development of a story in countless ways.

Journalists must develop a variety of relationships with sources in order to gather

information. Some journalists cultivate a network of trusted “moles” throughout their career (Hencke, 2000), and build relationships with sources who they can speak to as a matter of routine. At other times, they connect with sources on an ad hoc basis or in response to specific stories.

Sources are quite central to journalists’ work, and many journalists actively keep track of trusted and reliable sources as well as potential new leads. The veteran investigative journalist Steve Weinberg (1996) argues that current and former sources can provide helpful leads in stories. Journalists, he suggests, are generally good at finding “currents” (e.g., current employees, current friends, spouses, co-workers) who can shed light on a story, but sometimes neglect “formers” (e.g., former employees) who can provide useful information in connection to an investigation.

Of course, sources are not necessarily reliable. Sources may have their own agendas and may sometimes offer inaccurate information. As a consequence, journalists must be cautious and vet their sources. Journalists typically investigate the accuracy of statements from their sources by checking for inconsistencies with other evidence, such as public records. Finding reliable sources can require substantial time and effort, and the mutual development of trust.

Attribution is crucial to the maintenance of journalists’ relationships with their sources. Sources may or may not wish to be identified in a story in three capacities: Sources speak “on background,” as well as “on the record” and “off the record,” depending on the information they are sharing with the journalist. Sources may prefer to speak off the record at various points to share information that they would prefer not to publish in any capacity. Sources speaking on background may share tips or provide information on the relevant actors in a story, but do not want to have the information attributed to them. Their background information helps to provide

context as a journalist digs deeper for named sources who are willing to speak “on the record,” to corroborate facts of the story.

A reporter who I will call “Melanie” described her relationship to her sources and the importance of attribution. She told me that some sources feel comfortable sharing certain types of information when that information is not directly attributed to them:

They will talk to you on background and, because they know it's not going to be attributed to them, they'll tell you everything. All of the different political players, or whatever... I have police people who will talk to me about stuff that's going on. I have lawyers who will tell me about stuff that's going on in the department. Things like that. And that leads you to find people who will vouch for it. So, I've never written a story based purely on anonymous sources because the idea is that you find someone who will say this, who will go on record.

Learning about the broad contours of a story and finding background sources are both important starting points, but in general, having sources who are able to speak on the record is ideal. Barring unusual circumstances, journalists strongly prefer to publish quotes from identified sources because the information is thought to be more verifiable and credible than information provided by an anonymous source. In other words, the information is considered to be of higher quality. In contrast, it can be difficult to verify the legitimacy of an anonymous source, both for the journalist and for readers.

I found that many journalists prefer that sources speak on the record when possible, but speaking anonymously offers compelling advantages: (1) a person might face reprisal if identified as a source and (2) when anonymous, a source may feel more comfortable speaking candidly about the facts in a story. These advantages are not mutually exclusive. For example, a source might feel uncomfortable speaking being identified because of concerns about retaliation from their employer, and may feel more comfortable sharing information when confident that they will not face reprisal.

I spoke with an investigative reporter named “Bill,” whose reporting exemplified the need for anonymity. At the time, Bill was conducting an ongoing investigation of a nonprofit organization in his city and had reported that the organization gave misleading information to donors about how their donations were used. He conducted his research by first getting tips from anonymous sources within the organization. Because he could not corroborate the claims of his sources, and as a matter of course, he made requests for public records based on the tips.

We interviewed current and former [nonprofit] staffers and volunteers. And they actually gave information for the story on the condition of anonymity, because they continue to work with [the nonprofit] ... [They] have a policy, like many large companies or institutions that don't want people talking to the press outside of the strict process channels. And if you're out there, there can be some form of punishment.

When sharing privileged or damaging information about their employer, sources may prefer not to be identified. However, even when sharing information that isn't strictly privileged, large organizations may also be concerned about how their employees represent them. Sharing information at odds with the public image of an organization can be sufficient to warrant nonattribution. As another reporter, “Nick” suggested, “They may get criticized or attacked, because the institution they work for—the government or agency in question—doesn't want to be seen as taking that position publicly.” In these cases, even if the information is not particularly sensitive, it may be information that their organization would prefer not to be publicized.

Another value of nonattribution is that many people simply feel more comfortable speaking off the record, and can “open up” about the details of a story. According to Melanie:

One of the deals with privacy and with confidentiality is that people open up! They say what they are thinking and what it is that they want to tell you, whereas if you turn on a tape recorder, for most people, it's a different game. So I typically will not record anything on the first meeting with anybody, because just the presence of a tape recorder is a little too transactional, and it's too daunting, intimidating. So I try to meet with a source face-to-face if possible... Typically I like to have a long conversation with them before, talk about what it is they want to talk about, have them lead the conversation, and then come back and say let's do this on record.

Particularly in recent years, sources involved in national security and foreign affairs reporting have taken advantage of nonattribution, even when speaking about information that is not privileged or sensitive. I spoke with a journalist, who I will call “Ted,” about his reporting on the Department of Justice. In his work, he found that some confidential sources habitually speak on background for “no good reason.” However, there are also people who he suggests have “a good reason” when speaking about sensitive or privileged information. He observed that nonattribution has become the norm among public officials, particularly in Washington D.C., the central locale for national security, intelligence, and foreign affairs reporting. Concerned with potential blowback for their comments, sources in national politics—particularly government employees—have taken to speaking confidentially by default:

Unfortunately, in Washington, people in government are mostly speaking confidentially or without attribution... It's common practice here. We've been mystified as to why people are so into speaking that way. It's like a habit, I think... I talk to people who are in the Public Information Office at the White House and the Justice Department, and it's almost always not for attribution by name, unless they issue a formal statement. And that's just the people at the [Public Information Office], and it's their job to talk to us. You would think that they would speak on the record...

It's a very bad habit in Washington. People think they're less likely to get in trouble, I guess, if they tightly control how they're quoted. It's just become the norm.

Among public officials, attribution can be a political liability. According to the Committee to Protect Journalists, the problem has become especially pronounced during the Obama administration (Rafsky, 2014). Ted asserted that officials are increasingly wary about speaking with journalists, even when sharing inconsequential information. The national security reporters I spoke with suggested that the Obama administration's Justice Department has taken an aggressive stance against government employees who speak with reporters, no matter how benign the conversation. In a small number of cases, the government has taken legal action

against government employees who speak with reporters (see Section 4.2.1). When I asked Ted whether investigative journalism has changed in recent years, he continued:

In response to Snowden, it's quite clear that sources are more afraid to communicate with journalists than they used to be, and I think that's changed things dramatically. It's hard to communicate by email, it's hard to communicate by phone. People are afraid now to talk to reporters, much more so than they used to be. I think that's dried up a lot of information. It's not only Snowden, but also the fact that the Obama administration has been so aggressive about pursuing leaks.

Ted echoed the sentiment of other national security reporters I spoke with. National security reporters have a reputation for being cautious about their information security. A Pew Research survey found that roughly two out of three investigative journalists believe the government has collected data about their communications (Pew Research Center, 2015). That number is higher (71%) for national security and foreign affairs reporters than for journalists who cover different beats (62%). When asked about the arenas where journalists are likely to have confidential sources, the journalists I spoke with agreed that source protection in national security reporting is particularly crucial. Pew Research found that national security and foreign affairs journalists were more likely than other journalists to have changed how they manage information security since learning about the government surveillance programs. They were more likely to have changed how they store sensitive documents and communicate with colleagues, more likely to use security tools, more likely to research how to secure their communications, and more likely to be concerned about losing valuable sources to a competitor with better security. In other words, national security and foreign affairs journalists appear to take their security posture quite seriously.

I spoke with security specialists who sought to combat the perception that information security is a problem only for a narrow range of beats, including national security. These specialists point out that journalism organizations can be breached by the “weakest link” in a

news organization's security. Because national security reporters are stereotypically the "strongest links" in news organizations, an attacker may not target those reporters' systems, instead opting for people perceived to be easier targets. For example, I spoke with one information security specialist who said that if she wanted to breach a news organization's network, she would not attack a national security journalist's computer. Instead, she said that she would have the most success by breaching the systems of unsuspecting journalists, offering the example of a fashion reporter. It is unclear whether fashion reporters, in fact, lack a strong security posture, but the stereotype is pervasive. Depending on the nature of their work, journalists have altogether different expectations of digital threats to their communications and personal data. They may not see the need to secure their communications with sources.

It is clear that sources have a variety of motivations for speaking anonymously, on background, or off the record. Sometimes their conversations involve the exchange of sensitive information. Sometimes their conversations involve information that emerges outside of the control of their employer. Sometimes being seen communicating with a journalist at all can be problematic for the source. Likewise, specific pieces of information are sometimes kept off the record, while the rest of the conversation can be quoted. These splintered responses begin to make sense when considering how journalists perceive potential digital attackers and their capabilities.

5.3 Threat Modeling

As the above examples illustrate, anticipating potential eavesdroppers is important for protecting the confidentiality of a source. In chapter 4, I introduced this process as *threat modeling*. Threat modeling involves considering what data requires protection, as well as envisioning potential "attackers" and their capabilities. In so doing, threat modeling can help a person formulate

appropriate strategies to protect their information. In the context of investigative reporting, journalists are typically concerned with information that can be used to identify their sources and potentially other types of sensitive information. Threats can be lone individuals (e.g., hackers). However, the threat can also come from institutions, such as an employer or a government. Depending on the journalistic beat, the journalist may know whether an institution, group, or individual is a likely attacker.

Understanding likely attackers depends on the particular context. For example, journalists working on domestic national security reporting may have strong reasons to believe that the government would be interested in their sources, while journalists investigating hacking groups may find that their sources are connected to sophisticated attackers who may pose a threat. Threat modeling is usually the first step to considering how to protect sources in a contextually appropriate fashion.

In practice, threat modeling can be quite difficult because the capabilities of an adversary are not always clear. For example, Bill worked with a team of investigative journalists well trained in information security practices. Depending on the nature of his sources and the information they could offer, he had to consider how to speak with them without leaving information that could link them to his organization. As he stated,

If you're doing your job correctly, you're doing threat modeling. A lot of people don't know that term, but they're doing it. So working with [the nonprofit's] case is very different than working with an NSA source... They're not the government. But still, I try to be very careful and I've become more conscious over the past couple of years about keeping stories secure, being careful about what you put in emails... If you're talking to someone who works at an organization [that we're investigating], don't call him or her at work. You need to deliberately think about this. Certainly don't do anything that could jeopardize anyone who has requested [anonymity], because we take those requests very seriously.

During Bill's nonprofit investigation, he had to assume that his adversary (the nonprofit)

would not have access to information about his correspondence with sources because he called them outside of obvious work channels. In other words, he had to rely on informed assumptions to produce his threat model.

While journalists often consider threats to their sources, the identity of the journalist and the nature of their reporting strongly influence how they think about threat modeling. In general, journalists conducting sensitive work often have to assume that their potential attackers are more capable than those potentially faced by parties involved in less sensitive reporting. As a consequence, threat models are closely tied to stereotypes about sensitive journalistic beats and topics. For example, in high-profile national security or foreign affairs reporting, it is difficult to understand the capabilities of attackers, but it is often safe to assume that they involve technically sophisticated governments around the world. In contrast, multiple journalists (often jokingly) told me that sports and fashion reporters were not likely to be targeted. In other words, many journalists may not expect attackers when working with information that is not privileged, is not obviously sensitive, and appears unlikely to attract the close scrutiny of a third party.

5.4 Information Security Practices and Challenges

The journalists had a variety of perspectives on data security, often diverging in beliefs and practices. They described techniques involving encryption, the use of multiple accounts to compartmentalize their data, and creative techniques to obfuscate their activities when communicating with sensitive sources. They sometimes use physical mail and face-to-face meetings to prevent the digitization of their communications—both out of necessity and for the sake of convenience. By using security tools to reach out to journalists, I found out for myself that the tools sometimes required considerable effort. In this section I explore journalists' information security practices in the context of email, instant messaging, phone calls, physical

meetings, and the security of their own computers. Many of the journalists have their own methods and ad hoc techniques. Out of respect for participants, I withhold a small number of revealing security approaches. Finally, I describe the successes and shortcomings of the different approaches, as well as the impact they have on journalists' lives within the United States and abroad.

5.4.1 Adoption, Concerns, and Challenges with Email Encryption

When conducting interviews, I reached out to many journalists using their publicly available PGP public keys to encrypt our email exchanges. Some of the journalists posted public keys alongside other contact information, including their name and email, on their professional websites and article columns. In a few instances, we spoke over encrypted channels for the interviews themselves. This was not absolutely necessary—after all, we weren't usually talking about sensitive information. Nonetheless, the exercise helped me to understand how difficult PGP can be to set up and use.

While the journalists had mixed feelings about the utility of the software, they independently converged on the same description for PGP: “A pain in the ass.” One cybersecurity reporter, Nick, summed up his concerns:

I've tried to get PGP to work and I'd largely failed, because it's complex and largely a pain in the ass. But there are people who wanted to communicate that way, so I figured it out with the help of the tech people here... When the motive was there, I figured it out. It's not that hard really, it's just that I'm lazy.

To ask journalists what, in particular, makes PGP difficult is a bit like asking an academic what is problematic about the scholarly review process. Where to begin? When I asked “Laurel,” a technology reporter at *Fusion*, what made PGP difficult to use, she countered my question with another question. “Well, you use it, right? Do you think it's easy to use?”

Glenn Greenwald, the journalist who first broke the Snowden disclosures with the *Guardian*, is perhaps one of the most famously unwilling adopters of PGP. In his early interactions with Snowden, the ex-NSA contractor provided detailed instructions on using the email protocol to secure their communications, but Greenwald did not install PGP for months. I spoke with Greenwald in a brief interview, and during our conversation I asked about the challenges of using PGP. In his words:

PGP is this technology developed in the early 90s. And it hasn't really evolved that much since then in terms of being user friendly because it's mostly been used by nerds and hackers, and people who almost like the fact that it's so complicated. But if it's going to spread it needs to become much more user friendly, precisely because it is so daunting now for non-experts.

Greenwald and the other journalists listed countless issues that reflected my own challenges with the software. PGP required practice, and despite using it extensively in this research, I did not master it. I first consulted guides aimed at journalists themselves, as well as related blog posts. PGP's setup process involved punching in commands on my console terminal and downloading multiple pieces of software. I published my key to MIT's PGP key server (<https://pgp.mit.edu/>), a public directory that acts as a sort of "phone book" for PGP users. I installed Mozilla's Thunderbird email client with Enigmail, a Thunderbird extension that allows users to encrypt their emails. Enigmail connects with my PGP "keychain"—my personal address book for the keys I gathered on journalists' websites and through the public key server. When I sent encrypted recruitment emails, I occasionally made mistakes. I would forget to attach my public key to the email, or I would accidentally encrypt the message to the journalist's old key instead of a new one, leaving the email unreadable. Occasionally, they could not read my messages, and I needed to send them in plaintext—a luxury I have, but an at-risk user might not. If this sounds complicated, that's because it is.

Eventually, I began to correctly send the emails almost as fluidly as I would send any other, but I learned that PGP caused headaches for many of the message recipients. In spite of streamlining my process, it required disproportionate time and effort to locate the journalists' keys and to confirm that I had the correct information.

Many of the journalists pointed out that they did not use PGP very often, and when they did, it was often in circumstances (like mine) where they did not believe it was absolutely necessary. Nearly everyone, even the technically savvy among them, lamented how difficult PGP is to use for multiple reasons:

- (1) Nearly universally, the journalists agreed that it is unnecessarily difficult to use.
- (2) PGP users need their private key to decrypt messages, and they don't always have access to the computer with their private key. Users must also have the appropriate applications installed on their machine to decode the email. In effect, this means that journalists can be locked out of their encrypted email on their phones and when traveling.
- (3) PGP only masks the email's content and not the email's metadata—information about who sent the email to whom, and when. In effect, PGP may not be suitable for journalists who seek confidentiality.
- (4) Most of the journalists kept tight schedules. Because it took time and effort to use, some preferred not to send emails over PGP unless it was necessary.
- (5) Finally, if a sophisticated attacker has already compromised the machine, encrypting the emails won't prevent the attacker from reading them. For all of these reasons, unless it was absolutely necessary, many of the journalists preferred not to use PGP with sources.

Even after taking the steps to set it up, many journalists seldom went on to use encryption because their sources rarely used such measures. At the time, PGP email encryption was one of

the most popular tools for communicating securely. Although nearly all guides for information security in journalism recommend setting up PGP, most journalists with whom I spoke agreed that they would never ask a source to set it up because it was so difficult to use for the uninitiated.

One *New York Times* journalist, “Timothy,” related his anxieties with PGP because he well understood the software’s shortcomings. Timothy cited an example of the former CIA employee, Jeffrey Sterling, who was convicted in early 2015 of violating the Espionage Act by sharing information with another *New York Times* reporter, James Risen (Maass, 2015b). Their email and phone communications linked the two, and their metadata was found to be sufficient evidence against Sterling:

Metadata is what matters as much as anything, not e-mail content... Look at Sterling—he was just convicted based on the circumstantial evidence, including all his contacts with Risen where they could go back and get the phone metadata but hadn't wiretapped the content. Another reason encryption is not the panacea its proponents sometimes hold it out to be. It would have to be encryption plus Tor, which is both something no ordinary person is capable of doing, and would be extra red flaggy. I don't think there is a technological solution in sight yet.

Timothy points out two major issues with using email encryption to secure communications: (1) It requires incredible effort and technical knowledge to do so with all of the appropriate precautions, and (2) doing so may still call attention to the conversation, potentially making it “red flaggy.” PGP exposes metadata about the conversation, including the names of the sender and receiver, thus potentially revealing identifying information about a confidential source. To mask their metadata, a source would need to set up PGP through anonymizing software (such as Tor). Masking metadata is technically feasible, but no ordinary source would go through the unusual effort to do so. In other words, using PGP meaningfully in a journalist-source context can be extraordinarily challenging.

Despite the challenges, many journalists use email encryption, particularly in national security, foreign affairs, and cybersecurity reporting. Cybersecurity journalists were likely to have technically sophisticated sources who already used the tools. However, journalists working on sensitive topics related to the military and intelligence were also motivated to protect their communications when speaking about highly sensitive information, even when speaking on background or off-the-record. When speaking about sensitive information, many of the reporters simply preferred to minimize their electronic records by speaking in person.

Email is also problematic for journalists because news organizations may be targeted in digital attacks. Of the many forms of potential digital attacks, Jonathan Stray at Columbia University suggests that journalists are most likely to fall victim to “phishing” emails (Stray, 2014). Phishing describes attempts to gather sensitive information (e.g., login information) by impersonating a trustworthy party. Journalists may receive a phishing email from a third party, for example, claiming to belong to a trustworthy organization (e.g., Twitter) and providing links to a fake version of a login homepage. Typically the fake website will replicate a trustworthy website, creating an opportunity for victims to unwittingly enter their login credentials. If the journalists are not vigilant, they may not notice that their link redirects to an altogether different webpage.

5.4.2 Successes and Compromises in Instant Messaging

Journalists have a variety of approaches to obstruct potential digital threats in their personal messages, in some cases using encrypted messaging tools, and in other cases opting for more routine consumer tools such as Google Hangout chat.

Off-the-record (OTR) chat is an encryption protocol that provides a layer of encryption over existing chat programs, for example, AOL Instant Messenger, Google Hangout, or

Facebook private messenger. Much like PGP, OTR encrypts the content of a message and allows users to verify their conversational partner, but their metadata can still be intercepted. OTR should not be confused with Google Hangout's "off the record" function. OTR is generally quite easy to use, and can be installed with a single application and a plug-in using Adium on Mac OS X, or Pidgin on Windows or Linux. Several other clients (e.g., Jitsi) support OTR for encrypted video chat. However, proprietary messengers like those offered by Facebook or Google will still retain the encrypted messages on their servers. While the content of these encrypted messages won't be legible to Facebook, for example, the metadata is still readily available. Security-conscious journalists may prefer to use a free and open source protocol called Jabber as an alternative to proprietary messengers for sending messages using OTR. Together, Jabber and OTR can provide an alternative to popular messaging services. Using proprietary instant message services is convenient and relatively secure from third parties—except the company itself. Most companies with messaging services (e.g., Facebook, Google) will encrypt their messages in transit, but their messages may be decrypted by the company in response to a court order (Lerner & Bar-Nissim, 2014). Barring unusual circumstances, many of the journalists with whom I spoke preferred to use proprietary instant messaging applications to connect with their sources.

A journalist named "Jimmy" told me that he keeps in touch with his sources over Google Hangout and Twitter direct messages. He said that he does not have sources who are worried about the U.S. government. Instead, he worked with Southeastern Asian activists in a region with weak diplomatic ties to the United States. They are more concerned with their own government. He assumed that American companies would protect his conversations with foreign sources because they are not obliged to share information with those governments. Furthermore, he said

that he needed to trust his sources and their knowledge of the story, and to meet them on communication channels they actually use:

Some of them were willing to give their info, others weren't, and they wanted to communicate in a channel that was secure. Unfortunately a lot of people end up using Skype [messaging], which is not—it's really not what you want to do. But that's the problem, you have to go where the people are.

While he admitted his approach could have been stronger, he told me that it worked for the purposes of his story. Jimmy's story is somewhat common; many journalists prefer to use instant messages for a quick, simple channel to speak with their sources. Like all communication channels, security in instant messaging depends on assumptions about the capabilities of the attacker. In his case, he felt his foreign sources were not at risk because he contacted them through a service that would not give their conversational data to the foreign government. Phone calls can operate similarly, and I found that journalists have demonstrated resourcefulness with their use of phones.

5.4.3 Phones and Mobile Devices

Investigative journalists, particularly national security reporters, have been highly creative about obstructing surveillance of their phone activities. They described a variety of strategies to leave misleading phone records when tackling a sensitive story.

Ted, an experienced national security reporter based in Washington D.C., said he made considerable efforts to combat phone surveillance. Years ago, he used pay phones—now largely extinct in the U.S. capital—and now he uses disposable, prepaid “burner” phones.

In the old days of pay phones, we used to run downstairs, wherever we were working on a case and we just called somebody from a pay phone so that there wouldn't be a record of the call. We don't have pay phones anymore, so you can't do that... I keep a couple of disposable prepaid cell phones to use in the rare cases where I have an extremely sensitive conversation, and I've been recommending that to reporters. I go through great lengths to make sure that those cell phones can't be traced. I pay for them in cash, I pay for the additional minutes in cash. I get a couple of cheap phones from the drug store, or

something, so that the numbers aren't associated with me. I try not to use them to call multiple sources at the same time.

Previous research by Human Rights Watch and the ACLU (2013) found similar trends, observing that journalists in national security (and related arenas) adopted burner phones. I saw that the national security reporters have been inventive with their phone tactics, in some cases calling from multiple phones, using the phones of nearby businesses, or calling a large number of extraneous numbers to wash out the “signal” of their one legitimate call in the “noise” of unrelated calls. In each case, they hoped to confuse potential eavesdroppers. Most preferred not to bring their personal phone to a face-to-face meeting with a sensitive source because the phone can potentially provide electronic records of their location through GPS, wi-fi connections, and their proximity to nearby cell phone towers.

The journalists emphasized that obfuscating phone records is generally reserved for rare circumstances when sharing sensitive information or connecting with a source who could be at risk. For routine work, cell phones and their landline phones at work are often sufficient and are generally more convenient. Electronic eavesdropping is a serious concern, but even for national security journalists the use of burner phones or elaborate measures with phones is exceptional.

As Nick told me:

[Eavesdropping] does happen, but it's not routine in my work... What we try to do is perceive stories and sources that would trigger particular scrutiny, and be extra careful in those circumstances. It's hardly every day, nor is it every week, but every once in a while.

Some of the journalists have begun to adopt mobile encryption applications for their phones, including Signal, RedPhone, and TextSecure—interoperable applications developed by a nonprofit called Open Whisper Systems. Signal allows users to communicate through encrypted phone calls and text messages with other users over their Apple mobile device. For Android

devices, RedPhone encrypts phone calls, while TextSecure encrypts text messages. I spoke to a smaller number of journalists who reported using Threema, a mobile application for encrypted text messages. The tools are generally well designed and more accessible than older tools for sources and journalists who wish to speak over encrypted channels.

I reached out to one journalist, Laurel, through encrypted email. When we concluded our interview, she requested that I keep in touch with her using the Signal mobile app instead of PGP.

5.4.4 Malicious Software and End Point Security

The security approaches discussed above have generally focused on personal communications. However, even these precautions would not protect a user whose computer has been compromised by surveillance tools or malware. If the user's "end point"—their device—has been compromised, communication security tools will not protect their data. As a consequence, information security specialists encourage journalists to encrypt their hard drives, making retrieval of personal data substantially more difficult if their machine is ever confiscated, lost, or stolen (Lee, 2015b). I found that many of my interviewees who worked as security specialists have prompted journalists to encrypt their hard drives and have provided walkthroughs in their training sessions. The journalists learned about hard drive encryption through training or on an ad hoc, individual basis.

An attacker having physical access to a machine is a serious concern, but so are remote attackers. Multiple reporters suggested that sophisticated attackers could breach their news organizations' networks, and sometimes they could not entirely trust the integrity of their own machines. Foreign governments have made a habit of penetrating the networks of large American news establishments (Uberti, 2015). For example, Nick told me that his organization,

the *Washington Post*, has suffered attacks by the Chinese government. The *Post* is only one of many organizations that have been targets of the Chinese government and other foreign governments. In 2014, Google security researchers Huntley and Marquis-Boire reported that 21 of the 25 largest news websites have been targeted in state-sponsored attacks. They found that journalists were “massively over-represented” in targeted digital attacks (Wagstaff, 2014). At the time, *Bloomberg News* and the *Wall Street Journal* had recently announced that their systems had been compromised in Chinese cyberattacks (Perlroth, 2013).

Privacy-conscious journalists are routinely warned by information security specialists to avoid opening suspicious documents or links that they receive in emails because they may execute malware. Some of the journalists must assume that their machines have been compromised as a matter of course. Security-conscious journalists may avoid opening documents sent by untrusted sources on the Web, even though using these documents is profoundly central to their work. Others habituate to the dangers.

Some of the most widely available commercial hacking tools can log victims’ keystrokes, take screenshots of their computer in use, turn on their webcam or microphone, and send the data back to a remote server, allowing one or many distant attackers to spy on the victim. Others allow the attacker to parse the computer’s files (N. Anderson, 2013; Marquis-Boire et al., 2013). Taking over the machine can be surreptitious or an obvious tool of terror against the victim. The practice is astonishingly simple, requiring little more than installing a program and getting an unsuspecting user to open a file or a link that will execute malicious code. The malicious code can be delivered however the attacker wishes, for example through an email with a link to an automated file launcher. Journalists may be of interest to a variety of attackers ranging from governments (Wagstaff, 2014) to amateur malicious hackers. Regardless, the perpetrator is

typically ambiguous to the victim. Researchers have documented a wide variety of attacks “in the wild.” For example, researchers and forensic specialists have identified the Syrian government targeting political activists with hacking software (Marquis-Boire & Hardy, 2012). Using more rudimentary tools, young men use similar techniques to spy on unsuspecting women in their homes through their webcams (N. Anderson, 2013). The tools are relatively easy to use and are widely available to anyone with sufficient knowledge to learn more through a quick Google search. The malware can be delivered to the victim through ordinary-looking documents.

The possibility of downloading malware complicated my interview recruitment. As part of a prerequisite for recorded research interviews, I was required to send information sheets about the study to interviewees. I sent the PDF documents detailing notifications of their rights as study participants and information to situate their expectations for the interviews. However, I later learned that many security-conscious journalists would not open the documents I sent along, as they could have been used to deliver and execute malicious software on their machines.

For technically sophisticated users, particularly cybersecurity journalists, the documents should only be opened with specialized software or on a relatively risk-free machine. For example, a few of the journalists told me they had “airgapped” computers that they never connect to the Internet. They download the file onto a USB device and transfer it to the airgapped machine before opening it. If the machine is infected, the infection is thought to be relatively benign. Some journalists use Google services to open their documents instead. Being aware that Google has access to their data, some journalists view documents in Google Docs to avoid executing files on their computer. Finally, some of the interviewees said they feel more comfortable opening documents in the ephemeral Tails operating system. Tails “forgets” all activities of the user after the machine is turned off, and is thought to be safer than opening

documents on their regular work machine with a persistent operating system (e.g., Mac OS or other UNIX-based systems, as well as Windows). While there are many ways to use Tails, for many journalists the process would include using a USB key to boot a copy of Tails on a separate machine, and waiting for it to load the operating system. There are many ways to transfer the file to Tails before executing it, and indeed, files can be transferred via USB to Tails. The operating system can also connect to the Web and download files. Yet, the amount of time and effort to open a document from a stranger is disproportionate. In the end, many of the journalists simply opened the PDFs I sent along on their computers, and others declined to look at them altogether.



Figure 3. NSA Tailored Access Operations implanting “beacons” into computing equipment (Greenwald, 2014, pp. 148-149).

Malicious software is a common threat to the security of a machine, but hardware can also be vulnerable. The Snowden disclosures demonstrated that U.S. intelligence has tampered with computing equipment in this way. As far back as 2010, the National Security Agency redirected shipments of computing equipment for “beacon implants” into targeted network

devices (see Figure 3). It remains unclear who, in particular, is a likely candidate for “supply-chain interdiction,” as internal NSA documents dub the practice (Greenwald, 2014, p. 149). In general, substantially less effort is required to deliver malware to a recipient than to physically tamper with a machine in order to install surveillance tools.

While it isn’t clear whether anyone has, in fact, meddled with the physical machines of any of the journalists with whom I spoke, two of the journalists who worked on information security expressed concerns about the possibility of interdiction. One journalist, “Alex,” shared his concerns about shipping after learning about Snowden’s disclosures:

I don’t think I’d buy a computer, or any piece of hardware, off the Internet and have it mailed to my house, because I’m concerned about it being potentially intercepted and bugged. I wouldn’t buy a router, you know, from Amazon at this point. I just feel that I’m a prime target.

Another information security journalist previously worked as a system administrator. She had been summoned by the Department of Justice on multiple occasions for expert testimony. When we met in person, her computer was adorned with stickers, some of which covered the machine’s input jacks and ports. She told me that she coated the screws on the bottom of her computer with nail polish—a technique used by some hackers and digital security specialists to reveal tampering with their machines (Borland, 2013).

In essence, no matter the level of effort a journalist devotes to their communication security hygiene, end point security is paramount. Their end point can be compromised through both software and physical hardware. Unfortunately, the security of an individual machine is often uncertain. In the event that a journalist’s machine is compromised, without an enormous level of technical expertise they may never know who targeted it.

5.4.5 Avoiding Electronic Records

Journalists have good reasons to doubt the security of their own computers and mobile devices

when working on sensitive stories. Even if a source trusts the journalist, they may not be able to trust the journalist's electronic devices. As a consequence, meeting sources face-to-face, communicating with physical mail, paying with cash, and taking physical notes are often simple and reliable ways to conduct their work while minimizing their electronic records. Although the different types of information and communication technologies are always changing, these well-tested analog approaches have persisted for decades.

Journalists' time is at a premium, and face-to-face conversations are less convenient than a quick call or instant message. Nonetheless, for many of the journalists, electronic records are a liability when communicating with sources about sensitive information, and protecting the confidentiality of a source is often simpler in person. If reasonably nearby, meeting in person can be ideal for sensitive conversations. Melanie told me that she conducts primarily local reporting and works with local sources in Southern California, allowing her the flexibility to meet in person:

I have never had a source who needs to use encryption. And for the people who have more sensitive stuff to tell me, because they don't want to lose their jobs, or they don't want to burn their coworkers, that's done in person, because I have that luxury.

Being local is an enormous boon, allowing plausible deniability for chance encounters at ordinary locations. One journalist with the *Guardian* suggested that locations with ambient noise are ideal for face-to-face meetings—for example, bars and pubs. Because face-to-face meetings can be valuable for sharing sensitive information, some reporters occasionally travel to meet sources in person. However, travel is costly. In my conversations with reporters, they suggested that traveling to a remote location to meet sources is quite rare.

Only under extraordinary circumstances did the journalists meet remote sources in person. A digital crime and cybersecurity reporter named “Alex” told me about one instance

where he traveled out-of-state to meet a source. At the time, he had been reporting on a well-known computer hacker. In the course of his investigation he received access to a trove of documents about the hacker from a source located in another state. Recognizing the sensitivity of the documents, he was uncomfortable with transferring them remotely because he felt that there were “too many variables and risks involved.” His news organization decided to fly him out to another state to view the cache:

One of the decisions that we made was that trying to transfer the entire trove of documents over the Internet was just a horrible idea... Part of the security that we decided on was not uploading them at all—not attempting to encrypt them and transfer them over the Internet.

His sources often included foreign and domestic hackers who may be involved in security breaches, and he suspected that some could be deemed worthy of further scrutiny by authorities. He told me that the Snowden disclosures influenced his approach to information security, stating “I think I talked more online and communicated more easily online with sources and colleagues in the past.” He admitted that he hardly uses unencrypted chat any more, and when he does, he routes his Web traffic through a Virtual Private Network—a remote server that acts as a secure tunnel to send his traffic to its intended recipient. He set up PGP and occasionally prods sources and colleagues to move sensitive digital conversations to off-the-record chat. He doesn’t open email attachments because they might contain hidden malware. In his work, he had to be careful because he documented the work of hackers, some of whom are willing to help him and others who threaten his reporting. Yet, this situation was different. In his view, the extraordinary sensitivity of the documents, as well as their raw volume, made it both unwise and impractical to send them over the Web. He instead went to meet his source in person:

If I was more technologically adept, I probably could have found a way to [encrypt it]. It was a large file; I could have broken it down. It wasn’t something that could have been emailed because of the size. We could have broken it down... There’s obviously other

ways to do it... But at the end, we decided why don't I just go over there, so we don't have to take that chance?

Compared to many other reporters in his organization, he worked with sources that could be considered quite sensitive. Again, unlike most of his organization, Alex could do so because he communicated with technically sophisticated sources who already set up encryption software independently. He did not ask anyone to do so:

The people that I work most closely with use tools like Tails when they're viewing documents. They're using an airgapped machine that they use to view documents. Jabber. Stuff like that.

Many journalists including Alex point out that their colleagues appeared not to take such measures because they had different beats and different kinds of sources that exchanged entirely different kinds of information. Even for Alex, receiving a cache of sensitive documents was highly unusual.

Face-to-face meetings are not only valuable for security. Meeting in person allows journalists to speak more frankly with sources and confirm their identities. It is possible that the source is providing misleading information, and journalists will look for information to confirm the legitimacy of their sources before quoting them in a story. A single bad source can undermine readers' trust in the story, the journalist, and their organization (Carlson, 2011b; Reich, 2011b). One reporter, Jimmy, put it succinctly: "You have to be skeptical of your own sources and vet them. And even if they convince you, you have to convince the reader." In person, sources can provide identification to demonstrate they are who they say they are, and can answer personal questions with less risk.

Some journalism organizations attempt to minimize electronic records by sending and receiving physical mail, even if it happens to slow the news process substantially. Physical mail can help to provide initial points of contact before speaking over alternative channels. Some

journalists will pay for items related to work with cash. Some journalists working on sensitive stories will take physical notes rather than type their notes. In a few cases, the journalists avoided creating any records whatsoever—even on paper. As Nick told me, the only recordkeeping tool he trusts is his own mind:

I don't really store data that I think is worth anything to anybody. Maybe I'm being naïve, but we collect documents specifically with the desire to publish them. ... I literally won't write people's names in my notebook if I think that [it's a risk.]

5.4.6 Why Not Use Encryption?

Many reporters don't use encryption, including cases where they cover national security issues. They had countless reasons not to use encryption tools. Many of the journalists described frustration with difficult-to-use software, while others claimed it scared sources. Still others simply had no interest in using the tools. In other cases, many journalists used the tools fairly infrequently after learning to use them.

I asked one national security reporter named “Ted” whether he uses security software to communicate with sources. He said he did not. For Ted, a seasoned reporter based in Washington D.C., encryption appeared complicated and out of reach:

I'm an old guy, so I'm less technological than maybe a younger reporter would be. I sometimes record calls on my telephone if I can figure out how to use the software to do it.

When speaking about the Snowden disclosures, I asked a press advocate named “Paul” if he observed changes with the journalists he has worked with. He responded, “God, I hope so.” Not long before we spoke, he served on a conference panel about information security in journalism, with an audience of hundreds of journalists. He asked how many of the national security reporters had their hard drives encrypted—one of the simplest measures that an individual could take to protect their locally-stored data:

I'm not talking PGP email, I'm not talking—you could even use proprietary software, BitLocker—maybe seven people raised their hands out of several hundred. And one of them was my executive director, who, when I started my job, I was like, you have to do this. And these are things that are built in!

I spoke with journalists who reported on issues related to cybersecurity, many of whom were exceptionally savvy in their information security approaches. Even they used encryption quite selectively, particularly when working with specific sources or sensitive information. A growing number of large news organizations increasingly adopted a subscription-based secure communication suite, Silent Circle, to support encrypted text messages, phone calls, video calls, and email. Nick, a cybersecurity reporter, told me that he “goes through waves” with many of the tools:

I try to use a VPN. I use PGP. We all occasionally use Silent Circle, the phone app. But it's not super common—I go through waves with it, where I deal with someone who's worried about it, or I'm worried about it on their behalf. But again, it's not super routine, even in what I do. I do think there's colleagues of mine who deal more consistently with national security stuff who have to deal with it more often than I do.

Reporters in cybersecurity have sources who understand the technology better than most. Sources related to cybersecurity tend to be technically savvy—information security experts, hackers, and occasionally government officials who are keenly aware of their how they disclose their personal data. Nonetheless, Michael was sympathetic to journalists who found the tools challenging. He echoed the sentiments of many journalists and advocates I spoke with:

There are some serious limitations as far as using encryption goes right now, one of the primary ones is that using it may scare people off. They may think they are doing something wrong just by attempting to use it, and that's why ultimately, the long term goal is to make encryption ubiquitous so that it's involved in all communications we use and that people don't even notice the difference... Because everyone is using it, the stigma attached to it becomes much less.

Irrespective of the journalistic beat, some sources view encryption with suspicion. Even if the journalist trusts the tools, if the source won't use them, the conversation cannot be secured.

The journalists usually need to meet their sources where they are—speaking to them by email, text message, phone calls, or in person. Many of the journalists would not go through the effort of encrypting their communications unless it was absolutely necessary.

For many investigative journalists, security is an assumed part of their work. Tools and techniques can be understood as a “security toolbox” from which journalists can draw at any time. Yet, few use their security toolbox constantly. For many of the journalists, digital security is about readiness, anticipation, and selective deployment of strong responses.

5.4.7 Other Security Considerations

While sophisticated security techniques are interesting points of conversation, passwords are perhaps the weakest link in online security. Hackers can easily guess passwords with programs that will automatically cycle through a dictionary of countless passwords. As a general rule, short and predictable passwords can take minutes or seconds to guess with password cracking software. Many journalists will use lengthy, randomized passwords or complex passphrases to help secure their accounts. Password management software (e.g., 1Password, KeePass) provides users with a straightforward suite to randomize and store long passwords, as well as to automatically fill out websites with login information.

While some online forms may only require a single password—a single “factor”—a growing number of Web-based tools and services support multi-factor login authentication for stronger security. In general, multi-factor authentication requires that users have access to both something they know (typically their password), and something they own (e.g., a mobile device). Facebook, Twitter, Google, and Dropbox support two-factor authentication, and more services will likely follow suit in the future. It is technically possible to bypass multi-factor authentication (Schneier, 2009), but the approach is a significant obstruction to most attackers.

5.5 Secrecy and Invisible Surveillance

While many of the journalists are increasingly aware of surveillance, there exist few clear confirmations that they have been directly monitored. Multiple reporters told me that their news organizations have become increasingly careful about information security because they are aware of many cases where journalists' phone records have been seized. In circles of national security reporters, the Justice Department's 2013 seizure of phone records from the Associated Press (see section 4.2) signaled that their phone records could be collected at any time.

Ted: I think we're all totally aware that they can get access to our email and phone records both with very little difficulty, and the telephone companies are working closely with them.

It is unclear whether such practices are commonplace, but in the case of the *Associated Press* leak investigation, the organization was not informed that their records were being collected. Because the surveillance is often conducted in secret, without informing the person or institution being monitored, it can be difficult to contest. Nick told me:

The stuff with the AP was covered in the press. My understanding is that their phone records were collected without them knowing. The AP Washington Bureau—two years ago maybe... Well, it was quite a stink, and has led to a degree of reform under at least the Holder administration and the Justice Department. Because, okay, the government can make an effort to grab your records, but that's different than saying we don't even have a chance to object to it if it's done in secrecy.

Some of the national security journalists, through personal experience, learned that their phone records are readily available in leak investigations. Ted recounted instances when prosecutors targeted him in a string of high-profile federal investigations.

I've been the subject of [multiple] major national leak investigations, and that has certainly changed how I communicate with sources if the material is extremely sensitive. I learned from those investigations that it's extremely easy for the government to get my phone records.

The government can compel the recipient of a leak to disclose information about the leak

through a search warrant or subpoena, can capture their communications as they occur (e.g., wiretaps), or can request the data from third parties (Lerner & Bar-Nissim, 2014). In his case, Ted refused to share evidence that would give away the identities of his sources, but it ultimately did not matter. The government went directly to Ted's phone company and gathered the records independently.

Confirmed seizures of journalists' electronic records are somewhat rare. Electronic surveillance can be conducted invisibly, without the subject noticing. With so few confirmations, it can be nearly impossible to tell if they are being monitored. However, both real and imagined surveillance can make some journalists feel as though they are constantly monitored outside of their professional lives.

5.6 Outside of Work

Reporters were generally willing to share information about their professional activities—often, activities they've already published on, and that have already been exposed to the public. I scarcely asked about their security habits in their personal lives. However, occasionally we did explore their concerns with surveillance beyond work.

In one unusual case, one interviewee worked with colleagues who had access to highly sensitive documents. Her colleagues were the focus of multiple U.S. federal investigations. After traveling outside of the country to visit her colleagues, she found that she was stopped consistently when visiting airports. She subsequently became more alarmed about surveillance in her personal life.

I get freaked out Web browsing sometimes... It's completely changed my pornography habits! I'm terrified now! This is something that [her colleague] and I talk about a lot. It's not what you say publicly—that's not what they get you on. It's the stuff that you do in private. It's the very personal secret. It's like how you interact with anonymous Web boards, and who you send your nude pictures to. That's the stuff, if another person were to know, I would flip out. [If someone were to say] "Oh, you wrote this in an article, oh

you tweeted it,” yeah, that’s public, whatever. It’s the stuff that I don’t want public, or that I don’t engage in as a public person that freaks me out.

I asked if she used any privacy measures (e.g., anonymity software) to counter potential eavesdropping on her browsing. She told me that she did not, suggesting that she did not know how to use the tools, and protested that she should not have to use security software.

I don’t know how to use Tor! I’m kind of like, well, whatever, because I’m not doing anything illegal. I’m not purchasing drugs off of Silk Road. It’s not like any of the pornography that I’m looking at is illegal... But somebody knows that I’m looking at this right now.

Tor Browser can be relatively easy to use but can also be intimidating—even to journalists. She told me a story of an instance where her boyfriend contemplated downloading a pirated copy of a television program off of the filesharing website, the *Pirate Bay*. While the site hosts a great deal of legitimate content, it also attracts people who use the platform to host and download pirated copies of copyrighted content, including movies and music.

My boyfriend is sometimes like, “Oh I’ll just get this [television show] off Pirate Bay, and I’m like, don’t do that, don’t do that! They even say stuff like that at work... Be smart; don’t needlessly put us at risk. So I’m like, we need to buy that off iTunes!

While his experience is remarkable, Glenn Greenwald offered a parallel insight. Following his primary reporting in the Snowden leaks, he has been more careful about his communications outside of work. He is careful not to talk about anything sensitive in places where he suspects that he could be monitored.

I would never have any remotely sensitive conversation on an unencrypted phone line. I won’t say much of anything if I’m communicating with somebody using unencrypted email. We’re even careful in our home and in our car about the things we talk about. If there’s something sensitive to discuss, we’ll just pick a place that’s really difficult to eavesdrop on. So of course, when you’re involved in a story like this or other ones, you have the responsibility to take real precautions. But you want to avoid being paranoid and being over the top with concerns, but you definitely want to err on the side of being secure.

Greenwald highlighted the challenge of finding balance between reasonable “real precautions” as opposed to “being over the top.” Because digital threats are often imperceptible, negotiating this balance is quite difficult. The opacity of electronic surveillance leads to the perception that surveillance does not stop when leaving work. For some journalists it is never clear, even in their own homes, whether they are being watched.

5.7 Technology Companies and Surveillance in Journalism

In the above sections, we have seen that some journalists are concerned about the electronic records they leave in the hands of their telephone company, email, social media, and instant messaging services. Nonetheless, out of necessity, convenience, or routine, the use of consumer technologies is increasingly embedded in American journalism.

Many news organizations rely on the same few consolidated services to manage their internal communications. For example, Ashkan Soltani (previously with the *Washington Post*) found that 12 of the 25 largest news websites relied on Gmail or Microsoft Outlook as their internal email platform (Pepitone, 2014). Many news organizations use email services alongside a suite of tools for instant messaging, calendars, editing documents, and file sharing. When I asked Nick if he trusted information technology companies with his work-related data, he said he assumed that his conversations with sources could always be available for scrutiny in the future when the data are accessible to companies. He was more concerned with the U.S. government than the companies themselves. It is entirely possible that a company could be subpoenaed for his conversations with sources. Knowing the possibilities, he regularly provides misleading electronic records when speaking with sensitive sources:

Even though my company uses Microsoft Outlook email, I don't really think that Microsoft is going to read my email. I think that the business embarrassment for them if they were discovered doing that is extremely high... It doesn't really bother me. What I worry about more is that the commercial collection creates data repositories that the

government could lay its hands on, if they wanted to. So again, email, Google Maps, my Verizon phone tracking me where I am all the time, those things do worry me. If I was going to meet a secret, secret source, obviously I would leave my phone behind.

Melanie was more outspoken than many other journalists about consumer privacy. Citing the Snowden disclosures, she said she was concerned about online tracking by information technology companies involved in the PRISM program. Much like Nick, she does not entirely trust the companies, but continued to use their services nonetheless.

I [used to find] Google to be kind of a neutral entity. Same with Yahoo—not that I've ever used Yahoo. I want to say that those were just neutral players. Ah, they sell my data to companies that want to advertise to me, and whatever. But ever since [the Snowden disclosures] I've been like, you guys are evil. Does that mean I've stopped Google searching? No. But I no longer believe them.

Large technology firms in Silicon Valley have had strained relationships with the government in light of the ongoing NSA disclosures. At the time, high-profile cyberattacks on companies including Sony (Cook, 2014) and the health insurer Anthem (Nelson, 2015) culminated in massive leaks of personal data of millions of U.S. consumers. Against the backdrop of escalating cyberattacks and mounting distrust of the government following Snowden's disclosures, the Obama administration and the intelligence communities increasingly worked to maintain dialogues with Silicon Valley leaders (Yadron & Paletta, 2015). In February 2015, the Administration organized a "Cybersecurity Summit" at Stanford University to meet with information technology business leaders. A few key players including Google and Yahoo declined to participate in the event. President Obama spoke about the evolving nature of U.S. cybersecurity, stressing the need for mutual cooperation between the government and technology companies. He did not mention the elephant in the room—that the government legally compelled the compliance of many of the largest Silicon Valley technology companies in untargeted surveillance of their users. Apple's CEO Tim Cook confronted the issue and spoke at length

about the need to protect consumer privacy (Paletta & Yadron, 2015; Yadron & Paletta, 2015).

Alex told me that he was reassured that the companies did not appear cozy with the government. He and other technology reporters followed the Cybersecurity Summit closely, commenting that they were skeptical of the Administration, particular in light of emerging leaks about Western intelligence agencies breaking into the systems of technology companies. Shortly after the event, the NSA and its British counterpart, the GCHQ, were revealed to have breached a multinational phone hardware company, Gemalto, and to have stolen encryption keys that the corporation used to secure the communications of cell phone users around the world (Scahill & Begley, 2014). As Alex recounted, the symbolic irony of the Cybersecurity Summit was not lost on him:

It's comforting to see so many business leaders stand up to the NSA and the President who is actively trying to convince industry leaders, tech leaders, to cooperate with the government in information-sharing. He launched a new agency with the intention of setting up a central data-sharing hub for cyberthreats, and has coded that with the idea that it's all about consumer protection. Obviously, a week later we find out that they're hacking into private companies and compromising their security, so I think he has some egg on his face this week.

Silicon Valley is becoming a powerful political hub, and press advocacy organizations value their proximity to the companies. Because the companies have profound influence over the privacy protections for users around the world, advocacy organizations can be incentivized to network with technology companies within the Bay Area. Furthermore, world-renowned academic institutions with strong ties to Bay Area technology companies are nearby, funneling well-educated students into positions with information technology companies. A press advocate named Paul told me:

There's a reason why I'm based in San Francisco... This is where the position is for a reason. I'm [nearby] Twitter; I'm a 45-minute drive from Facebook, Google, 30 from Berkeley, 45 from Stanford, roughly. It's really clustered here, except for—I don't know, Tumblr is in New York? A great deal of the infrastructure is here. The economic and

financial infrastructure is largely here.

The advocates lean on technology companies to better support their most vulnerable users, including journalists and activists. Michael, an executive at a press advocacy organization, told me that he felt technology companies have a responsibility to protect their users “as much as legally possible.” He writes often about the need for technology companies to support encryption in their products. He urged companies to support end-to-end encryption, referring to encryption standards that allow only the sender and intended recipient to decrypt a message. Even if a company receives a legal order for communications on their servers, if they are end-to-end encrypted, the company would not have the appropriate keys to decode the conversation.

Information technology companies wield power to encrypt the communications of millions of people simultaneously, without them even knowing. For example, in late 2014 the mobile messaging app, WhatsApp, deployed the TextSecure protocol with the help of Open Whisper Systems—the developer of Signal and TextSecure, both used to encrypt text messages (Newman, 2014). WhatsApp’s decision to integrate end-to-end encryption delivered substantially stronger security for hundreds of millions of people with nearly no additional effort demanded of its users. In late 2014, Google and Apple similarly announced plans to encrypt Android phones and iPhones by default (Kravets, 2014; Timberg, 2014). When technology companies enable encryption by default, journalists and ordinary consumers both enjoy the security benefits.

5.8 American Journalism in Global Context

U.S. journalists and reporters who operate in English-speaking countries can typically assume that they will be able to use technologies created by large technology firms in their work. This is not necessarily true in non-Western countries. With her Silicon Valley-based digital rights

advocacy organization, the Electronic Frontier Foundation, Eva Galperin had worked with multiple news organizations and press advocacy groups. She had worked with journalists internationally, including in Ethiopia and Vietnam—both countries where activists and journalists have been targeted with commercial hacking software (Marquis-Boire et al., 2013).

The most common populations that I work with are generally journalists and activists. So often it's very difficult to tell the difference between these two things in many countries, especially in countries where independent journalism essentially is activism.

A significant part of her work is alerting Silicon Valley companies to interventions that could help vulnerable journalists and activists. As she told me, “One of the reasons we are here, and not in Washington D.C., is that we believe we can affect change through the companies.” Galperin shared one example of a well-known Ethiopian news organization called Ethiopian Satellite Television (ESAT), one of the few remaining independent news organizations in the country’s tightly controlled media environment. Some ESAT journalists are based in the United States. As an independent news organization, they are at times critical of the Ethiopian government. She learned from a researcher working with ESAT that the government was using commercial surveillance tools to monitor the journalists.

The way that they would do it is that they would send phishing emails with attachments, and the attachments would be infected, and the infection would spread to their computer. We found some of the infected attachments... The security researcher told these guys, “Please stop opening attachments on your computer! If you want to not re-infect yourself all the time, you should go into Google Docs and open these attachments in Google Docs... A couple of months go by, and he talks to the guys at ESAT, and they’re all infected again. So what part of “don’t open these attachments” don’t you understand?

It was not simply a matter of understanding the instructions of the security specialists. Rather, Google Docs did not support Amharic, the Ethiopian written language. The journalists continued to open the attachments on their machines so that they could read documents and do their work. Upon learning this, Galperin approached Google with the information, and only a couple of

months later, Google began to support Amharic.

In addition to technical support, U.S. journalists enjoy an incredible level of protection from government intervention in their reporting. As Nick pointed out, “Even the Brits don’t get the protections of the First Amendment. American journalists are incredibly privileged.” I spoke with a journalist, “Nathra,” who worked with a Middle Eastern newswire and was temporarily living in the United States. She requested that I avoid using identifying details about any of the groups she worked with. Nathra worked in regions that, in her words, fall into the “failed state spectrum.” She observed that American news organizations have recently become much more aware of surveillance since Snowden’s disclosures and newfound legal pressure against journalists and their sources under the Obama administration’s Justice Department. While these issues are increasingly salient in American journalism, many Middle Eastern regions have long understood surveillance as a fact of life:

There’s a difference between, the worst that can happen is I can be held in contempt—which is bad too—and you can get blown up on your way in the morning. Which sounds like a crock, but it’s true. From 2005-2009, there were assassinations targeting journalists and activists in [Lebanon]. So it is different, I would say. However, the awareness that you’re being watched, and the awareness that, you know, I’m not going to carry a smartphone, I’m going to carry an old black and white mobile phone. I mean yeah, we see that happening here.

In her work, sources are quite different than sources in the United States. Within senior levels of the U.S. government, sources may be concerned with the threat of legal reprisal when speaking with journalists. In contrast, her sources spoke with journalists in order to call attention to their desperate situations in her war-torn region.

Once your back is against the wall, they’re not afraid any more. Even if they’re caught... Will they reach out? Yeah, they reach out, they’re being bombed anyway.

Surveillance was an afterthought for some of the activists and informants who shared information with her. Although they assumed the government monitored the platform, sources

reached out to share information with her through Facebook. In regions where Nathra worked, surveillance simply became an expected part of life. It's difficult to be concerned with surveillance when they are more concerned with physical danger:

My assumption in life in general is that everything is being watched, I'm not kidding... It's not like, okay, I have to be careful at work. But I wasn't particularly more stressed or annoyed than I have been in life because [a neighboring country] was under a dictatorship and [my country] was right next door... Surveillance is not new to many parts of the world. They live with it every day. Journalists and non-journalists alike, of course it's exacerbated for journalists and activists, but it's there for everyone. They live with it.

During our interview, Nathra recounted a story in which Nokia Siemens sold surveillance software to the Bahraini government. The software allowed the government to remotely monitor Bahraini human rights activists. She forwarded me an article about the story, including interviews with the Bahraini activists. One activist reported that he was detained and beaten with rubber hoses in interrogations that went on for months, from August 2010 to February 2011. He reported that he was questioned by an official who showed him his own mobile text message records and "details from personal mobile phone conversations." (Silver & Elgin, 2011) In countries where she reports, Nathra pointed out that this kind of surveillance has long been used to monitor and undercut dissent among politically active citizens. As a consequence, her sources had to assume that they were routinely the subjects of surveillance. Some of the most well-documented cases of commercial surveillance involve Bahrain (Marquis-Boire et al., 2013), as well as Egypt (Kimball, 2015) and Ethiopia (Marczak et al., 2014; Marquis-Boire et al., 2013).

How journalists attempt to resist surveillance depends significantly on their local political climate, yet it is also clear that practices of surveillance are increasingly globalized through sales of commercial surveillance software. Journalists also straddle their local and global climate through the use of online platforms. Multinational companies Google and Facebook offer their

services to users around the world at little or no monetary cost, allowing journalists and ordinary users to globally publicize information about their local concerns. Many American journalists have only recently begun to pay close attention to surveillance, but elsewhere—particularly in politically volatile regions—surveillance is a fact of life.

Section 3. Synthesis

Chapter 6

Discussion: Key Factors for Resisting Surveillance

As we have seen, modern forms of surveillance are increasingly marked by the pervasive collection, aggregation, and analysis of data by an assemblage of organizations, including international corporate and government actors. Journalists who work with confidential sources must take an ecological view of surveillance, calculating what data may broadcast about their communications and assessing potential threats to their personal data. Those potential threats increasingly involve the use of consumer technologies that collect personal data by default.

As investigative journalists become aware of surveillance in its many forms, reporters can foreclose data access to present and future eavesdroppers by using disposable cell phones, pay phones, third party phones, encryption tools, and anonymization software, and through face-to-face meetings that can help to minimize their electronic records. They may find it necessary to use airgapped computers and disposable operating systems (e.g., Tails) to securely open documents and to avoid malware. However, as discussed in chapter 5, journalists apply information security tools and techniques in highly selective and context-dependent fashions. For example, if a story is not sensitive and depends on routine sources, many journalists will not put in the added effort of securing their communications. Information security practices have substantial costs—time, effort, and money, among other inconveniences. Additionally, many journalists suggest they have little need for such approaches in their routine work. It is therefore important to explore key factors in journalists' choices to selectively adopt security tools and techniques.

6.1 Selective Security Approaches in Investigative Journalism

Even within the same reporting beats, or when working with similar sources, journalists will have divergent approaches to managing their personal data. No two people are the same. Two

national security journalists within the same news institution may have quite different philosophies about speaking with sources in a relatively secure fashion. Journalists also have divergent opinions about the efficacy of their information security approaches.

Information security habits are shaped by the particular context faced by the journalist. For the purposes here, “context” refers to the dynamically changing conditions around the journalist that influence their work. Context should not be understood as static, but instead, under constant renegotiation (Bauman & Lyon, 2013; Dourish, 2003). Learning new information can provide new context, and new context can provide new topics that journalists may wish to investigate. The reflexive relationship between learning and context is foundational to their behavior. In my interviews, I found that three primary factors influenced journalists to impede surveillance: (1) awareness of surveillance, (2) motivation to stem the disclosure of information, and (3) the perception of costs.

Awareness. The person must be *aware* of surveillance and its perceived mechanisms to assess how to respond. For example, when speaking with sources through text messages, journalists must be aware that the telephone company maintains electronic records of those messages. Likewise, they must know that the telephone company is obliged to respond to legal requests that could reveal their messages.

Motivation. The person must have sufficient *motivation* to slow or prevent disclosure of information. For example, the journalist may or may not be highly motivated to secure their instant messaging conversations while chatting with personal and professional contacts.

Perceived costs. The person will perceive that impeding surveillance has costs. Encryption tools, for example, may be seen as costly because they require time and effort to learn and master. The tools can sometimes be inconvenient, or may carry financial costs. However, there may also be

social costs—for example, I spoke to journalists concerned that the use of security software could make them appear paranoid. Even if highly motivated, a journalist may choose not to secure a conversation if their sources find the tools inconvenient or intimidating. As a consequence, it is often easier to simply chat with sources however they feel most comfortable—ordinary phone calls, instant messaging, email, and so on. Journalists inevitably find costs for security approaches, but when they are aware of how to do so, they may be highly motivated to secure their conversations and personal data.

The above three factors can be used to explain individual decision-making in relation to subjective conditions of learning and context. All three conditions are necessary to stir someone to resist surveillance. I describe how the above three factors help us understand journalists' selective information security practices.

6.1.1 Awareness of Surveillance and its Conditions

As Foucault described, people are often unaware of when they are being watched, and the lack of clarity can feel deeply disempowering (Foucault, 1977). The problem is further exacerbated in contemporary systems of electronic surveillance, where the conditions for being monitored are often ambiguous. Those systems should not be understood as disembodied, but rather, rendered imperceptible to the subject of surveillance. The underlying mechanisms aren't often visible to most people—hardware composed of computers tied together by the sinew of underground fiber optic cables, distributed satellites, and cell phone towers. These physical components are typically unclear to ordinary users.

Brunton and Nissenbaum (2013) argue that the invisibility of surveillance yields fundamental power asymmetries between the watcher and the watched:

The asymmetry problems to which we alluded above are, first, an asymmetry of power: rarely do we get to choose whether or not we are monitored, what happens to information

about us and what happens to us because of this information. We have little or no say when monitoring takes place in inappropriate contexts and is shared inappropriately with inappropriate others. The second asymmetry, equally important, is epistemic: we are often not fully aware of the monitoring, and do not know what will become of the information produced by that monitoring, nor where it will go and what will be done with it. (p. 166)

Schneier (2015) asserts that modern surveillance is often invisible because it is embedded in technologies that are not fundamentally surveillance technologies, but rather, allow surveillance as a byproduct of their intended function. As he argues, information technology businesses will collect data about their customers by necessity. Every social media website, phone call, text message, and financial exchange must leverage information about users in order to allow communications to take place. A smartphone must collect information about where the user is, and must yield information about the call recipient to the phone company and intervening cell phone towers in order to connect the call. Even without nefarious purposes, companies often must surveil users. How the consumer data are used in practice is often unclear. Surveillance is thus everywhere and nowhere simultaneously, existing both as a requirement and a potential, making it largely imperceptible without extraordinary vigilance.

It is challenging to be aware of surveillance and its mechanisms because they are so often covert or simply undisclosed. For example, the American public would know much less about untargeted U.S. surveillance without Edward Snowden's disclosures. Indeed, the NSA's surveillance authorities rest on laws interpreted in relative secrecy within the intelligence community. Public officials argue that these systems require secrecy to avoid giving clues to foreign adversaries, terrorists, criminals, and other actors who could potentially learn to circumvent surveillance techniques. Corporate actors also depend on secrecy for the competitive advantage of their products. Again, education is critically important for making informed decisions to counter surveillance, but it isn't always clear how to assess surveillance with so little

information about its basic political and technical mechanisms.

Today, information security professionals work closely with journalists to teach them to wield tools to impede surveillance, whether from government institutions, consumer technology companies that host their phone calls or emails, or their Internet service provider. Journalists might also be concerned with keeping their data out of the hands of remote hackers or unwanted acquaintances. Threat modeling is perhaps the first lesson most information security specialists will teach, and yet threat modeling depends on awareness of surveillance and its mechanisms. It can often be quite difficult to predict what information security practices are most appropriate.

I found that journalists receive few confirmations about when they are being directly monitored. In the context of government surveillance, some journalists spoke of being stopped or having their bags searched at airports, and in other cases finding sophisticated monitoring software on their machines. Total awareness is not possible. Nonetheless, I found that many journalists are highly motivated to learn more about information security and to integrate new approaches into their toolkit.

6.1.2 Motivation for Security Approaches

Journalists can be highly motivated to employ information security practices for the protection of their newsroom, their sources, and their own personal data. Depending on the nature of their work and preferences, they may have altogether different motivations for using security tools and techniques. I want to highlight two motivators in particular: privacy-enhancing tools and techniques can (1) impede unwanted eavesdroppers and data thieves, and (2) also represent a statement of political opposition to surveillance.

Some journalists use information security tools and techniques as a matter of principle, as well as to connect with their sources. They are typically mindful of their security habits and may

leverage a variety of tools. For example, journalists covering technology or cybersecurity often work with technically savvy sources who use privacy-enhancing tools as a political statement, representing what Joh (2013) called a “privacy protest.” While the tools may be ideal for communications with a highly sensitive source, those instances are somewhat rare. The tools are not simply a pragmatic way to connect with their sources, but rather, serve to demonstrate a shared understanding of information security more broadly.

While individual journalists may be highly motivated to take security measures in their personal reporting, they may have colleagues who are less concerned and less motivated to use security approaches. Without sufficient motivation, a strong security posture feels needless and burdensome. Reporters assess the likelihood of their data being compromised according to the nature of their story, their sources, and the information being exchanged. If they are reporting on a highly sensitive topic, they may be more motivated to consider heightened security measures.

Many news organizations also provide training for journalists, instructing vigilance and highlighting best practices to prevent their machines from being compromised. A single computer can have access to a news institutions’ internal infrastructure, for example its intranet or email services. In practice, a newsroom’s security is only as strong as its weakest link. Unfortunately, the practice of developing information security skills and knowledge is often an ad hoc endeavor (McGregor et al., 2015). When it comes to security, journalists often act as “lone wolves.” The individualistic nature of their information security behaviors can often be at odds with the collective nature of security in the newsroom.

One reason journalists manage their information security so individually is that their data can be hosted by their news institution as well as on their own devices. Their data are distributed across their institutional infrastructure, email clients, Web activities, and phone records. Of

course, like anyone else, reporters have personal data that they wish to keep to themselves, and they may keep sensitive information on personal devices.

Finally, source attribution is a central motivator for adopting information security practices (Human Rights Watch & ACLU, 2014). A breach of their computers or networks could reveal information about confidential sources. However, U.S. investigations involving the phone records of the Associated Press (Savage & Kaufman, 2013) demonstrate that legal orders can yield information about confidential sources. If a source requests to speak anonymously or on background, journalists usually take the responsibility to respect attribution quite seriously. In national security reporting, for example, journalists work with the government in both official channels (e.g., through a Public Information Office) and through unsanctioned channels. With government sources, providing unsanctioned information, and in some cases participating in any unsanctioned conversation with a journalist, can be problematic. However, many government sources simply prefer to speak on background out of habit, even when they are providing entirely sanctioned information. Regardless of the source's reasoning, journalists are often motivated to protect sources because they intend to develop long-term relationships that may yield regular streams of information for their reporting. Respecting source attribution serves the goal of ensuring that the source returns for future reporting. Information security, in effect, becomes a vehicle for managing the integrity of their data and ensuring that attribution is properly upheld.

6.1.3 Costs of Action

When confronted with the possibility that they may need to secure communications with sources or take countermeasures against potential surveillance, journalists envision the appropriate security approaches. However, these approaches are usually perceived to add costs to journalists' work. There are no universal costs, but rather, costs are related to the journalists' specific

situation and security needs. For example, they may need specific types of security tools and methods when working on a particular story, or depending on the type of source they are working with, their relationship to the source, and the information being exchanged. Additionally, journalists may learn new information that influences their decisions to adopt security measures. The costs of using security approaches are unpredictable and context-dependent.

The costs of adopting information security tools and techniques are not usually about money. Many of the most popular security tools and protocols are maintained by networks of software developers who collectively publish their code, host the security tools, and make the tools accessible to the general public for free. Sometimes, convenient security tools used by journalists require a subscription fee (e.g., Silent Circle). The costs are not prohibitive for news organizations that support investigative journalism, which itself can be quite expensive.

Instead of financial costs, the most obvious costs of security take the form of inconveniences to routine work, characterized by lost time and effort. Security techniques can require highly specific knowledge and maintenance of elaborate software. Some of the journalists described how they investigated security approaches themselves and also received formal training from specialists. In other cases, they might look for selective help as needed. Their time is at a premium, and learning to use security methods can often divert attention from other tasks that are important to them. As a consequence, they may prefer not to use security tools when the required time and effort is out of proportion for their needs. As long as journalists must take security into their own hands, their personal investment of time and effort will never go away.

Security-enhancing communication tools are not very useful for protecting sources if

sources won't use them. Even the most widely adopted communication tools suffer from this fundamental challenge—what Carl Shapiro and Hal Varian dubbed *network effects*. In their words, “Network effects arise when the value one user places on a good depends on how many other people are using it” (Shapiro & Varian, 2013, p. 45). Many of the journalists described speaking to their sources over the phone, social media accounts (e.g., Twitter), and consumer chat software (e.g., Google Hangout) because those are the places that their sources can be conveniently reached. Conversely, national security or technically inclined sources may have already adopted PGP or Signal on their smartphone, thus enabling relatively secure conversations without much additional investment for the source. However, the journalists with whom I spoke typically wouldn't ask their sources to use communication tools that they did not already use. In other words, network effects constrain the communication channels that are available between journalists and their sources.

Many Americans actively decline to use security tools to manage their personal data because they are concerned that doing so will invite further scrutiny, or because they have “nothing to hide” (Madden, 2015). Pew Research found that 49% of Americans believe that it is acceptable for the U.S. government to monitor a person who has used encryption software to hide files (Shelton et al., 2015). Unfortunately, stigma, fear, and misunderstanding of security tools can exacerbate network effects, ultimately making effective security approaches far less valuable than they could be for source protection. Many journalists simply won't ask their sources to use the tools unless they believe the source desperately needs to. Even if a tool is cryptographically sound, secure communication software will not help if the source does not use it.

Journalists and their sources must confront tools that are often poorly designed and

challenging to use. Journalists who set up PGP typically do not ask their sources to do so because—having done so themselves—they are aware of how daunting the setup procedure can be. Additionally, PGP and many communication tools like it will not encrypt information about the authors of the communications. To ensure confidentiality, a journalist must ask their source to use PGP *and* an anonymization tool such as Tor. Setting up encrypted and anonymous communications can be intimidating for the uninitiated. Without sufficient motivation and know-how, it is impractical and difficult to secure oneself.

In practice, the problems of usable security tools are two-fold: (1) Usable security tools are underutilized, and (2) the tools require too much effort for journalists and their sources. This is no revelation to journalists familiar with security tools. Throughout this investigation, I spoke with a growing chorus of security researchers, developers, and electronic policy advocates and journalists who agree that usability represents a serious challenge for securing communications. So what can human-computer interaction researchers and technologists do?

At a conference aimed at developing user trust in data security, the security specialist Bruce Schneier proclaimed, “Twenty years of PGP has taught us that one-click encryption is one click too many” (Rosenblatt, 2014). Schneier’s comment turned out to be prescient, with a growing wave of consumer electronics companies enabling end-user encryption by default, and without any additional input from users. In 2014, Google and Apple declared that they would encrypt Android and iPhone mobile devices by default. Apple has begun doing so in newer models of mobile devices (Kravets, 2014; Reilly & Sledge, 2014). Shortly after Apple’s and Google’s announcements, a popular mobile messaging application called WhatsApp (owned by Facebook) integrated default end-to-end encryption into its platform, thereby boosting the security of communications for hundreds of millions users around the world (Newman, 2014).

All three companies' decisions elevated security their services in ways largely imperceptible to their users.

Security researchers disagree on the efficacy of these companies' efforts. For example, Kobeissi (2015) argued that WhatsApp's end-to-end encryption is insufficient because it can be circumvented through technical attacks. In particular, WhatsApp does not allow users to verify that their messages are going to the intended recipient. An unwitting user can encrypt their message to the attacker, who may then encrypt and forward the message to its intended recipient. The two legitimate conversational participants would not be aware that a "man in the middle" could listen to their fully encrypted conversation. To thwart man-in-the-middle attacks, PGP and OTR allow users to verify that users are speaking to their intended recipients, but for the moment, WhatsApp does not. For that reason, WhatsApp's encryption may not be sufficient for high-risk users who may be targeted in digital attacks. For ordinary users, however, the changes offered by WhatsApp represent opportunities for heightened security with little or no additional effort, thus diminishing the costs for those users.

I have described a host of costs to the adoption of information security approaches. The most pressing concerns for journalists include inconveniences, time, effort, technical problems, network effects, and the stigma attached to security practices themselves. When working with sensitive information, investigative journalists are forced to overcome these enormous hurdles.

6.2 Acts of Resistance

The journalists made creative uses of telephones, software tools, computing hardware, and face-to-face meetings with sources to disrupt potential eavesdroppers. I have argued that journalists have both pragmatic and principled reasons to resist surveillance, and in spite of the costs, can be highly motivated to do so. In the end, their knowledge, their particular context, their motivations,

and the perceived costs of security efforts will either fail or succeed to stir them to action.

Some journalists described awkward positions that emerge when asking sources to use encryption, or when considering countersurveillance. Indeed, many do not *want* to use elaborate security approaches, but feel they have to. As one reporter interviewed for the ACLU and Human Rights Watch report (2014) asserted, “There’s something about using elaborate evasion and security techniques that’s offensive to me—that I should have to operate like a criminal, like a spy” (p. 46). To suspicious law enforcement and government officials, impeding surveillance may appear to indicate criminality, as the same techniques may be used to skirt the law (Brunton & Nissenbaum, 2013; Galetta, 2014; Joh, 2013). For example, a growing chorus of intelligence and law enforcement officials are increasingly concerned about the prospect of potential leads on “bad guys” collectively “going dark” through the growth of default smartphone encryption (O’Brien, 2015). Journalists complicate these narratives not only by conducting lawful work, but through their practical and ethical considerations for sources (Deuze, 2005; Ettema & Glasser, 1998). For some journalists, security can be a burden on their broader work—a speed bump that slows their ability to connect with sources and colleagues as well as their ability to publish. Information security can slow the work that they care about, and yet they resist surveillance because they feel they have the responsibility to do so.

Many journalists use information security approaches because it’s seen as a practical way to protect their sources. However, they also have largely principled reasons to do so. Joh (2013) described principled resistance as “privacy protests” whereby people use evasive methods to undermine surveillance as a political critique. She described a range of activities that closely mirror the behaviors of journalists when connecting with sensitive sources: paying with cash, using disposable burner phones, using Tor for anonymous information exchange, and other

behaviors. For example, many of the journalists and advocates I spoke with preferred to use encryption methods to communicate as a matter of principle. They use security approaches to make a political statement, even when they don't have a personal need to do so.

While the aims and various forms of countersurveillance techniques might be similar, they represent distinct security approaches. Multiple scholars have attempted to provide meaningful categories of resistance to surveillance. For example, Marx (2003) described eleven “moves” for neutralizing and resisting contemporary forms of surveillance. Other scholars have explored the political goals and outcomes of resistance (Brunton & Nissenbaum, 2013; Scott, 1985). For instance, in a study of welfare auditing, Gilliom (2005) described welfare mothers who defy state surveillance by strategically hiding their possessions, relationships, and personal finances.

For the purposes here, I focus on Schneier's (2015, pp. 214-219) four categories of resistance to mass surveillance. In a critical analysis of contemporary surveillance, he provides a relatively simple outline for describing how people impede surveillance in contemporary practices of “big data” collection, aggregation, and analytics. Schneier categorizes resistant behaviors into the following four categories: avoiding, blocking, breaking, and distorting surveillance.

Avoiding surveillance means declining to participate in electronic recordkeeping. Typically such approaches involve the use of alternative technologies or services to minimize electronic records from transactions. For example, journalists may avoid surveillance by using analog approaches when conducting their work. They may pay for news-related transactions with cash rather than their credit card. Likewise, they may send and receive physical mail rather than email. They may similarly choose to jot down notes rather than type them into their electronic devices. However,

avoidance tactics may imply refraining from certain activities, for example, declining to use cloud services to store certain types of files, avoiding certain topics of conversation, or withholding information during phone calls. Journalists might choose to move sensitive conversations to alternative communication channels. Likewise, they may avoid electronic communications in favor of a face-to-face setting.

Blocking means using privacy-enhancing technologies that can help to render data collection practices less useful or to prevent data collection altogether. For example, browser plug-ins such as Privacy Badger, Disconnect, Ghostery, and Flashblock will block browser-based tracking cookies. In so doing, the plug-in denies tracking data to advertising companies.

Breaking surveillance involves undermining surveillance systems. While avoiding and blocking are defensive, breaking is offensive. For example, a person can break surveillance by using a can of spray paint to obscure a camera's lenses, or by attacking a surveillance system through technical vulnerabilities (Schneier, 2015). However, breaking surveillance often conflicts with the law. Among the journalists with whom I spoke, I saw no evidence of breaking surveillance.

Distorting surveillance is sometimes called *obfuscation*. In their research, Brunton and Nissenbaum (2011) describe obfuscation as “the production of misleading, ambiguous and plausible but confusing information as an act of concealment or evasion.” Investigative journalists can be extraordinarily creative in their obfuscation practices. Some journalists provide misleading information in their phone activities by using disposable burner phones, calling dozens of people in succession to obscure the target of their call, and calling from others' phones. Public locations (e.g., a pub) may similarly provide the appearance of chance encounters for planned meetings with sources. Some journalists prefer to speak with sources in noisy locations to make eavesdropping difficult. The Tor anonymity network represents another

example of digital obfuscation. Tor obscures the location of individual users by shuffling their traffic within its distributed network before they get to their destination (e.g., a website). To the website, the user will appear to come from an altogether different IP address than their location—perhaps from a different country. The anonymous file drop box platform, SecureDrop, is built on top of Tor’s architecture, allowing tipsters a relatively secure point of communication with journalists. Tor’s method of obfuscation allows users to communicate or send files and tips to journalists anonymously.

Brunton and Nissenbaum (2013) argued that practices of obfuscation need not be digital, but can also be terrestrial. For instance, to obscure their location, World War II pilots dropped aluminum-coated strips of paper from their planes when passing over German watch posts to confuse German radar systems with a flood of fake targets.

Brunton and Nissenbaum argue that obfuscation asymmetrically benefits the less politically powerful over the more politically powerful. People with less political power, they argue, typically have fewer options at their disposal than the more politically powerful. While Brunton and Nissenbaum intended to describe power asymmetries that may be confronted specifically through obfuscation, their logic also applies to parallel forms of resistance to surveillance described by Schneier (2015, pp. 214-219). Avoiding, blocking, and breaking surveillance are all practices oriented to diminishing power asymmetries between the watchers and the watched.

The distinction between Schneier’s categories can often be subtle, and different countersurveillance methods can ultimately serve the same goal. For example, I spoke with journalists who have taken different approaches to impeding phone surveillance when meeting with sources in person. They can remove the battery from their phone before meeting a source in

person (blocking phone surveillance) or alternatively leave their phone at home, thus attempting to avoid surveillance. In both cases, the journalist subsequently attempts to avoid surveillance by meeting in person.

It is important to highlight that the above categories describe *perceived* resistance, rather than successful resistance. It is quite possible that countersurveillance approaches can be overcome, or they can be unsuccessful. For example, turning off a phone at the same time as a source may tip off suspicious authorities, transforming a security-enhancing approach into a red flag.

One challenge with Schneier's schema is that resistance is often quite subtle and can involve paradoxical tactics. For instance, many reporters who are aware of surveillance in their own work consider strategic inaction to be a tactic for avoiding further surveillance. Some of the journalists pointed out that security techniques—for example, the use of communications encryption—could be a “red flag” that can call attention to a conversation with sources. In turn, paradoxically, they may attempt to avoid surveillance by leaving their messages *unsecured*. In other words, everyone else's ordinary text messages, phone calls, chat messages, and emails become their camouflage of choice. This “strategic compliance” can represent simultaneous resistance to, and observation of surveillance.

Chapter 7

Conclusion

To protect themselves and their sources, journalists employ diverse information security practices to secure information in the face of surveillance and data breaches. They use both standard methods recommended by security experts and their own ad hoc approaches. Some investigative journalists have adopted elaborate methods to protect their sources—avoiding online communications and meeting in person, arranging meetings with disposable “burner” phones instead of their personal phones, and using encryption software to scramble their communications to potential eavesdroppers (Human Rights Watch & ACLU, 2014; Pew Research Center, 2015). Some journalists (e.g., technology reporters) are more likely than others to use privacy-protecting communication channels (e.g., encrypted phone calls) if their sources are familiar with the tools. However, most of the journalists did not use information security approaches for routine work.

My interviews likely overrepresent journalists with elaborate information security knowledge and journalists who have spoken publicly on issues of surveillance. Likewise, the journalists almost certainly withheld substantial information during our interviews. I nonetheless found a wide range of perspectives on surveillance and practices for managing information security. Because the group most likely overrepresents journalists with broad knowledge of security practices, it is striking how selectively they deploy these approaches in their work.

To be effective guardians of their information, journalists must be aware of their digital threats, must be sufficiently motivated to impede those threats, and must overcome the perceived costs of doing so. The present context and personal knowledge of their situation are crucial factors as well. For journalists, context is closely tied to the stories they want to develop for publication. In the course of conducting research, as well as communicating with colleagues and

sources, I found that journalists made decisions about when to (and when not to) deploy information security approaches. However, for many journalists information security can slow down their workflow, distracting from their real interest—reporting the news. Surveillance and potential information breaches are especially problematic when journalists seek to keep their sources confidential. Their work drives them to learn more about security, but data interception is typically invisible, making it difficult to preempt surveillance. For many journalists, it isn't always clear what situations merit information security practices, and implementing them typically slows down their work.

Compared with previous literature (e.g., Human Rights Watch & ACLU, 2014), I found that journalists employ sophisticated communication security tools and techniques quite selectively. In particular:

1. The journalists attempted to prepare for potential sources to speak to them over secure channels as they develop specific stories, or to exchange particularly sensitive information. However, routine work does not demand sophisticated information security practices.
2. Many reporters are overburdened from the outset. Using information security tools and techniques can be costly, requiring significant time and effort to learn and maintain.
3. Many journalists prefer not to use information security tools and techniques when they do not have to, because the tools can be difficult to use.

First, the journalists described specific situations when they felt they needed to use sophisticated security approaches; these situations involved work on a sensitive story or exchanging highly sensitive information. Previous research suggests that face-to-face meetings are one of the most common approaches for speaking to sources about sensitive information (Pew Research Center, 2015). When working on less sensitive stories, many of the journalists

described speaking to sources over the phone, text messages, email, consumer chat programs, and social media websites. The journalists attempted to speak to sources wherever they could, despite concerns about interception of their data. In other words, communications are usually driven by sources (McGregor et al., 2015).

Second, security approaches are often costly, requiring considerable time and effort to set up and maintain. Most of the journalists have busy schedules dictated by an unpredictable news cycle and a regular flow of deadlines. As a consequence, few privacy-protecting habits are simple enough to implement for regular use. However, a few methods require little sustained effort. For example, some journalists encrypt their computer and phone hard drives, keep lengthy passwords, and use privacy-enhancing browser plug-ins. These approaches require little additional work after some initial effort, compared to most other techniques that take more time and effort to learn and require continued maintenance. For example, the journalists develop more complex toolboxes that can be deployed selectively, making use of email and instant messaging encryption, privacy-protecting operating systems, anonymity software, and burner phones. Some journalists avoid electronic records by withholding certain topics of conversation online, meeting sensitive sources in person, hand-delivering (or receiving) sensitive documents, and paying for work-related expenses in cash. Less frequently, some use disposable operating systems (e.g., Tails) and airgapped computers to open sensitive documents. Depending on the nature of their sources, the nature of the story they are developing, and the information under threat in the course of their work, the tools in their information security toolboxes are always available. I found that many investigative journalists didn't fish through their security toolboxes as a matter of routine, but were instead prepared for ideal moments to deploy security tools and techniques to protect themselves and their sources.

Finally, even highly motivated journalists were often unhappy about using certain types of security tools because they are unnecessarily difficult to use and understand—for example, PGP email encryption. Usability is a serious challenge for countless communication tools. Network effects further exacerbate the problem. When usability problems discourage users, they are not affected in isolation; the people around them may not use privacy- and security-enhancing communication tools either.

There is a silver lining: A small but growing number of security tools represent stronger design ideals. For example, many of the journalists used the iPhone mobile application, Signal, to encrypt their phone calls and text messages, with design quality comparable to their mobile devices' default messaging services. Compared to complicated security software and standards, many of the journalists described feeling more comfortable asking their sources to use encrypted communications when the tools were relatively easy to use.

Taking security measures requires effort and time. On the infrastructural level, encryption protocols can be deployed in the background of software invisibly and by default. In so doing, developers allow users to connect with one other while thwarting unwanted eavesdropping. By enabling unobtrusive encryption by default, developers can allow heightened security with relatively little change in users' outward experiences of software. For example, HTTPS-encrypted website connections protect users from third party eavesdropping with relatively little change in their experience of the website. Similarly, WhatsApp's support for end-to-end message encryption can protect users from potential eavesdroppers (Newman, 2014). Industry technologists are faced with difficult choices about the privacy-enhancing opportunities enabled through the deployment of security measures and whether to deny themselves access to certain

forms of user data. Nonetheless, these examples show that a third party can reduce the costs of security measures unilaterally and with relatively little or no additional effort demanded of users.

Few are as motivated as investigative journalists to take extraordinary information security measures. Journalists demonstrate that lone people, with ad hoc approaches, can manage selective disclosure of their personal data. However, to lower the extraordinary costs of resisting contemporary electronic surveillance, we require bottom-up security measures and techniques for lone users, as well as top-down administrative and technical infrastructure driven by industry players that can protect customers from leaking personal data. These bottom-up and top-down approaches represent not only technical but also policy interventions that should be understood in relation to one another. It is incumbent on researchers, policymakers, and technologists to collaboratively develop tools, techniques, and theory in response to practices of informational resistance.

References

- Ackerman, S. (2015, May 21). FBI used Patriot Act to obtain “large collections” of Americans’ data, DoJ finds. *The Guardian*. Retrieved from <http://www.theguardian.com/us-news/2015/may/21/fbi-patriot-act-doj-report>
- Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday*, 13(3). Retrieved from <http://firstmonday.org/ojs/index.php/fm/article/view/2142>
- Allen, D. S. (2008). The trouble with transparency. *Journalism Studies*, 9(3), 323–340.
- Anderson, C. (2008). Journalism: Expertise, authority, and power in democratic life. *The Media and Social Theory*, 248–64.
- Anderson, N. (2013, March 11). Meet the men who spy on women through their webcams. *Ars Technica*. Retrieved March 17, 2015, from <http://arstechnica.com/tech-policy/2013/03/rat-breeders-meet-the-men-who-spy-on-women-through-their-webcams/>
- Andrejevic, M. (2002). The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society*, 2(4). Retrieved from <http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3359>
- Andrejevic, M., & Gates, K. (2014). Big data surveillance: Introduction. *Surveillance & Society*, 12(2), 185–196.
- Angwin, J., Savage, C., Larson, J., Moltke, H., Poitras, L., & Risen, J. (2015, August 15). AT&T helped U.S. spy on Internet on a vast scale. *The New York Times*. Retrieved from <http://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html>

- Apuzzo, M. (2015a, January 12). Legal fight ends for James Risen of the New York Times. *The New York Times*. Retrieved from <http://www.nytimes.com/2015/01/13/us/times-reporter-james-risen-will-not-be-called-to-testify-in-leak-case-lawyers-say.html>
- Apuzzo, M. (2015b, January 26). C.I.A. Officer guilty in leak tied to reporter. *The New York Times*. Retrieved from <http://www.nytimes.com/2015/01/27/us/politics/cia-officer-in-leak-case-jeffrey-sterling-is-convicted-of-espionage.html>
- Armao, R. (2000). The history of investigative reporting. In B., Marilyn Greenwald & J. Bernt (Eds.), *The big chill: Investigative reporting in the current media environment* (pp. 35–50).
- Aucoin, J. L. (2006). *The evolution of American investigative journalism*. University of Missouri Press.
- Bahajji, Z. A., & Illyes, G. (2014, August 6). HTTPS as a ranking signal. Google online security blog. Retrieved from http://googleonlinesecurity.blogspot.com/2014/08/https-as-ranking-signal_6.html
- Ball, J., Borger, J., & Greenwald, G. (2013, September 6). Revealed: how US and UK spy agencies defeat internet privacy and security. Retrieved December 4, 2014, from <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>
- Bauman, Z., & Lyon, D. (2013). *Liquid surveillance: A conversation*. John Wiley & Sons.
- Beckett, L. (2014, June 13). Everything we know about what data brokers know about you. *ProPublica*. Retrieved from <http://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you>

- Bernt, J., & Greenwald, M. (2000). Enterprise and investigative reporting in metropolitan newspapers: 1980 and 1995 compared. In M. Greenwald & J. Bernt (Eds.), *The big chill: Investigative reporting in the current media environment*, 1.
- Bigo, D. (2006). Globalized (in)security: The field and the ban-opticon. *Illiberal practices of liberal regimes: The (In)security games, L'Harmattan: Paris*, 5–49.
- Bivins, T. H. (2014). The language of virtue : What can we learn from early journalism codes of ethics? In W. N. Wyatt (Ed.), *The Ethics of Journalism: Individual, Institutional and Cultural Influences*. I.B. Tauris.
- Bogard, W. (2006). Surveillance assemblages and lines of flight. In D. Lyon (Ed.), *Theorizing surveillance: The panopticon and beyond*. Routledge.
- Bonforte, J. (2014, January 7). HTTPS now default in Yahoo mail. Retrieved from <http://yahoomail.tumblr.com/post/72588816144/https-now-default-in-yahoo-mail>
- Borland, J. (2013, December 30). Don't want your laptop tampered with? Just add glitter nail polish. Retrieved April 1, 2015, from <http://www.wired.com/2013/12/better-data-security-nail-polish/>
- Bossewitch, J., & Sinnreich, A. (2013). The end of forgetting: Strategic agency beyond the panopticon. *New Media & Society*, 15(2), 224–242.
- Brunton, F., & Nissenbaum, H. (2011). Vernacular resistance to data collection and analysis: A political theory of obfuscation. *First Monday*, 16(5). Retrieved from <http://firstmonday.org/ojs/index.php/fm/article/viewArticle/3493>
- Brunton, F., & Nissenbaum, H. (2013). Political and ethical perspectives on data obfuscation. In M. Hildebrandt & K. de Vries (Eds.), *Privacy, Due process and the computational turn: The philosophy of law meets the philosophy of technology*. Routledge.

- Carlson, M. (2011a). *On the condition of anonymity: Unnamed sources and the battle for journalism*. University of Illinois Press.
- Carlson, M. (2011b). Whither anonymity? Journalism and unnamed sources in a changing media environment. In B. Franklin & M. Carlson (Eds.), *Journalists, sources and credibility: New perspectives* (pp. 37–48). Retrieved from <http://www.caerdydd.ac.uk/jomec/resources/foj2009/foj2009-Carlson.pdf>
- Clarke, R. (1988). Information technology and dataveillance. *Commun. ACM*, 31(5), 498–512.
- Cohen, D. (2013, July 31). HTTPS is now the default for all Facebook users. Retrieved March 28, 2015, from <http://www.adweek.com/socialtimes/https-default/426092>
- Committee to Protect Journalists. (2012). *CPJ journalist security guide: Covering the news in a dangerous and changing world*. Retrieved from <https://www.cpj.org/reports/2012/04/information-security.php>
- Committee to Protect Journalists. (2014a). *China is world's worst jailer of the press; Global tally second worst on record*. Retrieved from <https://www.cpj.org/reports/2014/12/journalists-in-prison-china-is-worlds-worst-jailer.php>
- Committee to Protect Journalists. (2014b). *CPJ's 2014 global impunity index spotlights countries where journalists are slain and the killers go free*. Retrieved from <https://www.cpj.org/reports/2014/04/impunity-index-getting-away-with-murder.php>
- Davis, M. (2010). Why journalism is a profession. In C. Meyers (Ed.), *Journalism Ethics: A Philosophical Approach* (pp. 91–102). Oxford University Press.
- De Burgh, H. (2000). *Investigative journalism: Context and practice*. Psychology Press.
- Deleuze, G., & Guattari, F. (1988). *A thousand plateaus: Capitalism and schizophrenia*. Bloomsbury Publishing.

- Deuze, M. (2005). What is journalism? Professional identity and ideology of journalists reconsidered. *Journalism* 6(4), 442–464.
- Devereaux, R., Greenwald, G., & Poitras, L. (2014). Data pirates of the Caribbean: The NSA is recording every cell phone call in the Bahamas. *The Intercept*. Retrieved from <https://firstlook.org/theintercept/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/>
- Devine, T. M., & Katz, S. L. (2014). The national security whistleblower's tightrope: The legal rights of government employees and contractors. In P. Rosenweig, T. J. McNulty, & E. Shearer (Eds.), *Whistleblowers, leaks, and the media: The First Amendment and national security* (pp. 81–105). American Bar Association Publishing.
- Dourish, P. (2003). What we talk about when we talk about context. *Personal and Ubiquitous Computing* 8(1), 19–30.
- Downie, L., & Schudson, M. (2009, October 19). The reconstruction of American journalism. *Columbia Journalism Review*. Retrieved February 3, 2015, from http://www.cjr.org/reconstruction/the_reconstruction_of_american.php
- Drum, K. (2013, May 21). How the world's dullest story became the target of a massive leak investigation. Retrieved February 22, 2015, from <http://www.motherjones.com/kevin-drum/2013/05/how-worlds-dullest-story-became-target-massive-leak-investigation>
- Eckersley, P., & Schoen, S. (2014, October 6). How CloudFlare moved the Web toward ubiquitous HTTPS. *Electronic Frontier Foundation*. Retrieved December 10, 2014, from <https://www.eff.org/deeplinks/2014/10/how-cloudflare-moved-web-toward-ubiquitous-https>

- Edgar, H., & Schmidt, B. (1973). The espionage statutes and publication of defense information. *Columbia Law Review*, 73, 929.
- Electronic Frontier Foundation. (2015a). Jewel v. NSA. Retrieved February 4, 2015, from <https://www.eff.org/cases/jewel>
- Electronic Frontier Foundation. (2015b, February 4). Surveillance self-defense: Tips, tools and how-tos for safer online communications. Retrieved November 10, 2014, from <https://ssd.eff.org/en>
- Electronic Privacy Information Center. (2014). FISA court orders 1979-2014. Retrieved April 6, 2015, from https://epic.org/privacy/wiretap/stats/fisa_stats.html
- Ettema, J. S., & Glasser, T. L. (1998). *Custodians of conscience: Investigative journalism and public virtue*. Columbia University Press.
- FDR Group, P. A. (2013). Chilling effects: Nsa surveillance drives us writers to self-censor. *PEN America*. Retrieved from <http://www.pen.org/chilling-Effects>
- FDR Group, P. A. (2015). *Global Chilling: The impact of mass surveillance on international writers*. *PEN America*. Retrieved from <http://pen.org/global-chill>
- Foucault, M. (1977). *Discipline and punish: The birth of the prison*. (A. Sheridan, Trans.). New York: Vintage.
- Franklin, B., & Carlson, M. (2011). *Journalists, sources, and credibility: New perspectives*. Routledge.
- Freedom of the Press Foundation. (2013, July 2). Encryption works: How to protect your privacy in the age of NSA surveillance. Retrieved November 10, 2014, from <https://freedom.press/encryption-works>

- Fung, B. (2013, August 31). The NSA hacks other countries by buying millions of dollars' worth of computer vulnerabilities. *The Washington Post*. Retrieved from <http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities/>
- Galetta, A. (2014). New surveillance, new penology and new resistance: Towards the criminalisation of resistance? In *Reloading Data Protection* (pp. 101–114). Springer. Retrieved from http://link.springer.com/chapter/10.1007/978-94-007-7540-4_6
- Gallagher, K. (2014, September 12). Fifteen months after the NSA revelations, why aren't more news organizations using HTTPS? *Freedom of the Press Foundation*. Retrieved December 10, 2014, from <https://freedom.press/blog/2014/09/after-nsa-revelations-why-arent-more-news-organizations-using-https>
- Gallagher, R. (2014, December 4). Operation AURORAGOLD: How the NSA hacks cellphone networks worldwide. *The Intercept*. Retrieved from <https://firstlook.org/theintercept/2014/12/04/nsa-auroragold-hack-cellphones/>
- Gans, H. J. (1979). *Deciding what's news: A study of CBS Evening News, NBC Nightly News, Newsweek, and Time*. Northwestern University Press.
- Gellman, B., & Poitras, L. (2013, June 7). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. *The Washington Post*. Retrieved from http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html
- Gellman, B., & Soltani, A. (2013, October 30). NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. *The Washington Post*. Retrieved from

http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

Gilliom, J. (2005). Resisting surveillance. *Social Text*, 23(2 83), 71–83.

Glaser, B. G., & Strauss, A. L. (1967). *The discovery of Grounded Theory: Strategies for qualitative research*. Transaction Publishers.

Gordon, M., & Mendoza, M. (2014, March 3). AT&T, Verizon and Sprint push back against the NSA, too. Retrieved November 11, 2014, from

http://www.huffingtonpost.com/2014/03/03/att-verizon-sprint-nsa_n_4891533.html

Greenwald, G. (2013a). XKeyscore: NSA tool collects “nearly everything a user does on the internet.” *The Guardian*. Retrieved November 21, 2014, from

<http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>

Greenwald, G. (2013b, June 6). NSA collecting phone records of millions of Verizon customers daily. Retrieved November 11, 2014, from

<http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. Metropolitan Books.

Greenwald, G., & MacAskill, E. (2013, June 6). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Retrieved from

<http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>

Haan, Y. de, Landman, A., & Boyles, J. L. (2014). Towards knowledge-centered newswork: The ethics of newsroom collaboration in the digital era. In W. N. Wyatt (Ed.), *The Ethics of Journalism: Individual, institutional and cultural influences*. I.B. Tauris.

- Habermas, J. (1991). *The structural transformation of the public sphere: An inquiry into a category of bourgeois society*. (T. Burger, Trans.). MIT Press.
- Hafez, K. (2002). Journalism Ethics Revisited: A comparison of ethics codes in Europe, North Africa, the Middle East, and Muslim Asia. *Political Communication*, 19(2), 225–250.
- Haggerty, K. D. (2006). Tear down the walls: on demolishing the panopticon. (2006): 23-45. In *Theorizing surveillance: The panopticon and beyond* (pp. 23–45). Willan Publishing.
- Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *The British Journal of Sociology*, 51(4), 605–622.
- Hallin, D. C., Manoff, R. K., & Weddle, J. K. (1993). Sourcing patterns of national security reporters. *Journalism & Mass Communication Quarterly*, 70(4), 753–766.
- Hamilton, J. M., & Krinsky, G. (1996). *Hold the press: The inside story on newspapers*. LSU Press.
- Hampton, K., Rainie, L., Lu, W., Dwyer, M., Shin, I., & Purcell, K. (2015). Social media and the “spiral of silence.” Pew Research Center Internet, Science, and Technology Project. Retrieved from <http://www.pewinternet.org/2014/08/26/social-media-and-the-spiral-of-silence/>
- Hanitzsch, T. (2007). Deconstructing journalism culture: toward a universal theory. *Communication Theory*, 17(4), 367–385.
- Hanitzsch, T. (2009). Comparative journalism studies. In K. Wahl-Jorgensen & T. Hanitzsch (Eds.), *The Handbook of Journalism Studies* (pp. 413–427). Routledge.
- Hanitzsch, T., Hanusch, F., Mellado, C., Anikina, M., Berganza, R., Cangoz, I., Yuen, E. K. W. (2011). Mapping journalism cultures across nations. *Journalism Studies*, 12(3), 273–293.

- Harris, S. (2012, August 22). Who's watching the N.S.A. watchers? *The New York Times*. Retrieved from <http://www.nytimes.com/2012/08/23/opinion/whos-watching-the-nsa-watchers.html>
- Hencke, D. (2000, July 24). A little mole told me - honest. *The Guardian*. Retrieved from <http://www.theguardian.com/media/2000/jul/24/mondaymediasection.pressandpublishing>
- Henrichsen, J. R., Betz, M., & Lisosky, J. M. (2015). Building digital safety for journalism: A survey of selected issues. *UNESCO*. Retrieved from http://www.unesco.org/new/en/media-services/single-view/news/building_digital_safety_for_journalism_unesco_launches_a_new_publication/
- Human Rights Watch. (2014a). *US surveillance harming journalism, law, democracy: Government spying undermines media freedom and right to counsel*. Retrieved from <https://www.hrw.org/news/2014/07/28/us-surveillance-harming-journalism-law-democracy>
- Human Rights Watch. (2014b, March 25). Ethiopia: Telecom surveillance chills rights. Retrieved December 12, 2014, from <http://www.hrw.org/news/2014/03/25/ethiopia-telecom-surveillance-chills-rights>
- Human Rights Watch & ACLU. (2014, July 28). With liberty to monitor all: How large-scale US surveillance is harming journalism, law, and American democracy. Retrieved August 17, 2014, from <http://www.hrw.org/node/127364>
- Jaycox, M., & Kayyali, N. (2015, May 31) Section 215 expires—for now. *Electronic Frontier Foundation*. Retrieved June 1, 2015, from <https://www EFF.org/deeplinks/2015/05/section-215-expires-now>

- Joh, E. E. (2013). Privacy protests: Surveillance evasion and Fourth Amendment suspicion. *Arizona Law Review* 55, 997.
- Columbia Journalism School. *Journalism after Snowden: In defense of leaks - A lecture with Jill Abramson*. (2014). Retrieved from <https://www.youtube.com/watch?v=ueDd-Vkvkzg>
- Keeble, R. (2008). *Ethics for journalists*. Routledge.
- Kerr, O. S. (2012). The mosaic theory of the Fourth Amendment. *Michigan Law Review* 111, 311.
- Kimball, S. (2015, March 9). After Arab Spring, surveillance in Egypt intensifies. *The Intercept*. Retrieved from <https://firstlook.org/theintercept/2015/03/09/arab-spring-surveillance-egypt-intensifies/>
- Kobeissi, N. (2015, April 10). How WhatsApp needs to improve its encryption. Retrieved from <http://blog.nadim.computer/post/115940264683/how-whatsapp-needs-to-improve-its-encryption>
- Konigsburg, E., Pant, R., & Kvochko, E. (2014, November 13). Embracing HTTPS. *New York Times Open Blog*. Retrieved December 10, 2014, from <http://open.blogs.nytimes.com/2014/11/13/embracing-https/>
- Krause, M. (2011). Reporting and the transformations of the journalistic field: US news media, 1890-2000. *Media, Culture & Society*, 33(1), 89–104.
- Kravets, D. (2009, July 15). Obama claims immunity, as new spy case takes center stage. *Wired*. Retrieved May 25, 2015, from <http://www.wired.com/2009/07/jewel/>
- Kravets, D. (2013, June 27). NSA leak vindicates AT&T whistleblower. *Wired*. Retrieved November 21, 2014, from <http://www.wired.com/2013/06/nsa-whistleblower-klein/>

- Kravets, D. (2014, September 25). Apple, Google default cell-phone encryption “concerns” FBI director. *Ars Technica*. Retrieved November 10, 2014, from <http://arstechnica.com/tech-policy/2014/09/apple-google-default-cell-phone-encryption-concerns-fbi-director/>
- Larson, J., Perlroth, N., & Shane, S. (2013, September 5). Revealed: The NSA’s secret campaign to crack, undermine Internet security. *ProPublica*. Retrieved December 4, 2014, from <http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption>
- Lee, M. (2015a, January 27). How to leak to the Intercept. *The Intercept*. Retrieved from <https://firstlook.org/theintercept/2015/01/28/how-to-leak-to-the-intercept/>
- Lee, M. (2015b, April 27). Encrypting your laptop like you mean it. *The Intercept*. Retrieved from <https://firstlook.org/theintercept/2015/04/27/encrypting-laptop-like-mean/>
- Lerner, J. I., & Bar-Nissim, R. (2014). *Law enforcement investigations involving journalists*. In Ellen Shearer, Paul S. Rosenzweig and Timothy J. McNulty (Eds) Whistleblowers, leaks and the media: The First Amendment and national security.
- Liptak, A. (2014, June 2). Supreme Court rejects appeal from Times reporter over refusal to identify source. *The New York Times*. Retrieved from <http://www.nytimes.com/2014/06/03/us/james-risen-faces-jail-time-for-refusing-to-identify-a-confidential-source.html>
- Los, M. (2006). Looking into the future: Surveillance, globalization and the totalitarian potential. In D. Lyon (Ed.), *Theorizing surveillance: The panopticon and beyond*. Routledge.
- Lunden, I. (2013, April 10). Facebook launches partner categories, 500+ generic profiles to Target ads better, with data From Datalogix, Epsilon, Acxiom. *TechCrunch*. Retrieved from <http://techcrunch.com/2013/04/10/facebook-launches-partner-categories-500->

profiles-to-target-ads-better-on-mobile-and-desktop-using-data-from-datalogix-epsilon-and-axciom/

Lyon, D. (2003). *Surveillance after September 11* (Vol. 11). Polity.

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society*, 1(2). Retrieved from <http://bds.sagepub.com/content/1/2/2053951714541861>

Maass, P. (2015a, February 18). Stephen Kim spoke to a reporter. Now he's in jail. This is his story. *The Intercept*. Retrieved from <https://firstlook.org/theintercept/2015/02/18/destroyed-by-the-espionage-act/>

Maass, P. (2015b, May 11). CIA's Jeffrey Sterling sentenced to 42 months for leaking to New York Times journalist. *The Intercept*. Retrieved from <https://firstlook.org/theintercept/2015/05/11/sterling-sentenced-for-cia-leak-to-nyt/>

Madden, M. (2014). Public perceptions of privacy and security in the Post-Snowden era. Pew Research Center Internet, Science, and Technology Project. Retrieved from <http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/>

Madden, M. (2015, April 14). Why some Americans have not changed their privacy and security behaviors. *Pew Research Center Fact Tank Blog*. Retrieved from <http://www.pewresearch.org/fact-tank/2015/04/14/why-some-americans-have-not-changed-their-privacy-and-security-behaviors/>

Marczak, B., Guarnieri, C., Scott-Railton, J., & Marquis-Boire, M. (2014, February 12). Hacking Team and the targeting of Ethiopian journalists. *Citizen Lab*. Retrieved from <https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists/>

- Marquis-Boire, M., & Hardy, S. (2012, June 19). Syrian activists targeted with BlackShades spy software. *Citizen Lab*. Retrieved from <https://citizenlab.org/2012/06/syrian-activists-targeted-with-blackshades-spy-software/>
- Marquis-Boire, M., Marczak, B., Guarnieri, C., & Scott-Railton, J. (2013, April 30). For their eyes only: The commercialization of digital spying. *Citizen Lab*. Retrieved from <https://citizenlab.org/2013/04/for-their-eyes-only-2/>
- Marthews, A., & Tucker, C. (2014). Government surveillance and Internet search behavior. *Available at SSRN*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564
- Marwick, A. E. (2012). The public domain: Social surveillance in everyday life. *Surveillance & Society*, 9(4), 378–393.
- Marx, G. T. (1988). *Undercover: Police surveillance in America*. University of California Press.
- Marx, G. T. (2003). A tack in the shoe: Neutralizing and resisting the new surveillance. *Journal of Social Issues*, 59(2), 369–390.
- Masco, J. (2014). *The theater of operations: National security affect from the Cold War to the war on terror*. Duke University Press.
- Mathiesen, T. (1997). The viewer society: Michel Foucault’s “panopticon” revisited. *Theoretical Criminology*, 1(2), 215–234.
- McGregor, S. E., Charters, P., Holliday, T., & Roesner, F. (2015). Investigating the computer security practices and needs of journalists. In *Proceedings of the 24th USENIX Security Symposium, 2015*.
- Mitchelstein, E., & Boczkowski, P. J. (2009). Between tradition and change: A review of recent research on online news production. *Journalism*, 10(5), 562–586.

- Muller, M. (2014). Using curiosity, creativity, and surprise as analytic tools: Grounded theory method as a way of knowing in HCI. In *Ways of Knowing in HCI*. Heidelberg: Springer-Verlag.
- Nakashima, E. (2010, July 14). Former NSA executive Thomas A. Drake may pay high price for media leak. *The Washington Post*. Retrieved from <http://www.washingtonpost.com/wp-dyn/content/article/2010/07/13/AR2010071305992.html>
- Newell, B. C. (2013). The massive metadata machine: Liberty, power, and secret mass surveillance in the U.S. and Europe. *I/S: A journal of law and policy for the information society* 10(2), 481–522.
- Newell, B. C., & Tennis, J. T. (2013). Me, my metadata, and the NSA: Privacy and government metadata surveillance programs. *Proceedings of iConference 2014* 345–55.
- Newman, L. H. (2014, November 18). WhatsApp is the first major messaging service to add strong end-to-end encryption. *Slate*. Retrieved from http://www.slate.com/blogs/future_tense/2014/11/18/whatsapp_adds_textsecure_end_to_end_encryption_by_partnering_with_open_whisper.html
- Nissenbaum, H. (1997). Toward an approach to privacy in public: Challenges of information technology. *Ethics & Behavior*, 7(3), 207–219.
- Nissenbaum, H. (1999). The meaning of anonymity in an information age. *The Information Society*, 15(2), 141–144.
- Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79, 119.
- O'Brien, K. J. (2015). How journalists should reframe the encryption debate. *Columbia Journalism Review*. Retrieved from http://www.cjr.org/behind_the_news/how_journalists_are_fighting_t.php

O'Connor, J. D. (2005, May 31). "I'm the guy they called deep throat." *Vanity Fair*. Retrieved from <http://www.vanityfair.com/news/politics/2005/07/deepthroat200507>

Office of the Director of National Intelligence. (2013, December 21). DNI announces the declassification of the existence of collection activities authorized by President George W. Bush shortly after the attacks of September 11, 2001. Retrieved February 4, 2015, from <http://icontherecord.tumblr.com/post/70683717031/dni-announces-the-declassification-of-the>

Office of the Director of National Intelligence. (2014, December 12). The Department of Justice releases additional documents concerning collection activities authorized by President George W. Bush shortly after the attacks of September 11, 2001. Retrieved December 12, 2014, from <http://icontherecord.tumblr.com/post/105032620703/the-department-of-justice-releases-additional>

Office of the Director of National Intelligence. (2015, February 27). Joint statement by the Department of Justice and the Office of the Director of National Intelligence on the declassification of renewal of collection under Section 215 of the USA PATRIOT Act (50 U.S.C. Sec. 1861). Retrieved February 27, 2015, from <http://icontherecord.tumblr.com/post/112255431548/joint-statement-by-the-department-of-justice-and>

Office of the Press Secretary. (2014a, January 17). Presidential policy directive - signals intelligence activities. Retrieved May 23, 2015, from <https://www.whitehouse.gov/node/253456>

- Office of the Press Secretary. (2014b, March 27). Fact Sheet: The Administration's proposal for ending the Section 215 bulk telephony metadata program. Retrieved February 24, 2015, from <http://www.whitehouse.gov/node/267741>
- Paletta, D., & Yadron, D. (2015, February 11). White House to create new division to streamline cyberthreat intelligence. *Wall Street Journal*. Retrieved from <http://www.wsj.com/articles/white-house-to-create-new-division-to-streamline-cyberthreat-intelligence-1423572846>
- Pepitone, J. (2014, March 24). Digital rights group slams Microsoft for reading blogger's Hotmail. *NBC News*. Retrieved from <http://www.nbcnews.com/tech/security/digital-rights-group-slams-microsoft-reading-bloggers-hotmail-n60561>
- Perloth, N. (2013, February 1). Washington Post joins list of news media hacked by the Chinese. *The New York Times*. Retrieved from <http://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html>
- Peterson, A. (2014, March 7). Snowden: I raised NSA concerns internally over 10 times before going rogue. *The Washington Post*. Retrieved from <http://www.washingtonpost.com/blogs/the-switch/wp/2014/03/07/snowden-i-raised-nsa-concerns-internally-over-10-times-before-going-rogue/>
- Pew Research Center. (2015). *Investigative journalists and digital security*. Retrieved from <http://www.journalism.org/2015/02/05/investigative-journalists-and-digital-security/>
- Policinski, G. (2014). First Amendment considerations on national security issues: From Zenger to Snowden. In P. Rosenweig, T. J. McNulty, & E. Shearer (Eds.), *Whistleblowers, leaks,*

- and the media: The first amendment and national security* (pp. 63–79). American Bar Association Publishing.
- Powers, A., & Fico, F. (1994). Influences on use of sources at large US newspapers. *Newspaper Research Journal*, 15(4), 87–97.
- Prince, M. (2014, September 29). Introducing universal SSL. Retrieved December 10, 2014, from <http://blog.cloudflare.com/introducing-universal-ssl/>
- Privacy and Civil Liberties Oversight Board. (2014). *Report on the telephone records program conducted under Section 215 of the USA PATRIOT Act and on the operations of the Foreign Intelligence Surveillance Court*. Retrieved from https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf
- Rafsky, S. (2013). The Obama administration and the press. *Committee to Protect Journalists*. Retrieved from <https://www.cpj.org/reports/2013/10/obama-and-the-press-us-leaks-surveillance-post-911.php>
- Rafsky, S. (2014). One year after CPJ’s US report, little has changed between Obama and press. *Committee to Protect Journalists*. Retrieved from <https://cpj.org/blog/2014/10/one-year-after-cpjs-us-report-little-has-changed-b.php>
- Freedom of the Press Foundation. *Real-world encryption problems*. (2014). Retrieved from <https://www.youtube.com/watch?v=JktB6h-qnKA>
- Reich, Z. (2011a). Source credibility and journalism. *Journalism Practice*, 5(1), 51–67.
- Reich, Z. (2011b). Source credibility as a journalistic work tool. In B. Franklin & M. Carlson (Eds.), *Journalists, Sources, and Credibility: New Perspectives* (pp. 19–48). Routledge.
- Reilly, R. J., & Sledge, M. (2014, October 16). FBI director calls on congress to “fix” phone encryption by Apple, Google. *Huffington Post*. Retrieved December 10, 2014, from

http://www.huffingtonpost.com/2014/10/16/james-comey-phone-encryption_n_5996808.html

Reporters Committee for Freedom of the Press. (2014). Number of states with shield law climbs to 40. Retrieved May 25, 2015, from <https://www.rcfp.org/browse-media-law-resources/news-media-law/news-media-law-summer-2011/number-states-shield-law-climbs>

Reporters Without Borders. (2014). *Biggest rises and falls in the 2014 World Press Freedom Index*. Retrieved from <http://rsf.org/index2014/en-index2014.php>

Reporters Without Borders. (2015, February 12). World press freedom index 2015: Decline on all fronts. Retrieved February 12, 2015, from <http://index.rsf.org>

Rettberg, J. W. (2014). *Seeing ourselves through technology: How we use selfies, blogs and wearable devices to see and shape ourselves*. Palgrave Macmillan.

Rosenblatt, S. (2014, February 27). TrustyCon's RSA conference rebels promise more to come. *CNET*. Retrieved April 17, 2015, from <http://www.cnet.com/news/trustycons-rsa-conference-rebels-promise-more-to-come/>

Savage, C. (2010, April 28). U.S. subpoenas Times reporter over book on C.I.A. *The New York Times*. Retrieved from <http://www.nytimes.com/2010/04/29/us/29justice.html>

Savage, C. (2013, February 28). Bradley Manning admits providing files to WikiLeaks. *The New York Times*. Retrieved from <http://www.nytimes.com/2013/03/01/us/bradley-manning-admits-giving-trove-of-military-data-to-wikileaks.html>

Savage, C., & Kaufman, L. (2013, May 13). Phone records of journalists of the Associated Press seized by U.S. *The New York Times*. Retrieved from

- <http://www.nytimes.com/2013/05/14/us/phone-records-of-journalists-of-the-associated-press-seized-by-us.html>
- Savage, C., & Weisman, J. (2015, May 7). N.S.A. collection of bulk call data is ruled illegal. *The New York Times*. Retrieved from <http://www.nytimes.com/2015/05/08/us/nsa-phone-records-collection-ruled-illegal-by-appeals-court.html>
- Savage, C., & Wyatt, E. (2013, June 5). U.S. is secretly collecting records of Verizon calls. *The New York Times*. Retrieved from <http://www.nytimes.com/2013/06/06/us/us-secretly-collecting-logs-of-business-calls.html>
- Scahill, J., & Begley, J. (2014, February 19). The great SIM heist: How spies stole the keys to the encryption castle. *The Intercept*. Retrieved from <https://firstlook.org/theintercept/2015/02/19/great-sim-heist/>
- Schneier, B. (2009, September 22). Hacking two-factor authentication. Retrieved from https://www.schneier.com/blog/archives/2009/09/hacking_two-fac.html
- Schneier, B. (2015). *Data and Goliath: The hidden battles to capture your data and control your world* (1st ed.). W. W. Norton & Company.
- Schwartz, M. (2015, January 19). How to catch a terrorist. Retrieved February 25, 2015, from <http://www.newyorker.com/magazine/2015/01/26/whole-haystack>
- Scott, J. C. (1985). *Weapons of the weak: Everyday forms of peasant resistance*. Yale University Press.
- Shane, S. (2010, April 15). Former N.S.A. official is charged in leaks case. *The New York Times*. Retrieved from <http://www.nytimes.com/2010/04/16/us/16indict.html>
- Shane, S. (2011, June 9). Plea deal struck in classified leaks case. *The New York Times*. Retrieved from <http://www.nytimes.com/2011/06/10/us/10leak.html>

- Shapiro, C., & Varian, H. R. (1999). *Information rules: A strategic guide to the network economy*. Harvard Business Press.
- Shelton, M., Rainie, L., Madden, M., Anderson, M., Duggan, M., Perrin, A., & Page, D. (2015). *Americans' privacy strategies post-Snowden*. Pew Research Center Internet, Science, and Technology Project. Retrieved from <http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/>
- Shoemaker, P. J., & Reese, S. D. (1991). Mediating the message: Theories of influences on mass media content. Retrieved from <http://library.wur.nl/WebQuery/clc/564841>
- Sigal, L. V. (1973). *Reporters and officials: The organization and politics of newsmaking*. Rowman & Littlefield.
- Silver, V., & Elgin, B. (2011, August 22). Torture in Bahrain becomes routine with help from Nokia Siemens. *Bloomberg*. Retrieved February 23, 2015, from <http://www.bloomberg.com/news/articles/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking>
- Simon, B. (2005). The return of Panopticism: Supervision, subjection and the new surveillance. *Surveillance & Society*, 3(1).
- Singer, J. B. (2010). Quality control. *Journalism Practice*, 4(2), 127–142.
- Splichal, S., & Sparks, C. (1994). *Journalists for the 21st century: Tendencies of professionalization among first-year students in 22 countries*. Ablex Publishing Corporation.
- Stray, J. (2014). *Threat modeling: Planning digital security for your story*. Retrieved from <https://vimeo.com/87957065>

- Tate, J. (2013, August 20). Bradley Manning sentenced to 35 years in WikiLeaks case. *The Washington Post*. Retrieved from http://www.washingtonpost.com/world/national-security/judge-to-sentence-bradley-manning-today/2013/08/20/85bee184-09d0-11e3-b87c-476db8ac34cd_story.html
- Timberg, C. (2013, July 10). NSA slide shows surveillance of undersea cables. *The Washington Post*. Retrieved from http://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html
- Timberg, C. (2014, September 18). Newest Androids will join iPhones in offering default encryption, blocking police. *The Washington Post*. Retrieved from <http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/>
- Tuchman, G. (1973). Making news by doing work: Routinizing the unexpected. *American Journal of Sociology*, 79(1), 110–131.
- Tye, J. N. (2014a). Why I spoke out against the NSA. *TED*. Retrieved from <https://www.youtube.com/watch?v=ATUoU9B187w>
- Tye, J. N. (2014b, July 18). Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans. *The Washington Post*. Retrieved from http://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html
- Uberti, D. (2015). The looming threat of newsroom cyber attacks. *Columbia Journalism Review*. Retrieved from http://www.cjr.org/behind_the_news/newsroom_cyber_attacks.php

- Wagstaff, J. (2014, March 28). Journalists, media under attack from hackers: Google researchers. *Reuters*. Retrieved from <http://www.reuters.com/article/2014/03/28/us-media-cybercrime-idUSBREA2R0EU20140328>
- Walker, C., & Waters, C. (2015). Learning security: Information security education for journalists. *Tow Center for Digital Journalism*. Retrieved from <http://towcenter.org/research/learning-security-information-security-education-for-journalists/>
- Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193–220.
- Weinberg, S. (1996). *The reporter's handbook: An investigator's guide to documents and techniques*. Macmillan.
- Wemple, E. (2014, October 27). USA Today's Susan Page: Obama administration most “dangerous” to media in history. *The Washington Post*. Retrieved from <http://www.washingtonpost.com/blogs/erik-wemple/wp/2014/10/27/usa-todays-susan-page-obama-administration-most-dangerous-to-media-in-history/>
- Wyatt, W. N., & Clasen, T. (2014). Ethics in the age of the solitary journalist. In W. N. Wyatt (Ed.), *The ethics of journalism: Individual, institutional and cultural influences*. I.B. Tauris.
- Yadron, D., & Paletta, D. (2015, February 13). Cybersecurity Summit exposes Silicon Valley's privacy fears. *Wall Street Journal*. Retrieved from <http://www.wsj.com/articles/cybersecurity-summit-exposes-silicon-valleys-privacy-fears-1423862917>

Youm, K. H. (2009). Journalism law and regulation. In K. Wahl-Jorgensen & T. Hanitzsch (Eds.), *Handbook of Journalism Studies* (pp. 279–294).

Zelizer, B. (1993). Has communication explained journalism? *Journal of Communication*, 43(4), 80–88.