2013

The Problematic of Privacy in the Namespace

Randal Sean Harrison
Michigan Technological University

THE PROBLEMATIC OF PRIVACY IN THE NAMESPACE

By

Randal Sean Harrison

A DISSERTATION

Submitted in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

In Rhetoric and Technical Communication

MICHIGAN TECHNOLOGICAL UNIVERSITY

2013

This dissertation has been approved in partial fulfillment of the requirements for the Degree of DOCTOR OF PHILOSOPHY in Rhetoric and Technical Communication.

Department of Humanities

Dissertation Advisor:	*Dr. Jennifer Daryl Slack*
Committee Member:	*Dr. Patty Sotirin*
Committee Member:	*Dr. Diane Shoos*
Committee Member:	*Dr. Charles Wallace*
Department Chair:	*Dr. Ronald Strickland*

I dedicate this work to my family for loving and supporting me, and for patiently bearing with a course of study that has kept me away from home far longer than I'd wished.

I dedicate this also to my wife Shreya, without whose love and support I would have never completed this work.

Table of Contents

Chapter 1. The Problematic of Privacy....7
1.1 Privacy in Crisis....7
1.2 The Emerging Surveillance Society....11
1.3 Conjunctural Analysis and the Problematic of Privacy....16
1.4 The Namespace....19
1.5 Radical Contextualism and Articulation....21

Chapter 2. A New Public Narrative of Privacy....26
2.1 Privacy in the Popular Media....26
2.2 Ideology and Common Sense....27
2.3 Privacy in the News....31
2.4 Big Brother as Common Sense State....33
2.5 Privacy in Film....46
2.6 Privacy in Video Games....50

Chapter 3. Privacy and Security in the Surveillance State....55
3.1 Societies of Control....55
3.2 The Snowden Revelations....59
3.3 Total Information Awareness....64
3.4 The Nascent Privacy Problematic....69
3.5 Twenty-first Century Statecraft....74

Chapter 4. Privacy and Convenience in the Information Economy....84
4.1 Ambient Findability....84
4.2 The Information Economy....88
4.3 Data Brokerages....91
4.4 Social Networking....93
4.5 The Californian Ideology....95

Chapter 5. Rearticulating the Namespace....97
5.1 Hegemonic Crisis....97
5.2 Individual Praxis....100
5.3 Collective Praxis....103
5.4 Expert Praxis....104
5.5 War of Position....106
5.6 Cultural Studies....111

References....114

Appendix A....138

Acknowledgments

I have been blessed by a community of friends and colleagues at Michigan Technological University. There are too many to name individually, but I count myself blessed to have collaborated with them and shared in their lives.

Most important to my success in graduate school has been my excellent committee, Dr. Jennifer Slack, Dr. Patricia Sotirin, Dr. Diane Shoos, and Dr. Charles Wallace. I can't begin to describe my debt to these four scholars. I am exceedingly grateful for the opportunity to work with them.

Abstract

In the twenty-first century, the issue of privacy—particularly the privacy of individuals with regard to their personal information and effects—has become highly contested terrain, producing a crisis that affects both national and global social formations. This crisis, or problematic, characterizes a particular historical conjuncture I term the namespace.

Using cultural studies and the theory of articulation, I map the emergent ways that the namespace articulates economic, juridical, political, cultural, and technological forces, materials, practices and protocols. The cohesive articulation of the namespace requires that privacy be reframed in ways that make its diminution seem natural and inevitable. In the popular media, privacy is often depicted as the price we pay as citizens and consumers for security and convenience, respectively. This discursive ideological shift supports and underwrites the interests of state and corporate actors who leverage the ubiquitous network of digitally connected devices to engender a new regime of informational surveillance, or dataveillance. The widespread practice of dataveillance represents a strengthening of the hegemonic relations between these actors—each shares an interest in promoting an emerging surveillance society, a burgeoning security politics, and a growing information economy—that further empowers them to capture and store the personal information of citizens/consumers.

In characterizing these shifts and the resulting crisis, I also identify points of articulation vulnerable to rearticulation and suggest strategies for transforming the namespace in ways that might empower stronger protections for privacy and related civil rights.

Chapter 1. The Problematic of Privacy

1.1 Privacy in Crisis

In the 1999 episode "The Short List" of the Emmy Award-winning television show *The West Wing*, U.S. President Bartlet (Martin Sheen) and his advisors are rethinking their initial choice for a Supreme Court nominee based on their discovery that the nominee does not recognize privacy as a guarantee of the United States Constitution. Deputy Communications Director Sam Seaborn (Rob Lowe) argues the importance of nominating a different judge—one with a stronger belief in privacy rights for citizens, particularly in light of the shifting technological landscape:

> It's not just about abortion, it's about the next twenty to thirty years. The twenties and thirties it was about the role of government. The fifties and sixties it was civil rights. The next two decades are going to be privacy. I'm talking about the internet. I'm talking about cell phones. I'm talking about health records and who's gay and who's not. And moreover, in a country born on the will of being free, what could be more fundamental than this?

What *The West Wing* so presciently foregrounded is the degree to which changes to privacy law and policy, economic and cultural structures and practices wrought in and through new technologies would become a central concern, for some the central concern, in an increasingly connected, information-dense, global space of networked computer media—in short, a privacy crisis. As Google's privacy disclaimer, so unwittingly pregnant-with-meaning, recently put it: "We're changing our privacy policy. This stuff matters."

Of course, if an anxious concern over the too-easy sacrifice of privacy remains a ubiquitous and familiar theme in our modern social imaginaries[1], some concept of the importance of privacy has deep historical roots in western discourse. In various forms privacy remains one of the most architectonic and abiding concerns stretching back through western civilization. The oft-cited warning by Roman poet Juvenal, for example, *Sed quis custodiet ipsos custodes*[2], indexes a number of closely related concepts such as wealth, power, transparency, autonomy, liberty, security, and especially privacy, which still resonate with us today. In fact, it is Juvenal's warning that Brian

---

[1] This is particularly evinced in the dystopic literature of the last century. See, for example, Bellamy (1898), Zamyatin (1924), Huxley (1932), Boye (1940), Orwell (1949), Bradbury (1953), Burgess (1962), Gibson (1984), and Vinge (2006).

[2] *But who will watch the watchmen?*

Clifton, Google's former Head of Web Analytics, invokes when asked in an interview, What central question should drive the current privacy debate? "For me," he answers, "the important debate is 'who is monitoring the monitors'" (question 6, para. 1). Privacy has long proven a concept central to our thinking about the ordering of bodies and spaces, citizens and states, beginning with Aristotle's early distinction between a political public sphere and a private domestic sphere, evolving toward contemporary understandings in the late Roman period, and emerging fully as a distinct social good in what Arendt calls the "modern age."[3]

Historically, privacy represents a bedrock economic, social, and political value in the United States, through its connection to the concept of freedom of autonomy—the right to make fundamental decisions about one's religion, politics, education, and especially the disposition of one's home and family affairs. Privacy's strong connection to freedom and liberty is represented in the stories we tell ourselves about ourselves with regard to our public and private selves. "The idea of man in control of his own private sphere," observe Kennedy and Alderman (1997), "has always been a basic organizing principle of American society. At America's birth, we adopted from our English ancestors the belief that a man's home is his castle and that man is king of that domain and, by extension, the whole of his private life…[T]he rugged, solitary individual was celebrated on the American frontier, in business, and in literature and popular entertainment, and became an integral part of American mythology" (p. 152). This narrative continues today, although, as I argue in chapter two, the myth of the "rugged, solitary individual" has in fact come to oppose the strong right to privacy that it once supported.

While privacy remains central to American life today through its connection to the notion of liberty, explicit references to privacy are not found in the U.S. Constitution. With regard to privacy, the Bill of Rights includes explicit protections against government intrusion in the form of two specific rights: the right to make fundamental decisions for oneself, and the right to avoid disclosure of personal matters. Like the fictional justice from *The West Wing*, above, Chief Justice John Roberts was challenged at length about his interpretation of constitutional guarantees of privacy. During his 2007 confirmation hearing, Roberts declared that although not acknowledged per se,[4] a penumbral right to privacy is constitutionally protected under

---

[3] For more on the transformation from pre-modern to modern understandings of *private* and *public*, see Arendt's *The Human Condition* (1958).

[4] While not explicitly addressed in the U.S. Constitution, many states constitutions explicitly guarantee a right to privacy, including Alabama, Arizona, California, Florida, Louisiana, Hawaii, Illinois, Montana, South Carolina, and Washington (Lenz, 1997).

the First Amendment (securing the right to free exercise of religion, and prohibiting the government's establishment of religion), the Third Amendment (securing one's home against the quartering of troops), and the Fourth Amendment (securing a person, their house, papers, and effects against unwarranted search). Many jurists also recognize additional privacy provisions in the Fifth Amendment (securing personal information through the protection against self incrimination), the Ninth Amendment (protecting the possibility of other unenumerated rights), and the Fourteenth Amendment (protecting infringement of one's liberty without due process).

Privacy protections also derive from legislation and a significant body of tort law. Anchoring the latter is Warren and Brandeis' *Harvard Law Review* article, "The Right to Privacy" (1890), which problematized the popularity of the emerging snap-photography technology first made available by Eastman Kodak in 1884. Warren and Brandeis were the first to address, jurisprudentially, the need to protect individual privacy from an emerging 'social medium' populated by overly avid amateurs photographers. These "Kodak fiends," as they came to be known, threatened to invade the "sacred precincts of domestic life," argued Brandeis and Warren (p. 195). Citing an abbreviated version of Cooley's definition of privacy as the "right to be let alone,"[5] the article sparked a small body of case law bolstering personal privacy rights over the next decades. However, it was Prosser's 1960 article "Privacy" which revived attention to personal privacy law by gathering and delineating extant case law into four distinct torts: *intrusion* (the invasion of another's solitude); *private facts* (the publication of a private citizen's personal information not of public concern); *false light* (the portrayal, typically but not necessarily negative, of a person in a misleading way); and *appropriation* (the damaging use of another's name or likeness without their consent). Although Prosser's taxonomy encouraged, over time, a far larger body of case law supporting personal privacy, the type and extent of privacy protections continue to vary because tort-law is state-specific. Even in states that do offer similar protections with regard to particular privacy rights, these rights may be interpreted differently. For example, in 2011 the California Supreme Court ruled that police may search the contents of any arrested person's password-protected cell phone. The Ohio Supreme Court, however, has rejected the right of law enforcement officers to search the phones of arrested individuals, arguing that the use of a password grants protections analogous to those who use a physical safe—an added level of protection for which law enforcement officers must obtain an additional, specific search warrant (Gahran, 2013). Each state thus represents a unique context from within which privacy must be continually negotiated. Personal privacy rights are, in each case,

---

[5] "The right to one's person may be said to be a right of complete immunity: to be let alone" (Brandeis & Warren, 1890, p. 29).

weighed against the possibility of other stronger rights, or societal interest compelling enough to trump individual privacy rights.

Thus, while privacy is putatively recognized as a social good and, in many cases, a legal right, the specific *nature* and *value* of privacy continue to be vigorously debated and legislated. Since the publication of Warren and Brandeis' article over a century ago, their definition of privacy has become but one of many competing for primacy. For example, as Allen points out, "If privacy simply meant 'being let alone', any form of offensive or harmful conduct directed toward another person could be characterized as a violation of personal privacy. A punch in the nose would be a privacy invasion as much as a peep in the bedroom" (1988, p. 7). Attempting to navigate the muddled state of contemporary privacy research, Solove (2005) delineates some of the disparate ways in which theorists have tried to define it: as "the right to be let alone," as "limited access to the self," as "secrecy," as "control over personal information," as "personhood—the protection of one's personality, individuality, and dignity," and as "intimacy—control over, or limited access to, one's intimate relationships or aspects of life" (p. 13). Defining privacy is notoriously difficult, he explains, because privacy is both communally and contextually defined. For these and other reasons, privacy remains for some theorists "nebulous…too vague and unwieldy a concept to perform useful analytical work" (Wacks, 2010, p. xi). Ultimately, admits Solove, while a concept crucial to social organization, privacy continues to resemble a "concept in disarray" (p. 8). "It seems as though everybody is talking about 'privacy' but it is not clear exactly what they are talking about" (Solove, 2008, p. 5). It would seem not much has changed since Alan Westin's seminal *Privacy and Freedom* (1967) in which he proclaimed, "Few values so fundamental to society as privacy have been left so undefined in social theory" (p. 7).

Despite an acknowledged difficulty in reaching agreement about the nature and value of privacy, an overwhelming and growing number of voices register urgent concern over the use, by state and commercial actors, of invasive new information-based surveillance technologies and practices associated with what has been termed, variously, the *computer age*, the *digital age*, the *information age*, the *network society*, and so on. Whichever term you prefer to characterize the highly technologized contemporary socio-historical moment, privacy argues Frau-Meigs, "has emerged as one of the salient issues of the twentieth century…[and] most researchers acknowledge that [it] is eroding in cyberspace" (2010, p. 80). This claim is supported by a 2008 Pew Internet & American Life Project survey in which nearly 1,200 leading Internet activists, builders, commentators, and stakeholders were asked to predict the effect of transparency and diminished privacy on the social, political and economic changes wrought by the Internet by the year 2020. At least half the respondents agreed that privacy is either changing and/or becoming scarce, pointing

to emerging digital technologies of surveillance as a significant factor.

Though scholars are divided as to the nature and value of privacy in its various contexts, Nissenbaum (2010) points out that the danger of lingering too long in definitional stasis: "Believing that one must define or provide an account of privacy before one can systematically address critical challenges can thwart further progress" (p. 2). As my focus here is on informational privacy, I rely on Westin's definition of privacy, in which he defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967, p. 158). I have chosen Westin's definition because its focus on informational privacy allows me a careful but decisive start to mapping the privacy crisis with regard to the changing nature of informational privacy in our contemporary historical conjuncture.

1.2 The Emerging Surveillance Society

"To participate in modern society," writes David Lyon, "is to be under electronic surveillance" (1994, p. 4). Large-scale political, economic and cultural transformations have been associated with what Lyon and others have termed the "surveillance society," including: the global spread of western capitalism, the emergence of an 'information' economy, the displacement of the social-welfare state with the 'security' state, as well as a broad technological and cultural convergence in which we move from relatively unidirectional electronic and other communication and media devices to a society of multi-directional, constantly communicating, ubiquitous, networked "smart" devices. For these reasons and others, the diminution of privacy under emerging surveillance regimes represents, according to Lyon, "the single most controversial and potentially alarming social issue prompted by the massive expansion of computer power in human affairs" (1994, p. 11). These transformations both drive and are driven by a significant reorganization of the structures and functions of the first version of the World Wide Web (Web) and correspond to radical advances in computer chip size, speed, data storage capacity, and reduced manufacturing costs, leading to the global ubiquity of the networked computing device. To put it somewhat reductively, where early iterations of the Web connected hobbyists, academics, and later mainstream consumers through networks of stationary desktop digital computers, the contemporary technological and cultural configuration that underwrites our current Web—often referred to as *Web 2.0*—represents a paradigm shift toward the articulation of new protocols, policies, and practices of ubiquitous computing, and a culture of openness, transparency, sharing, and collectivity through constant connectivity. Tim O'Reilly, who coined the term, describes it in this way:

> Web 2.0 is the network as platform, spanning all connected devices;

> Web 2.0 applications are those that make the most of the intrinsic advantages of that platform: delivering software as a continually-updated service that gets better the more people use it, consuming and remixing data from multiple sources, including individual users, while providing their own data and services in a form that allows remixing by others, creating network effects through an "architecture of participation," and going beyond the page metaphor of Web 1.0 to deliver rich user experiences. (para. 1)

This explains why in an increasing number of technologically developing countries, we constitute ourselves and our communities in part through our use of personal blogs (e.g., Blogger, LivePress, Wordpress), professional blogs (e.g., Boing Boing, Gawker, Lifehacker, Mashable), micro-and videoblogs (e.g., Twitter, Tumblr, Instagram), Massively Multiplayer Online games (e.g., EverQuest, World of Warcraft), social bookmarking sites (e.g., Delicious, DIGG, Pinterest Reddit, StumbleUpon, Twitter), video sharing sites (e.g., Vimeo, YouTube), social networking (e.g., Facebook, LinkedIn, MySpace, Orkut), location tracking (Loopt, Foursquare), crowdsourcing platforms (e.g., Kickstarter, RocketHub, Wikipedia) as well as hundreds of commercial sites from Amazon to Zazzle. We text. We email. Many of us consume music, literature and other forms of entertainment in digital forms, we buy and sell in digital forms, we report very many of every movement and thought online—in a word, we share immensely more personal data than we have in the past through digital devices. The preponderance of these new media are economically incentivized to privilege and promote sophisticated forms of surreptitious surveillance, including location tracking, the recording and databanking of personal information, all of which feed the newest form of hyperconsumerism—behavioral prediction of consumers through statistical modeling. Thus, in our increasingly technologized social landscape, the emerging imperative to share everything online represents both new possibilities for community, and new pitfalls for privacy.

While increasing numbers of contemporary critics spark concern over this surveillance society in which our lives are collected and recorded in massive databanks, serious concerns over the profound effects of digital computers on informational privacy are roughly coterminous with the birth of programmable computers around the middle of the twentieth century and the emergence of networked computing which followed. In an article in *The Atlantic,* jurist Arthur Miller reviewed the proposal for a National Data Center, the first large-scale databanking of citizens' personal and public information in a centralized digital repository. Writing in 1967, two years before the existence of the first packet-switching digital network and internet-precursor ARPANET, Miller predicted a future remarkably like our own: "Computer systems will be tied together by television, satellites, and lasers, and we will move large

quantities of information over vast distances in imperceptible units of time" (p. 52). The national data center would, he warned, combine with the "numerous subsystems or satellites" owned both by state governments and perhaps private organizations to form the "heart of a government surveillance system that would lay bare our finance, our associations, or our mental and physical health to government inquisitors or even to casual observers" (pp. 53-54). Without federal regulation, databanking proposed a radical new threat, warned Miller: The collection, by "relatively unskilled and unimaginative people who lack discrimination and sensitivity," of ever greater amounts of de-contextualized but essentially indelible data collected in personal or professional digital dossiers which, through either simple data corruption or the intervention by those with malicious intent, might have catastrophic consequences to one's life (p. 54). Moreover, cultural assumptions about the infallibility of data, as well as hierarchies of control, access, and ownership could prevent citizens' awareness of inaccuracies or corruption in their own dossiers and/or prevent them from emending them.

If Miller's scenario seems all too familiar, it is because the practice of databanking and of dataveillance, has become not only possible but standard practice for both state and federal governments, innumerable corporations, and even individual citizens. Debates over the diminution of informational privacy are thus often characterized by rising concerns over the development of an emerging "dossier society," whereby personal information from myriad networked computer "databanks" can be joined to create totalizing and readily accessible personal portfolios with sometimes deleterious effects for individuals' personal and professional lives. Roger Clarke termed this powerful new form of data-driven surveillance "dataveillance" (1988, p. 500). Popular treatments of the rise of dataveillance have treated surveillance in "colorful, at times even hysterical, fashion," argued Clarke, resulting in a "visionary, yet paranoiac 'literature of alarm'" (p. 498). Dataveillance, can be defined as use of networked computers to systematically collect information and/or communication about a person, persons, their associates, associations, and activities in order to document, predict, or promote/deter particular actions or behaviors. Dataveillance thus represents the possibility of new and powerful forms of electronic surveillance in which computer systems aggregate and analyze personal data. Whereas early forms of electronic surveillance represented an extension of the methods of visual and aural surveillance (e.g., binoculars, parabolic microphones, telephone wiretaps), dataveillance opens radically new possibilities of privacy violation. Clarke takes a balanced approach to dataveillance, however, suggesting that dataveillance need not lead to the tyranny of totalitarianism, as certain types of surveillance have always been necessary to the safety and stability of the state and that through proper regulation, dataveillance ultimately represents a social good.

While it is objectively true that many surveillance practices are necessary to the functioning of families, communities, organizations and governments, some studies have shown that predictive algorithms can use ostensibly innocuous data such as 'Likes' shared on the Facebook platform to predict with great accuracy: age, ethnicity, gender, happiness, intelligence, parental separation, personality traits, political views, religious views, sexual orientation, and the use of addictive substances (Kosinski, Stillwell, & Graepel, 2013). Similarly, the work of Acquisti and Gross (2009) supports the concern that statistical modeling of interconnected data sets may allow for privacy violation on a grand scale. By using the dataset that emerges from combining information from the publicly-available Social Security Administration's Death Master File and an individual's birthplace and birthdate available from any number of publicly-available databanks and/or social networks, they were able to algorithmically predict narrow ranges of numbers corresponding to social security numbers of large numbers of citizens. "Such findings," they explain, "highlight the hidden privacy costs of widespread information dissemination and the complex interactions among multiple data sources in modern information economies" (p. 10975). The algorithmic prediction of social security numbers opens up a range of problems, including not least among them, identity theft. Predictive demography has also led to problems such as redlining, the practice whereby statistics are used to name particular groups who are then victimized by predatory commercial pricing, or the denial of goods or services such as health insurance. It's logical to infer, then, that as these systems grow in the volume and type of data capture, and as the ability of computers to process powerful predictive modeling grows, so does the potential for privacy violation, with effects ranging from personal embarrassment, to the loss of reputation and/or employment, to, in some cases, even death.

With the emerging popularity of the social networking paradigm, the popular media has become rife with moving accounts of the dangers of sharing private information on public social networks. There have been a rash of suicides among teens attributed to the Web publication of personal details. For eighteen year-old Rutgers freshman Taylor Clementi, for example, the humiliation of the Web publication of video of his intimacy with another male student[6] ended in Clementi's suicidal leap from the George Washington Bridge. The potential for serious privacy violation in digitally interconnected spaces is why, suggests Executive Director of the Electronic Privacy Information Center, Marc Rotenberg, privacy may be "the top concern" for consumers of new media products and services. Nissenbaum also sees privacy as "one of the most enduring social issues associated with digital electronic information technologies" (Nissenbaum, 2010, p. 3). The now global embrace of social

[6] The footage was taken surreptitiously through a hidden webcam and broadcast on a social media platform by Clementi's then college roommate Dharun Ravi.

networking points to a larger challenge to privacy, then, in that consumers are encouraged to share large amounts of information about themselves with global multinational corporations such as Google and Facebook for the "free" services they provide. These services come at a cost, however, requiring consumers to enter into new and complex personal, professional, and sometimes financial relations with these organizations. Many critics also recognize that Web services which offer ostensibly free services in exchange for personal data are, in fact, receiving implicit payment in the exactly the form of currency that drives the information economy—information. A few of the data surreptitiously collected from users by these databanks include one's daily schedule and/or travel itinerary, search activity, personal and professional affiliations, the content of one's communication with others, academic affiliations, native language, and any other languages one speaks, images of one and one's social circle, and one's purchases. This tracking is supported by large-scale consumer ignorance of the extent and types of tracking taking place. The blurring of private and public produced by this popularity of social networking also raises a host of questions about the legal rights of those who live online with regard to intellectual property and especially privacy. For example, while information classified by the user as 'public' has for some time been allowed as evidence in legal proceedings, more and more judges have recently begun to allow information posted on social networks and classified 'private' to be used as evidence at trial. The benefits of social networking are thus balanced by the problem confronting millions globally, argues Jeffrey Rosen—the question of "how best to live our lives in a world where the Internet records everything and forgets nothing" (2010, para. 2).

As each of Miller's predictions have been fulfilled, this growing privacy crisis has come to pervade both the popular and academic media. "We have to recognize and address the problem of web-based information disclosure before we reach a point of crisis—a point that I believe is rapidly approaching," worries Conti (2006, p. xv). "Privacy itself is in jeopardy," worries Nissenbaum, "not merely in one or another instance but under attack as a general societal value" (2010, p. 6). "The manner in which information is collected, stored, exchanged, and used has changed forever," agrees Wacks, "and with it, the character of the threats to individual privacy" (2010, p. ix). Because of the global pervasion of dataveillance, the privacy crisis has become global as well. That crisis is undergirded by a steady stream of data communicated by ubiquitous, sophisticated information and communication technologies (ICTs) such as cell phones, tablets, laptops, and other 'smart' digital devices.[7] The anxiety over

---

[7] For Lievrouw and Livingstone (2002), the term ICT denotes a relationship between particular artifacts, practices and social arrangements, which have transformed global practices in a number of ways. Specifically, the spread of networked information and communications technologies which leverage an increasingly global, relatively unified

our seemingly diminished privacy rights at the hands of governments and private corporations has only intensified after the September 11, 2001 (9-11) terrorist attacks. Many critics see the terrorist attacks of 9-11 as the impetus for the rapidly burgeoning $3-5 billion industry in surveillance technology (Horwitz, Asokan, & Tate, 2011). Moreover, in the decade following the attacks, attendance at the surveillance tradeshow nicknamed the "Wiretapper's Ball" has grown by 40 times, to host over 1,500 participants currently. The most recent tradeshow was attended by representatives from at least 35 U.S. federal agencies (Elgin, 2011).

The U.S. government's laws and policies surrounding surveilling its own citizens have been the sites of intense ideological struggle, both historically and again very recently. In fact, as I write this, U.S. President Barack Obama's administration is struggling to re-legitimize its leadership in the area of domestic and foreign security policy in the face of a mounting wave of privacy-related scandals that has energized public protests. This crisis of authority is the product of the articulation of multiple individual crises with regard to the violation of constitutional guarantees: Early and sustained critique over initial discovery of, and continuing failure to close the Guantanamo Bay Prison facilities have raised questions of due process violations by the government. These combine with critiques over the discovery of a U.S. attack drone program which raises questions about the president's power to avoid due process and perform political assassination. Lastly, the recent re-discovery[8] of widespread direct and indirect blanket surveillance of U.S. citizens' telecommunications data and metadata by the National Security Administration (NSA) has sparked a singularly strong and focused public showing of antagonism in the popular media for the Obama administration, and the government in-general.

1.3 Conjunctural Analysis and the Problematic of Privacy

This burgeoning array of privacy violations, and especially the responses to it, suggest that privacy has become what cultural studies theorists term a *problematic*. A problematic is "usually lived (but not necessarily experienced per se) as a social crisis of sorts…when [particular] instabilities and contradictions appear at almost every point in the social formation and when [those] struggles become visible and self-

---

network of computing and other analog and digital information processing technologies, has engendered fundamental shifts, both positive and negative, across the articulation of behavioral, cultural, economic, institutional, and political and technological facets of the social formation (p. 1).

[8] The same discovery was made during the Bush administration. However, likely due to the recentness of the 9-11 attacks, the story gained much less traction than it has during the Obama administration (Risen & Lichtblau, 2005).

conscious" (Grossberg, 2010, p. 41). Problematics emerge from a unique historical context and constitute a "conjuncture," which describes a social formation which has become "fractured and conflictual, along multiple axes, planes, and scales, constantly in search of temporary balances or structural stabilities through a variety of practices and processes of struggle and negotiation. It is the complex product of multiple lines of force, determination, and resistance" (Grossberg, 2010, pp. 40-41). A conjuncture is neither historically given nor entirely constructed by the critic. The critic must carefully map the historical context, attending to what he or she sees as those particular lines of force and determination that seem to best explain the emergence of a particular problematic or problematics.

We can understand the concept of conjuncture by examining Jesse Schell's *Visions of the Gamepocalypse* (2010), in which he offers a map of an emerging conjuncture he terms the "gamespace," a technologically powered form of fast capitalism in which play becomes the socially ubiquitous point of articulation connecting an information economy and networked dataveillance practices. For Schell, powerful new *technologies* (e.g., ubiquitous computing, information communication technologies, wi-fi and cellular networks, enhanced sensor and screen technologies, biometrics, geo-tracking, cloud computing, corporate and government databanking, and digital dossiers) will articulate to new *cultural forms and practices* (e.g., shifting definitions of ownership, authenticity, and privacy, the blurring of work and play distinctions, the pervasion of play into virtually all sites of cultural production and economic consumption, the embrace of social networking), as well as to new *economic forms and practices* (e.g., the pervasion of virtually all sites of cultural production by net-enabled consumer incentivization, micro-tracking, a shift to quantifiable extrinsic rewards, adver-gaming, the pervasion of human dreams by advertisers through what he calls "REM-tertainment," and ubiquitous gaming aimed at training consumers to notice advertisements). The gamespace emerges through the interconnection of these particular subjectivities, ideologies, affects, technologies, cultural and economic practices, etc., which combine to produce radically new *social designs,* resulting in, among other things, the blurring of work and leisure driven by commercial trans-media information conglomerates promoting whole-life tracking for economic profit.

However, an historical context may yield multiple conjunctures, and each conjuncture, multiple problematics. Schell's choice to name this conjuncture the "gamespace" represents his recognition of the emergence of a 'ludic' problematic, wherein the struggle to redefine the relation of work and leisure can be seen as articulated to cultural and economic imperatives. My mapping work here draws upon

a majority of the same elements of Schell's conjuncture[9] (i.e., ubicomp, digital dossiers, consumer incentivization, etc.), but is focused on the problematic of informational privacy as it is transformed through its articulation to regimes of technologically-empowered surveillance. While both conjunctures emerge from the same socio-historical context and investigate the emergence of highly technologized forms of culture and deeply cultural technologies and their significance for social structures, I connect to Schell's focus on commercial actors with an economic interest in the diminution or transformation of privacy those state actors with a parallel political interests. Although I concede that the changing work-leisure balance is a recognizable feature and perhaps even an impetus for the conjuncture I map, the pervasion of play into socio-cultural life, at least as Schell envisions it, cannot happen without a transformation of privacy driving and driven by the cultural, economic, and political embrace of radical transparency.

Changes to the social and cultural, political and economic nature and value of privacy (i.e., particularly the diminution of privacy), thus represent the requisite and perhaps single-most-powerful change constituting the conjuncture I map here. For reasons I elaborate below, and playing on the pithiness of Schell's moniker, I term this conjuncture *the namespace*. I offer the term tentatively and advisedly, as the technocultural complexity of our current moment is especially resistant to terminological boundaries. As Resmini and Rosati (2011) point out, no term adequately captures the complexity of our current social-historical context, in which the economic, political, cultural, and technological are so completely imbricated and mutually constitutive: "We can call it ubiquitous computing, the Internet of things, Web Cubed, or the Intertwingularity. We can talk about smart things, sensor Webs, product-service systems, and collaborative consumption. But none of these labels begins to describe the extraordinary diversity of the ambient, pervasive, mobile, social, real-time mashups unfolding before our very eyes…But as we wander blindly in this landscape of vernacular chaos, one thing is clear: we need a new map" (p. xi). The namespace thus represents a proposed map of the complex conjuncture which I see as the articulation of economic, juridico-political, and ideological elements, including but not limited to the following: the rise of ubiquitous computing, including the widespread availability of wi-fi and cellular technologies connecting ICTs (e.g., laptops, 'smart' phones, and tablets); powerful advances in screen and sensor technologies which both promote the social and communal uses of ICTs and enable a radically invasive new surveillance regime; juridical and political forces, laws, policies and practices driving cultural imperatives toward an open public/closed state in the

[9] It does not share, however, Schell's imaginary "REM-tertainment," as I mean to keep my conjunctural analysis grounded by extant cultural and technical practices and apparatuses and ideologies.

continuing 'war on terror', including the multi-agency sharing of databases of citizen's digital dossiers; the articulation of technical and economic forces in the shift to cloud computing, corporate and government databanking and dataveillance, and staggeringly detailed but secret personal digital dossiers; the emergence of a new Web-based advertising paradigm driven by consumer incentivized micro-tracking and the corollary forms of fast capitalism built around 'information' economies. Each of these and many other elements of the Web 2.0 world involve—require, we are told—a tradeoff between stronger forms of personal privacy and security and convenience.

1.4 The Namespace

The namespace thus describes a space of concerted effort by both corporate and state actors to reimagine privacy in weaker forms that promote a burgeoning information economy, and a rising security state, respectively, driven by practices of dataveillance. Privacy in the namespace is thus part of two interlocking binaries deployed by the state and commercial sectors, respectively: privacy vs. security, and privacy vs. convenience. The namespace, similar to what Siva Vaidhyanathan (2008) terms the "nonopticon," represents an effort to control people not through direct coercion, but through dividualizing them to the point that they can be accurately named by the behaviors their data reveals and predicts about them:

> Even the state wants us to be ourselves. It wants subversive and potentially dangerous people to reveal themselves through their habits and social connections, not slink away in the dark to avoid obvious surveillance. After all, the Stasi lost in its efforts to control the East German people, despite exacting long-lasting damage to both the observers and the observed. Our state does not want social or cultural conformity. Domination does not demand it. The state wants to ferret out and punish the ne'er-do-wells and hooligans among us and limit due process along the way.

Everyone in the namespace (i.e., everyone with a digital identity) must be named, i.e., discovered/identified, categorized, quantified, quantized, dividualized, tracked, traded or sold in the interests of national security and economic prosperity. As Luke (2006) argues, the Web can also be seen as a space of political domination for states, a "governmentality engine" in which the subaltern publics represent "subpolitical assemblies of informatics artifacts" to be manipulated (p. 526). Under such a regime, privacy remains a primary locus for the re-articulation of socio-cultural forms constructed in and through emerging forms of surveillance. That rearticulation is having both positive and negative consequences for individuals who correspond to these "information artifacts." I explore privacy in the namespace along three levels of the social formation, the ideological, juridico-political, and economic, specifically

examining popular discourse surrounding the changing nature of privacy, law and policy defining and interpreting privacy rights, and the economic practices and protocols which shape the new information economy.

Though I delineate each level of the social formation into its own chapter, each level overlaps with and influences the others in multiple directions and intensities. Technological advances, for example, may be driven by social-cultural shifts which are themselves encouraged by economic forces enabled or resisted by jurists or politicians, leading to new law and policy enforcing technological restrictions, further leading to new or transformed techno-cultural forms. Likewise, economic forces may elevate political practices which drive the development of particular technologies, resulting in a cultural groundswell encouraging an economic boycott enacted with the help of social media which results in political regime change. And so on. The important thing to remember is that relations, phenomena, agents in each social formation interrelate in what Althusser describes as *overdetermined*—that is to say, no single force, phenomenon, or agent in the social formation is totally determinant of another, but each exists in a complex relation with varying strengths, intensities and durations with regard to each of the others.[10] A conjuncture thus represents a heterogeneous "unity in difference," formed in and by "forms of coalition…rather than a battle between two completely distinguishable and separable camps" (Grossberg, 2010, p. 42). While privacy represents a point of crisis, then, I don't want to suggest here that reactions to changes in privacy are somehow unified, coherent, or singularly critical. Conjunctural analysis requires understanding a conjuncture as a space of ideological struggle. That struggle takes place, according to Gramsci, through the alignment of political 'blocs' which take their unity from the contingent and temporary alignment of actors across a range of political and other commitments. In order to map the namespace, the theorist must carefully note the multiplicity of voices and perspectives in the privacy debate which emerge from a variety of political orientations.

And in fact, it is certainly not the case that all theorists completely reject a diminution of personal privacy. Some argue that the adoption of too conservative an

---

[10] For a fuller discussion of Althusser's understanding of social determination, see his essay "Contradiction and Overdetermination" in *For Marx* (1965). I have relied on Gramsci's work in this area, which Althusser praises in a footnote to that essay: "[Gramsci] touch[es] on all the basic problems of Italian and European history: economic, social, political and cultural. There are also some completely original and in some cases genial insights into the problem, basic today, of the superstructures. Also, as always with true discoveries, there are new concepts, for example, hegemony: a remarkable example of a theoretical solution in outline to the problems of the interpenetration of the economic and the political" (1965/2005, p. 114).

understanding of personal privacy may conceal domestic forms of oppression; may contravene or compromise national security; may hinder economic flows, particularly with regard to the emerging information economy; may limit the rights of individuals, corporations or the state; may violate the norms of particular communities; or may lead to forms of historical revisionism. Some argue that a more traditional notion of privacy is incompatible with the technologies which make up a completely integrated networked society. Others argue that privacy must be sacrificed in the name of both political and economic security. For example, the "privacy crisis" has a manufactured air for writer Jonathan Franzen, with "all the finger-pointing and paranoia of a good old American scare" (2003, p. 40). *Public Parts: How Sharing in the Digital Age Improves the Way We Work and Live* (2010) represented Jarvis' paean to the new "ethic of openness" he terms "publicness." And in a *Wired* article aptly entitled "Get Over It," Jeff Jarvis likewise critiques what he calls the "political press frenzy" which he claims has been manufactured by an over-zealous media: "It's not privacy that concerns me now…I fear our supposed privacy crisis…could result in our missing many of the opportunities the net affords to connect with each other" (2011b, para 2). Potentially invasive facial recognition technologies might be used, he insists, to "find missing people…(or terrorists)" (2011b, para. 3). Abandoning equivocation altogether, Peter Cashmore, founder and CEO of Mashable.com, is famous for declaring "Privacy is dead, and social media holds the smoking gun" (2009, para. 5). And of course, Cashmore merely echoes Scott McNealy, former CEO of Sun Microsystems, whom a decade before had famously observed, "You have zero privacy anyway—get over it!" (Sprenger, 1999, para. 1). What all this suggests is that, even lacking a clear consensus on the precise definition of a legally-, culturally- and politically protean term, there is a social crisis at hand, in the form of ideological struggle, centered on the changing nature and value of privacy. While cavalier statements made by Schmidt, Cashmore, McNealy, and others suggesting that the surveillance society is a fait accompli may contribute to the public's rising concern over privacy, they also certainly point to the fact of a widespread continuing and spirited debate—in a word, a problematic.

1. 5 Radical Contextualism and Articulation

If we are to weigh arguments fairly, we require a critical methodology with a sophisticated and nuanced understanding of social determination with which we can map the ideological, political, economic and technological forces in play—particularly if we are to contribute in any meaningfully way in the political struggle to ensure a society in which privacy policies ensure the greatest social justice and the preserve the constitutionally protected rights (and those as yet unenumerated) of individuals. This dissertation contributes to that project, and to the growing literature on privacy, by understanding the struggle which constitutes that crisis in terms of cultural studies'

concept of "radical contextualism." Radical contextualism can be understood as the claim that any carefully mapped conjuncture represents a complex of specific, but never pre-determined or guaranteed "articulations," formed by lines of force and determination across the economic, ideological, and juridico-political levels of the social formation (Grossberg, 2010, p. 20). The object of study in conjunctural analysis is thus never isolable to a particular text, event, subjectivity, or discourse, but takes as its object "a structured assemblage of practices—a cultural formation, a discursive regime…located in overlapping formations of everyday life (as an organized plane of modern power) and social and institutional structures" (Grossberg, 2010, p. 25).

Cultural studies thus recognizes social formations as dynamic, radically contextual, contingent, overdetermined, non-necessary unities, and articulation names both its theory, its practice, and its object of study. Hall defines an articulation as "the form of the connection that can make a unity of two [or more] different elements, under certain conditions. It is a linkage which is not necessary, determined, absolute and essential for all time…it has no necessary, intrinsic, trans-historical belongingness. Its meaning—political and ideological—comes precisely from its position within a formation" (qtd. in Chen & Morley, 1996, p. 142). The practice of articulation thus involves laying bare the contingent and heterogeneous elements that constitute conjunctural articulations for the purpose of intervening in them, and through disarticulating and rearticulating particular, and particularly important lines of force, reconstituting the conjuncture and changing the nature of the historical context itself. The theory and practice of articulation thus offers us a sophisticated way to both map and intervene in power and its effects among and between the various levels of a social formation. Rearticulation does not represent a 'step forward' in a grand narrative of progress, but represents the disconnection and reconnection of contingent and non-necessary elements whose relation may be manipulated in the interests of certain positions of power. The goal of the critical work of the articulation theorist—the rearticulation of conjunctural relations—thus represents the hope, but never the necessary guarantee, of greater social justice. For this reason, the critic must carefully map the conjuncture for those nodes which afford dis- and rearticulation, in the hope of transformative political change.

The namespace represents a conjuncture in which we find the articulation of state and corporate actors to information economic forces and structures, to the ideological formation of individuals as citizens and consumers, to the emerging technologies of ubiquitous networked digital communication technologies. This conjuncture opens progressive possibilities for transparency, connection, community, individual expression. As it is currently articulated, however, those benefits increasingly come at the cost of individual privacy rights. By mapping the namespace as an active socio-political process in which we may hope to intervene, I attempt to recognize those

lines of force and determination open to change in order to once again rearticulate/reassert stronger privacy protections, foregrounding and prioritizing them in this nascent namespace conjuncture, while also maintaining its progressive possibilities.

An accurate understanding of the ways in which contemporary technology articulates to social, economic, and political elements is crucial to accurately mapping the namespace. Although I argue that dataveillance, as currently deployed, may represent a radically different, new and powerful form of surveillance producing and produced by new social designs, and that such practices correspond to a powerful new technologies, I am not espousing a technological determinism in which networked computers have singularly produced a radical historical break which can be addressed with uni-lateral or uni-dimensional approaches. Thinking with articulation helps us imagine how social, political, and economic relations might be differently arranged, and to resist more reductive understandings of the relation between technology and culture, such as Nicholas Negroponte's famous declaration in *Being Digital* (1995), "Like a force of nature, the digital age cannot be denied or stopped" (p. 229). I reject any approach that 'solves for privacy' merely through proper technological safeguards, or through stricter legislative oversight. My use of articulation theory to map this conjuncture instead foregrounds the need, described by Slack and Wise in their book *Culture and Technology* (2005), to understand culture and technology *together*, to support and further their demand for "a model and a vocabulary that brings technology fully into the concept of culture" (p. 5). In their primer, they use the term "technological culture" to recognize that technology is and has always been cultural, culture always technological, and that neither technology nor culture stands as the sole causal agent in any social formation—both technology *and* culture, so imbricated, are inseparable for any theorist of social formations. This perspective lies at the heart of how cultural studies understands social formations. Cultural studies' radical contextualism represents a rereading of the Marxist model of determination, accepting as it does the importance of a non-necessary and contingent correspondence between ideology, social/cultural structures, and material relations of production, including, of course, technology. It understands each of these levels as imbricated and mutually constitutive, mutually determinant. In *The Long Revolution* (1961), Raymond Williams describes it as follows. It is worth quoting at length:

> We have got into the habit…of asking about these relationships in a standard form: "what is the relation of this art to this society?" But "society," in this question, is a specious whole. If the art is part of society, there is no solid whole, outside it, to which…we concede priority. The art is there, as an activity, with the production, the trading, the politics, the raising of families. To study the relations

> adequately we must study them actively, seeing all the activities as particular and contemporary forms of human energy. It is then not a question of relating the art to the society, but of studying all the activities and their interrelations, without any concession of priority to any one of them we may choose to abstract….I would then define the theory of culture as the study of the relationships between elements in a whole way of life. The analysis of culture is the attempt to discover the nature of the organization which is the complex of these relationships. (1961/2001, p. 61-63)

There is no culture *and* art, argues Williams. There is no culture *and* technology, argue Slack and Wise. These 'individual' elements, frequently abstracted and separated either through ignorance or for the sake of convenience, must be thought in terms of articulations. In each of the three chapters which follow, then, I explore those particularly tendential lines of force at work across the ideological, political, and economic levels of the social formation, respectively.

In chapter two, I use the work of Gramsci to powerfully extend Marx's theory of ideological struggle at the level of the conjuncture. Using Gramsci's notion of *hegemony* I explore the popular media's role in helping to construct a narrative of privacy that serves the interests of the dominant political bloc. This political bloc articulates the ruling-class fractions in the form of state and corporate actors, to subordinate/subaltern class fractions made up, broadly, of citizen-consumers who are persuaded to trade privacy for security and/or convenience. I look specifically at the discursive constructions of the changing nature and value of privacy in examples from popular news, film and video game entertainments, explicating the various ways in which popular media narratives of technocultural privacy draw on a cultural fund of values, visual and textual tropes, and generally accepted understandings which Gramsci terms "common sense," in ways that attempt to make natural and inevitable the use of surveillance by corporate and state actors.

In chapter three, I take the state as the locus for an historicized examination of the ideological struggle over informational privacy at the juridico-political level. I examine the rise of the Total Information Awareness program, and examine its role in producing the nascent security state of our present conjuncture. I also explore the way in which the terrorist attacks of 9-11 produced a moment of expansive hegemony, leading to the enactment of the USA PATRIOT Act and other pieces of legislation that have systematically dismantled a significant number of those privacy protections established over the last 125 years.

In chapter four, I take the commercial sector as the locus for an examination of a

fundamental technical and economic shift toward an 'information' economy powering the consumer Web today, and the challenges it poses to personal privacy. I look specifically at the way in which the two largest social networking corporations, Facebook and Google, lead technical and cultural innovation in databanking and dataveillance, articulated to a new advertising paradigm (targeted marketing), and the embrace of the technocultural form of social connectivity, ambient findability, which underwrites and emerges from the rising information economy.

Having mapped the articulation between public (state) and private (commercial) actors, I conclude by exploring what actions might be taken to engage in the privacy crisis at first the individual level, and finally the conjunctural level. I offer short-term and long-term, individual and collective possibilities for intervening in and rearticulating the namespace in ways that take advantage of the hegemonic crisis, the crisis of moral and intellectual leadership, which is now beginning to reveal cracks and fissures. These 'dominant' state and corporate actors, desperate to regain legitimate hegemonic leadership, may be pressured, I argue, to make concessions with regard to restoring increasingly diminishing privacy rights. The namespace, I conclude, is in fact ripe for rearticulation.

Chapter 2. A New Public Narrative of Privacy

2.1 Privacy in the Popular Media

In the previous chapter I described the conjuncture I term the namespace and argued that it represents an articulation of particularly tendential lines of force in the form of particular discourses, laws and policies, economic conditions and practices, and technical codes and protocols. Each of these serves as a point of articulation between the dominant social bloc (an articulation of social fractions in the form of state and corporate actors), and the subordinate social fraction (a broad public of what I term *citizen-consumers* for which communication and other cultural and social structures are largely mediated by networked digital computer technologies). This articulation, which has emerged to dominate the namespace, at least in the U.S., is one in which the dominant social fraction overwhelmingly sets the terms of the debate on many social issues, including the diminution of certain civil rights previously enjoyed by the subordinate social fraction. This is especially true of privacy, which has been successfully reframed as a double-binary in which the diminution of privacy is necessary to maintain the balance between both security and privacy, and convenience and privacy. In this chapter, I examine the ideological nature of the struggle to maintain that articulation, and the cost it has to personal privacy as it plays out in the discursive practices of the popular media.

It is putatively understood, particularly in developed western countries, that while the mass media represent a heterogeneous symbolic field, the news media generally draws from and helps reify a broadly shared set of cultural, social, and political values and assumptions. "It is here [in the news, advertising, and entertainment media] that dominant interpretations of reality and cultural values become stamped upon, or 'anchored within' the media products sold to the public in the form of news, entertainment, and culture. Hence, by providing the basis of a shared symbolic universe, the mass media ultimately foster a common (if contested and unstable) culture as a lived system of meanings and values" (Marmura, 2010, p. 6). Cultural values, beliefs, understandings, and assumptions are never immutable, but those which are particularly tenacious often move into the realm of 'common sense' where they have particular staying power. We draw upon these ready-made truths for the stories (both fiction and non-fiction) we tell ourselves about ourselves in the popular media. For this reason, it is important to recognize the role of news and popular entertainments in the struggle to [re-]frame the nature and value of privacy in the namespace. The popular media represent a particularly important force in this conjuncture, and must be examined if we are to engage with the ways in which people think, feel, and act with regards to the privacy crisis.

Below, I examine the way in which particular elements from that common symbolic fund are mobilized in particular popular media (i.e., news, film, and digital video games), underwriting the articulation of dominant and subordinate social fractions described above, through a tendency to draw on commonsensical understandings in describing or depicting the relation of technology to privacy and social control. Examining influential exemplars of the way we portray informational privacy and privacy violation in news and entertainment media, I draw out a ubiquitous and particularly tenacious narrative which naturalizes the vision of a society in which the diminution of informational privacy is a juggernaut that may not be resisted, but only fought from within by those who have mastered it by first accepting and inhabiting it. The question of whether we might resist the adoption of particular technologies and practices constituting a particular surveillance regime is often elided entirely in this narrative. In each popular medium I describe below, privacy violation is often understood in terms of overly-reductive literary tropes and narrative commonplaces which pit individuals against a monolithic state or corporate entity; little allowance is made in this narrative for the complex nature of social determination, nor for the role of public consent in underwriting the diminution of its own privacy rights. The story of privacy crisis in this narrative is an action-adventure in which, in the process of being hailed as the hero who fights for his or her privacy and other civil rights, individuals are necessarily subjected to a disempowering regime of technological surveillance they are required to accept in order to marshal any agency, any resistance to it at all.

2.2 Ideology and Common Sense

Before moving on to the discursive analysis of news and popular entertainments, I must define what I mean by 'ideology' and how I understand its role in political struggle. Though the term enjoys wide use in both critical-theoretical and popular discourses, uses of the term in each area diverge significantly. As Raymond Williams notes in *Keywords* (1983), in popular parlance ideology continues to denote an illusory understanding of real socio-economic relations, material conditions, facts, etc. "[I]n popular argument…[s]ensible people rely on experience…or have a philosophy; silly people rely on ideology" (p. 157). While Marx's view of ideology was more complex than this, this sense of ideology as false corresponds to that typically attributed to a classical or vulgar Marxism. In the field of cultural studies, the work of Antonio Gramsci has been central to reshaping the terrain of the Marxist problematic, contributing a more nuanced understanding of political power, social determination, and ideological struggle for advanced capitalist societies. A brief review of these concepts will help clarify the uses to which I mean to put them, here.

Marx embraces ideology as a concept central to the analysis of the social formation by positing an historical materialism in which societies are structured according to material conditions rather than philosophical ideas.

> In the social production which men carry on they enter into definite relations that are indispensable and independent of their will; these relations of production correspond to a definite stage of development of their material powers of production. The sum total of these relations of production constitutes the economic structure of society—the real foundation, on which rise legal and political superstructures and to which correspond definite forms of social consciousness. The mode of production in material life determines the general character of the social, political and spiritual processes of life. It is not the consciousness of men that determines their existence, but, on the contrary, their social existence determines their consciousness…In considering such transformations the distinction should always be made between the material transformation of the economic conditions of production which can be determined with the precision of natural science, and the legal, political, religious, aesthetic or philosophic—in short ideological forms in which men become conscious of this conflict and fight it out. (1859/1904, p. 11-12)

For Marx, a society's *forces of production* (the labor power, materials, and technologies—this technology, these machines, these human bodies, etc.) determine its *relations of production* (the social relations specific to modes of production—these working hours, these gendered working spaces, this wage variance, etc.), which together form the economic *base* of a society. The economic base, for Marx, determines the *superstructure* of a social formation, i.e., the social, political, legal, religious, and metapysical spheres of a society. The superstructure in turn produces a dominant ideology which functions to reproduce the material conditions of production.

Industrial capitalism, the economic form which for Marx most alienates humanity, thus emerges from material conditions which pit the bourgeoisie (dominant, capital-owning, ruling class) against the proletariat (subordinate, labor-owning, working class). Under this system, workers' labor only increases the capitalist's wealth as it increases the division of labor, alienation, and impoverishment of the worker. Ideology thus represents for Marx, a "false consciousness" functioning propagandistically at the superstructural level, and wielded by the ruling class to conceal the exploitative nature of economic structures under capitalism, by providing simplified and compartmentalized models of society which privilege the capitalist project. Though these structures are highly exploitative, ideology works to persuade

the proletariat that capitalism represents the highest stage of civilization, the rational ordering of an industrial society through which they might progress toward entering, ultimately, the ruling class.

The work of Antonio Gramsci powerfully extends and complicates Marx's understanding of social determination, particularly with regard to the mechanism of ideology in social determination, expanding and enriching the relation between the state and civil society. Gramsci, rejects Marx's class-correspondence, seeing the state in coordinated relation to a host of other institutions in civil society. Arguing that the ruling class need not correspond to a single equivalent ideology allows Gramsci to reject universal class conflict as a necessary condition of every state, recognizing instead that particular socio-historical conjunctures may produce provisional alliances, or "blocs," through bridging particular social fractions. The ruling bloc unites a variety of dominant social actors with varying political and ideological commitments. However, to win power, this ruling bloc must articulate to subordinate or subaltern social fractions, which must be persuaded to locate their own interests within the larger set of interests established and carefully maintained by the dominant bloc. Gramsci (1934) thus framed political power as a continuum of coercive and ideological methods of control. "The supremacy of a social group manifests itself in two ways, as 'domination' and as 'intellectual and moral leadership'. A social group dominates antagonistic groups, which it tends to 'liquidate', or to subjugate perhaps even by armed force; it leads kindred and allied groups…it subsequently becomes dominant when it exercises power, but even if it holds it firmly in its grasp, it must continue to 'lead' as well" (1934/1971, p. 57-58). Though sometimes necessary to the ruling bloc, coercive power is far less productive than ideological leadership and may in fact undermine its authority to lead.

Ideologies are built, Gramsci argues, upon two "floors," or levels of abstraction in the social formation. At the philosophical level, ideologies may be coherently elaborated. However, philosophically-elaborated and -unified ideologies are only effective when they engage with and ideally transform the more established and accepted ideologies at work in popular thought, against which they must contend. Gramsci is concerned with the power of popular thought as an historical force, and understands it as central to the production of political leadership. This "chaotic aggregate of disparate conceptions," i.e., maxims, folkways, received truths, 'homespun' wisdom, etc., Gramsci calls "common sense" (1934/1971, p. 324). Common sense is thus both a resource for and a central terrain for ideological struggle. When not specifically "arbitrary, rationalistic, or 'willed'," ideologies are simply *requisite*, functioning to "'organize' human masses, and create the terrain on which men move, acquire consciousness of their position, struggle, etc." (1934/1971, p. 377). In the U.S., common sense is mobilized powerfully through popular media, though Gramsci recognizes it at work in "everything which influences or is able to influence public

opinion, directly or indirectly…libraries, schools, associations and clubs of various kinds, even architecture and the layout and names of streets" (1934/1971, p. 15).

From this complex rereading of Marx's concept of ideology, Gramsci develops his concept of "hegemony." Hegemony describes a process of ideological struggle resulting in a period of political stasis, rare in practice, in which, successfully articulating the subordinate social fraction to itself, the dominant bloc secures for itself—always temporarily and contingently—a moment of political settlement which allows it to frame itself as the natural and inevitable moral and intellectual leader in the social formation. In *Policing the Crisis: Mugging, the State and Law and Order* (Hall, Critcher, Jefferson, Clarke, & Roberts, 1979), Hall et al. offer a succinct but thorough description:

> When a ruling-class alliance [or bloc] has achieved an undisputed authority and sway over all the levels of its organization—when it masters the political struggle, protects and extends the need of capital, leads authoritatively in the civil and ideological spheres, and commands the restraining forces of the coercive apparatuses of the state in its defence—when it achieves all this on the basis of consent…we can speak of the establishment of a period of hegemony or hegemonic domination. Thus what the consensus really means is that a particular…[bloc] shapes the whole direction of social life in its image…it encloses the material, mental and social universe of the subordinated classes, for a time, within its horizon. It naturalizes itself, so that everything appears 'naturally' to favour its continued domination. But, because this domination has been secured…on the basis of a wide consensus…that domination not only seems universal (what everybody wants) and legitimate (not won by coercive force), but its basis in exploitation actually *disappears from view*. Consensus is not the opposite—it is the complementary face of domination. (p. 216)

Hegemony may never be understood as a decisive, totalizing, or final victory by the dominant bloc, but is rather a temporary and precarious preponderance of influence in the balance of forces that make up a particular historical conjuncture. The dominant bloc must agree to particular concessions and compromises to win the consent of the subordinate bloc; this, though, necessarily alters the project of the dominant bloc. This contingent and temporary alignment of interests must be maintained continually, through both discursive and material means, as the dominant bloc works ceaselessly to negate or diminish the interests of other competing groups, while depicting their own goals as commensurate with the values and needs of the subordinated bloc. Hegemony must finally be understood, then, as the briefest stasis in a process of extended struggle, derived from the successful attempt by the ruling

bloc to set the intellectual and moral shape of a particular socio-historical context, allowing it to successfully define, redefine, or resolve the nature and meaning of particular conjunctures and problematics that may emerge.

The 9-11 terrorist attacks on the U.S. produced a unique moment of hegemony, producing a conjuncture overwhelmingly defined by the problematic of national security. The security crisis is coterminous with a concerted and multi-headed "war on terror," prompting legislation and other policies and practices which aimed to bolster national security at the cost of personal privacy. Thanks in part to the devastating nature of the attacks, the state was able to easily obtain the consent of a public only too relieved to trade privacy for security. Roughly a decade later, however, citizen-consumers face a fundamentally different conjuncture in which the problematic has shifted from a crisis of security to a crisis of privacy. The security/privacy binary appears to turn on its head, as it were. The articulation of particularly influential events and conditions such as the global economic collapse, the largest U.S. debt in history produced in part by two failed wars and the perpetual "war on terror" campaign, the deleterious effects of partisan political gridlock, and the demonstrable willingness of the state to violate constitutional rights of due process (e.g., the failings of Abu Graib, and Guantanamo Bay) and other civil rights such as privacy (e.g., the discovery of blanket domestic surveillance by the NSA), among others, have led to a rapidly diminishing public faith in the government. This demonstrable failure of moral and intellectual leadership has weakened the consent of the subordinate bloc to suffer what it now understands as illegitimate invasions of its privacy and other civil rights. However, while these and other factors help to foreground the emerging privacy problematic in the popular news and entertainments, it often remains characterized by the narratives and symbols that serve the dominant power interests. The ideological underpinnings of this commonsensical narrative must be carefully mapped if we are to insist on more nuanced accounts.

2.3 Privacy in the News

My project here is not to make an exhaustive study of the news, but to draw attention to the ideological dimension of the construction of news accounts with regard to the way in which they support the hegemony of the dominant bloc. While there is no single monolithic, narrative—a growing number of powerful interests produce counter-narratives which foreground the need for a strong right to personal informational privacy—I focus here on the dominance and ubiquity of a particular narrative in the news which, while ostensibly bemoaning privacy violation, actually works to naturalize privacy's diminution. This narrative encourages the news media to describe the privacy problematic in simple, unreflexive, commonsensical terms which wittingly or unwittingly underwrite the politics of an American surveillance state.

To say the news is socially constructed to favor a dominant politics is not, however, to place it in knowing collusion or political alignment with dominant ideologies. Rather, by drawing on professional codes, tropes, metaphors, and ways of seeing (and *not* seeing) established in a cultural fund of 'common sense' on offer in public discourses, the news is structurally predisposed to reinforce dominant ways of seeing. What is produced and presented to the public as news derives from the media's process of selectively defining what is newsworthy. When selecting what is newsworthy, journalists face an imperative to make events interesting, comprehensible, and meaningful to a relatively wide public. They do so, in part, by drawing on this shared fund or repertoire of metaphors, simple narrative structures, 'truthy' facts, commonly-held beliefs and values, and other figurative language densely packed with meaning. Common sense, that body of ready-to-hand explanatory elements, represents, according to Gramsci, an accumulated, sedimented record of other more elaborated philosophies which were once more systematized and contextualized, but have become decontextualized and reified, ultimately transformed into simply 'sense', which by virtue of being reduced and decontextualized, allows for greater identification by varied audiences. However, by readily employing and accepting commonsensical characterizations, the media and public remain mired in discussions of privacy in which the terms of the debate are often informed by symbolic representations of the now-reified politics by the dominant bloc. Hall et al. describe the structural relation in this way:

> There is of course no simple consensus, even here, as to the nature, causes and extent of the crisis. But the over-all tendency is for the way the crisis has been ideologically constructed by the dominant ideologies to win consent in the media, and thus to constitute the substantive basis in 'reality' to which public opinion continually refers. In this way, by 'consenting' to the view of the crisis which has won credibility in the echelons of power, popular consciousness is also won to support…the measures of control and containment which this vision of social reality entails. (Hall et al., 1979, p. 220-221)

For example, when looking to an authority on the significance of cloud-computing technology, the popular press will naturally select an author such as Google Chairman Eric Schmidt. As a spokesman for one of the wealthiest and most successful global multi-national Web service/cloud computing businesses, he represents a putative authority on the subject, and what Hall et al. term a "primary definer" (p. 62)—those cultural spokespersons drawn upon by the media to define the outer boundaries of sense. A book such as Schmidt's *The New Digital Age: Reshaping the Future of People, Nations and Business* (2013), co-authored with Director of Google Ideas, Jared Cohen, is useful for understanding the technologically determinist arguments made by certain commercial actors—that traditional notions of privacy and anonymity are

economically stifling, militarily dangerous, and culturally quaint, among others. Julian Assange described the book as a "startlingly clear and provocative blueprint for technocratic imperialism," as essentially a manifesto defining "a new idiom for United States global power in the 21st century," and a thinly veiled marketing statement for a global communications mega-corporation to define itself as "America's geopolitical visionary" (para. 1). Not only the argument of the book itself, but in fact, the testimonials on the book jacket from politicians such as former U.K. prime minister Tony Blair, former Secretary of State Henry Kissinger, and former CIA Director Michael Hayden, immediately rhetorically align the authors' politics with those state actors known for favoring a policy of total information awareness, which I discuss in chapter three.

However, this process of reductive transformation, as more elaborate theories make their way into the public fund of common sense, is a largely unconscious process. By selecting and reproducing the ideological positions of the primary definers (those "'accredited sources'" with access to the media), "the media stand in a position of *structured subordination* [emphasis added] to the primary definers" (Hall et al., 1979, p. 59). In this way, common sense indirectly underwrites the social construction of the news media, and offers powerful, if often unintended, support to the hegemony of the ruling bloc whose influence on the media, when not direct, persists structurally. To be sure—a dominant bloc does not merely supply the subordinate bloc with a particular ideology, nor does the subordinate bloc wholly adopt the dominant ideology. Instead ruling ideologies establish the limits of the sense and structure of meaning which bound the lived relations of the subordinate bloc. "Hence, in action as well as in thought, [members of the subordinate bloc] are constantly disciplined by them" (Hall et al., 1979, p. 154).

2.4 Big Brother as Common Sense State

With regard to the privacy crisis, an important way in which the news media underwrite the power of the dominant bloc is through overwhelmingly framing the privacy debate in vague but Orwellian terms, most often through employing the trope of "Big Brother" or referencing the author whose name has become an adjective ("Orwellian") synonymous with the surveillance society. While it's true that many understandings of the relation of culture, technology, and social control compete in the popular media, "Big Brother," as the culturally recognizable symbol of the machinery of total surveillance from George Orwell's dystopic novel *Nineteen Eighty-Four* (1992), is by far the most ubiquitous narrative invoked in the popular media to frame discussions of the violation of informational privacy. "[T]he influence of 1984 has been felt far beyond the merely literary. The metaphor of 'Big Brother', now expresses a profound cultural fear in areas quite remote from what Orwell originally had in mind" writes Lyon (1994, p. 11). For example, after revelations in June that

the government has engaged in broad, warrantless surveillance of phone and email metadata for hundreds of thousands of customers of telecommunications giants Google, Facebook, AT&T, Verizon, and others, sales of the novel spiked 5,000 percent for online bookseller Amazon.com (Riley, 2013, para 4.). Moreover, in responding to the scandal, President Obama, too, framed the question in Orwellian terms: "In the abstract, you can complain about Big Brother and how this is a potential program run amok, but when you actually look at the details, then I think we've struck the right balance" ("Obama's Remarks," 2013).

In fact, the number of articles and books which in some way reference Big Brother in framing privacy (particularly with regard to technological surveillance) is so large, ranging across a wide array of discourses in the popular media, that I can offer only a brief sketch of it here. Inaugural member of the field of surveillance studies, David Lyon observes: "When I tell people that I am studying surveillance, and in particular investigating the ways that our personal details are stored in computer databases, the most common reaction is to invoke Orwell; 'This must be a study of 'Big Brother'" (1994, p. 57). Fox News' Sean Hannity moralizes, "Big Brother is monitoring your every move, whether it be online or on the telephone…This is America, and as law-abiding citizens, you have a right to privacy" (qtd. in Gibney, 2013). "The way some people see it," warns popular television personality Katie Couric, "Big Brother is watching and his name is Google." "You are being watched," writes privacy scholar Raymond Wacks, "The ubiquity of Big Brother no longer shocks" (2010, p. 1). "Of course, technology has been tracking what people do for years," writes Thomas Goetz in a recent issue of *Wired*, with "top-down, Big Brother techniques" (2011, para. 16). And as Adam Bessie worries in *Truthout*, youth in this country, so smitten with social networking, don't recognize the real threat of a Big Brother attack on their privacy, represented by the omnipresent surveillance like that in Orwell's novel: "'OMG, Winston, chill out', one of my undergrads might languidly sigh, while at the same time deftly posting the big weekend plans on Facebook under her desk" (2010, para 3).

A search for "Big Brother" filtered for "privacy" on the Amazon.com site returns more than 100 books, in which some authors, such as John McGrath in *Loving Big Brother: Surveillance Culture and Performance Space* (2004), argue for the positive effects of privacy diminution: "[S]urveillance has proliferated not least because we desire it—we enjoy it, play with it, use it for comfort" (p. vii)[1]. Others like Mark Dice, in *Big Brother: The Orwellian Nightmare Come True* (2011), worry that surveillance

[1] The title of McGrath's book actually references the television show *Big Brother*. However, the show, in which contestants agree to be confined to a house in which they are constantly surveilled by hidden cameras, obviously indexes Orwell's novel in its title and premise.

technologies and practices threaten to "make our world just as horrific or even worse than the world George Orwell described" (p. 2). A search of NPR's website returns 512 results, with titles such as, "Self-Tracking: Becoming Your Own Big Brother," "Inside Big Brother's Watchful Eye," and "Is Big Brother Listening?" A search of the *New York Times* returns over 11,000 results, with titles such as "Big Brother is Us," "Court Asks if 'Big Brother' is Spelled GPS," and "Is Big Brother Coming, or Is He Here?" A search of CNN produced over 5,500 results, with titles such as "Big Brother Awards Highlight Privacy Complaints"[2] and "Will Big Brother Track You by Cell Phone?" *Forbes* registers 114 results, with titles such as "Dear Conspiricists, Big Brother Uses Big Data," and "Big Brother 2.0: What If the NSA Adopts Facebook's 'Hacker Way'?" A search of *Wired* magazine yields over 5,000 results, with titles such as, "Big Brother is Watching You Shop," "Another Tool for Big Brother," and "Big Brother is Watching Your Travel Habits." A search of *The Atlantic* produces 702 article results; *The Economist*, 50 results; *Newsweek*, 62 results; *Mother Jones*, 24 results; *Popular Science*, 1,160 results; *Time Magazine*, 107 results; The *Wall Street Journal*, 550 results. Put simply, work on privacy in the popular media is shot through with the trope of Big Brother.

Privacy violation and Big Brother are frequently linked visually, as well. For example, the recent image on the Guardian Web site which links to an article on NSA whistleblower Edward Snowden is a black and white photo of George Orwell sitting at his typewriter. Semiotically, this familiar image of Orwell is meant to link Snowden's revelations of the NSA's snooping to Orwell's dystopic classic, lending it similar gravitas. By linking Snowden to Orwell directly, Snowden is represented by association as an heroic chronicler and harbinger of the looming surveillance society. One of the most creative visual invocations of Big Brother can be seen in the way the popular web comic *Joy of Tech* semiotically binds Facebook CEO Mark Zuckerberg to Big Brother through intertextually referencing Apple's now famous Orwellian Macintosh commercial from the 1984 Olympics, directed by Ridley Scott (Nitrozac & Snaggy, 2009). Apple's original commercial depicts a futuristic scene of ideological indoctrination, as the massive face of Big Brother booms out from a telescreen: "We are one people, with one will, one resolve, one cause," to an audience of grey-pallored drones who stare silently as one in their uniform grey jumpsuits. Suddenly a brightly dressed woman runs on screen to hurl a hammer into the telescreen. Its destruction awakens the audience from their ideological slumber as the commercial's announcer intones: "On January 24th, Apple Computer will introduce Macintosh. And you'll see

---

[2] In fact, one of awards offered for those who most egregiously violate privacy by the international privacy watchdog Privacy International (mentioned in the previous chapter) is the "Orwell," a golden statue of a boot stamping on a human head—the very image the character of O'Brien uses to characterize the future of human civilization for Winston, in the end of the novel (Orwell, 1949/1992, p. 280).

why 1984 won't be like *Nineteen Eighty-Four*." In the *Joy of Tech* comic, however, it is CEO Mark Zuckerberg's face which looms large on the screen as, to similarly disaffected drones, he extols: "Greetings citizens of Facebookia. This is our land, a land of people and of privacy! That's why we have new privacy guidelines! From now on, by default, all your information is available to everyone on the internet. To remain private, share everything with everyone!" The rhetorical figure (παραδοξοσ) so brilliantly used in *Nineteen Eighty-Four ,* "WAR IS PEACE"; "IGNORANCE IS STRENGTH"; "FREEDOM IS SLAVERY," is displayed across Zuckerberg's face as: "PRIVACY IS SOCIABLENESS," "SECRECY IS SHARING," "PERSONAL IS PUBLIC."

It has become, then, "pretty clear what everyone mean[s] by the phrase 'Big Brother'," explains McGrath (2004), "they [mean] invasion of privacy," particularly at the hands of a panoply of powerful new surveillance technologies and practices (p. vii). Moreover, Big Brother and the various other Orwellian tropes have become *so* ubiquitous in popular media treatments that some critics have taken to praising their absence. The sheer number of references to Big Brother in the popular media reify its authority as a framework for understanding privacy with regard to social control such that even critics who reject an Orwellian frame are required to acknowledge it or reject it outright. For example, in reviewing Landau's *Surveillance or Security? The Risks Posed by New Wiretapping Technologies* (2011), Rothke is moved to praise Landau for *not* invoking Orwell: "*Surveillance or Security?* is one of the most pragmatic books on the topic in that the author never once uses the term Big Brother. Far too many books on privacy and surveillance are filled with hysteria and hyperbole and the threat of an Orwellian society." In an editorial by Mashable CEO Pete Cashmore, Orwell's novel is described as "incredibly prescient yet woefully incorrect," and our present historical moment as both "reminiscent of Orwell's vision and radically at odds with it" (Cashmore, 2012, para. 1). In his *New York Times Magazine* article "Little Brother is Watching," Kirn rejects references to Orwell out of hand, calling *Nineteen Eighty-Four* "a quaint scenario, grossly simplistic and deeply melodramatic" (2010, para. 2). While describing *Nineteen Eighty-Four* as "grossly simplistic" and "deeply melodramatic" seems to me a grossly simplistic reading of a novel generally recognized as a classic work of dystopic literature, it raises an apt question: Just why do critics in the popular media cling so to the glower of a Big Brother who, having failed to manifest in our own present moment, has little critical purchase in contemporary privacy debates?

The answer to this question is complex and multi-faceted. First, the novel's standing as a literary classic results from a rhetorical pathos which brilliantly addresses the historical conjuncture from within which it emerges and to which it responds. Lane describes the overwhelming cultural appeal of Big Brother as "a creation so plausible and so frightening that he instantly took his place alongside other literary metaphors

for human ingenuity run amok" (2011, p. 141). Orwell's novel speaks to an historically established anxious concern over the transfer of our dearest rights and freedoms to governments which, through powerful technologies of surveillance and control, strip citizens of fundamental human rights. Many see a direct causal connection between the emergence of the technologies and practices of pervasive social surveillance and the rise of totalitarianism—Orwell's novel dramatizes brilliant support for this argument. Set in what would be for Orwell a dystopic future, *Nineteen Eighty-Four* imagines the struggle of everyman Winston Smith against a rigidly totalitarian form of English Socialism[3] (Ingsoc), a regime under which citizens have lost or abandoned their rights to free expression, personal property, and especially privacy. Published at the conclusion of the Second World War, the novel held remarkable explanatory power for a public attempting to understand the rise of German Fascism and its ability, through propaganda and other means of control, to garner widespread support for its radical political program. Orwell addresses the importance of ideology in the political process, noting that as Ingsoc emerged, citizens offered little enough resistance to the loss of their social freedoms. "[T]he choice for mankind lay between freedom and happiness," explains Winston, "and…for the great bulk of mankind, happiness was better" (1949/1992, p. 275). This important aspect, the *consent* of the general public to have allowed the emergence of such a repressive regime, is often missed by the news media as Orwell's novel is fit to the procrustean bed of 'common sense', where Big Brother, simplified to represent not an articulation of ideological and material forces, but the monolithic state or corporations, takes on a singular anthropomorphic malevolence. For a public hungry to understand how something as horrific as the Holocaust could have happened, the vastly more complex novel offers a striking explication of an articulation of the means of social control by what were then newly emerging surveillance and computing technologies. Orwell's densely woven narrative described the extensive coordination across the various levels of a social formation necessary to produce such an unremitting form of totalitarianism. A brief review of that articulation reveals the complexity of Orwell's understanding of social determination.

Ingsoc was organized as the articulation of structures of political organization across the social formation. These were represented by four ministries. The Ministry of Plenty (Miniplenty) represented the economic arm. While ostensibly it ensured the distribution of goods and services, it ran the state-sanctioned market in a state of balanced, planned inefficiency. This bolstered the belief among citizens that they were sacrificing for the war effort. It also encouraged an illicit free market, which the government not only ostensibly tolerated, but employed to surveil those who patronized it.

---

[3] According to the book by Immanuel Goldstein, Ingsoc is technically organized as a form of oligarchic collectivism (Orwell, 1949/1992, p. 214).

The Ministry of Love (Minilove) represented the juridico-political arm. It fulfilled the first of the two primary goals of the State, the ability to surveil and predict the thoughts of every citizen. The State had abolished all laws but one, "the essential crime that contained all others in itself. Thoughtcrime they called it" (Orwell, 1949/1992, p. 21) and it consisted simply in having thoughts against the party. While the machineries of surveillance included standard police patrols, far more terrifying were the ubiquitous telescreens which both surveilled citizens and broadcast propaganda unceasingly. Citizens were terrorized by the constant monitoring which might reveal one's thoughtcrime, interpellated by the watchful symbolic gaze of Big Brother not only from the telescreens but from the media which surrounded them, "on coins, on stamps, on the covers of books, on banners, on posters, and on the wrapping of a cigarette packet—everywhere. Always the eyes watching you and the voice enveloping you. Asleep or awake, working or eating, indoors or out of doors, in the bath or in bed—no escape. Nothing was your own except the few cubic centimetres inside your skull" (Orwell, 1949/1992, p. 29).

The Ministry of Peace (Minipax) represented the military arm. Minipax fulfilled the second of the two primary goals of the State, to ensure perpetual global war between itself and the states of Eastasia, and Eurasia. Perpetual war was supported by a military industrial complex which had purposefully abandoned technological advance in favor of a tri-state balance of military strength. Perpetual war thus allowed the State to ideologically unite the people as one against an imaginary enemy traitor, in the form of racialized other Immanuel Goldstein, "the commander of a vast shadowy army, an underground network of conspirators dedicated to the overthrow of the state" (Orwell, 1949/1992, p. 15).

Perhaps the most important was the Ministry of Truth (Minitrue), which represented the state-controlled media arm. It was charged with encouraging political orthodoxy through the ideological interpellation of citizens by all means of discourse, communication, and signification. Minitrue had many functions, including producing political propaganda, and editing or "rectifying" historical documents by changing facts, figures, and the truth of historical events. "All history was a palimpsest, scraped clean and reinscribed exactly as often as necessary" (Orwell, 1949/1992, p. 42). The primary goal of Minitrue was its project to revise the English language, creating an ideologically pure version called "Newspeak," which would eliminate political unorthodoxy through the removal of words and concepts that were revolutionary, eventually obviating the need for machineries of surveillance themselves. All media, all acts of communication and signification were bound to the war effort, supported by the Ministry of Truth in the creation of everything from patriotic youth organizations, to posters depicting threatening racially-stereotyped enemy soldiers, to endless effigies, lectures, meetings, military parades and processions, novels, rumors,

slogans, songs, speeches, telescreen programs and films, and waxwork displays. The "Two-minutes Hate," for example, provided an outlet for direct and focused aggression which had taken the place of social and cultural connections which might organize individuals in collectives no longer possible. They had replaced privacy, love, friendship with mechanistic and superficial emotions such as fear, hatred and pain (Orwell, 1949/1992, p. 32). The propaganda machine represented a cultural force in the breakdown of institutions which might offer citizens anything but the state. Children were alienated from their parents through early enlistment in the "Spies" where they learned the techniques of spying on adults. Young adults were also constrained by membership in similarly focused state-sponsored organizations as the "Youth League" and the "Junior Anti-sex League." While prostitution was tacitly encouraged by the party as "an outlet for instincts which could not be altogether suppressed" (Orwell, 1949/1992, p. 68), romantic sex and the creation of families for other than procreation had been discouraged. This breakdown of the family, and romantic relations functioned to isolate individuals from each other and to articulate them solely and constantly to the State. This party view of sex was "rubbed into every Party member from childhood onwards" (Orwell, 1949/1992, p. 69). Elimination of affect through removal of familial bonds was in part replaced by the state-sponsored opiate "Victory Gin."

Orwell's detailed, horrific description of a model of total social control that perfectly integrates the economic, juridico-political, military, and especially ideological levels, may explain why it is Orwell's Big Brother who has emerged as our ubiquitous cultural shorthand for privacy violation, and not the "Well-Doer" from the less well-known but important dystopian precursor to *Nineteen Eighty-Four*, Zamiatin's *We* (1924). Like Orwell's novel, *We* understands political domination as the integration of economic, cultural, political, and technological forces, and in fact, the plot and setting of *We* are strikingly similar to those of *Nineteen Eighty-Four:* In the novel's "United State," citizens abandon personal and familial identities for state-issued numbers; they consume propagandist music and art; they relinquish nearly all private property and privacy; and they find themselves surveilled and hailed by a singular ideological figurehead. *We* describes very similar discursive and symbolic practices to *Nineteen Eighty-Four* for inscribing political orthodoxy, including similar techniques of surveillance and social control. "Normally," exclaims Zamiatin's narrator placidly, "we lie surrounded by transparent walls which seem to be knitted of sparkling air; we live beneath the eyes of everyone, always bathed in light. We have nothing to conceal from one another; besides, this mode of living makes the difficult and exalted task of the Guardians much easier" (Zamiatin, 1924/1983, p. 18). However, whereas *We* emphasizes a warped love story doomed by the dystopia which contextualizes it, *Nineteen Eighty-Four* represents a political meditation in which the love story provides only the impetus for the protagonist to begin his exploration. Likewise, whereas the Well-Doer of *We* offered an analog for Italian fascist Mussolini, the

figure of Big Brother offered an easily identifiable analog for the demagogues such as Stalin and Hitler whose atrocities were historically unparalleled. In short, Orwell's novel could be described as a work of literary political philosophy that tackles the difficult question of social determination—of how such a dystopia might come into being and be organized. To theorize such an architecture of control he invokes Bentham's model of social control, the Panopticon, of which I have more to say below. Orwell's novel thus helped describe for the public at the middle of the twentieth century the brave new world wherein vast computer databanks were not merely a dystopic prognostication, but the harbinger of an emerging reality. Published a quarter century before Orwell's novel, Zamiatin's descriptions of the technological means of total surveillance and total social control must have read like fanciful predictions. If Zamiatin's novel seemed prescient in *anticipating* technological and cultural changes, Orwell's novel *reflected* the terrifying probability of changes introduced by the co-terminous introduction of the first programmable computer.[4]

The novel has continued relevance for us in the first decade of the twenty-first century, as well, anticipating technological and cultural changes in our own time that have made possible many of the troubling synergies Orwell could only then imagine. Lane notes that with the rise of digital networked computing in the late twentieth century, Big Brother and the concept of the Orwellian state becomes "a veritable mantra" for civil libertarians and those interested in challenging the emerging practices of databanking and dataveillance (Lane, 2011, p. 220). For contemporary critics, at least three techno-cultural developments in the Orwellian social formation are held up as disturbingly predictive of changes we are witnessing in our own time. First, the state of perpetual war that was used to justify the violation of basic human rights in Orwell's dystopia are offered in similar support for the denial of basic civil rights during our own extended conflicts, e.g., the "cold war," the "war on drugs," and the "war on terror." Second, the development of the telescreen is frequently compared to the development of computers and especially ICTs, which are already used to track our location, and to mine and record what we often think of as personal data. Third, the Orwellian concept of "thoughtcrime" could only emerge in tandem with the use of predictive algorithms, such as those now employed by both the government and consumer entities. Many critics rightly discern the way in which the first line of force legitimizes and strengthens the second and third.

While the literary quality and technological prescience of the novel are acknowledged, there are fundamental reasons to challenge its value as a useful model of social control in understanding the contemporary privacy crisis. To imagine a direct analogy between Orwell's model of social determination and our own is problematic in several

---

[4] *Nineteen Eighty-Four* was published in 1949, two years after the initial military service date of the Electronic Numerical Integrator And Computer (ENIAC).

fundamental ways. First, Orwell's novel represents a fictional account of a society ordered according to the principles of a social design proposed by English philosopher Jeremy Bentham, termed the "panopticon." The panopticon was introduced by Bentham in 1791 as an architectural design for prisons, hospitals, and schools. It was designed as a circular building with inward-facing cells ringing the circumference, illuminated so as to be seen by a central watchtower. From within the central watchtower, shielded from the sight of those on the periphery, overseers surveil the inhabitants, each separated into his or her individual cell. This total, continual, and visible but unverifiable surveillance of individual inmates by an unknown, seeing but unseen principal was designed to eliminate the myriad negative effects produced by traditional dungeons, which locked the masses away together in dark spaces. It produces instead a machinery of light and vision in which omnipresent surveillance inculcates in the inmate the terror of an omnipotent overseer who might intervene punitively at any moment. The separation of individual from individual was designed to eliminate contagion in patients, collusion in prisoners, chatter and cheating in students, and productivity-limiting distraction in workers (Bentham, 1791/2011, p. 29).

Whether experimenting with punishments for prisoners, new efficiencies for workers, or new pedagogies for students, Bentham's panopticon thus offered the overseer a laboratory for the study, creation, alteration, and elimination of human behavior. Nor were the overseers themselves immune to the imperious gaze of this "machinery of furtive power….[this] concerted distribution of bodies, surfaces, lights, gazes," as their conduct and worth might too be read at any time in the condition and progress of their charges (Foucault, 1975/1995, pp. 202-204). The panopticon thus serves as a laboratory for power, observes Foucault, a "cruel, ingenious cage…a mechanism of power reduced to its ideal form" (1975/1995, p. 205). The efficacy of that power lay in its ability to use architectural structures and geometrical principles to induce, through an omnipresent psychological terror, self-control in its subjects: "[I]ts strength is that it never intervenes, [power] is exercised spontaneously and without noise…Because without any physical instrument other than architecture and geometry, it acts directly on individuals; it gives 'power of mind over mind'" (1975/1995, p. 206).

The social world described in the novel evinces each of the central mechanisms of the panopticon: *constant but unverifiable surveillance*, the *ideological interpellation of citizens* by powerfully repressive political orthodoxies, the *isolation of the individual* and erosion of familial and other traditional communal forms: "With the development of television, and the technical advance which made it possible to receive and transmit simultaneously on the same instrument, private life came to an end. Every citizen…could be kept for *twenty-four hours a day under the eyes of the police* and *in the sound of official propaganda*, with *all other channels of communication closed*. [emphasis

added] The possibility of enforcing not only complete obedience to the will of the State, but complete uniformity of opinion on all subjects, now existed for the first time" (Orwell, 1949/1992, p. 169-170). As many critics have noted, government surveillance in the U.S. is no direct analog for Orwell's Ingsoc. Certainly, limited panoptic practices are at work in certain banks, retail stores, and other situations/locations in which the conspicuousness of closed-circuit television (CCTV) surveillance are used to deter as much as discover criminal behavior. In any case, while the U.K. has adopted CCTV surveillance to drive law enforcement, with estimates ranging from 1.85 to 4.1 million cameras deployed publicly, the system has failed to produce radical reductions in crime. Moreover, even with the ostensible adoption of a large-scale panoptic regime of surveillance, the U.K. today little resembles Orwell's "Ingsoc," in which a terrified citizenry was ceaselessly interpellated by the ubiquitous presence of Big Brother: "On coins, on stamps, on the covers of books, on banners, on posters, and on the wrapping of a cigarette pack—everywhere. Always the eyes watching you and the voice enveloping you. Asleep or awake, working or eating, indoors or out of doors, in the bath or the bed—no escape. Nothing was your own except the few cubic centimeters inside your skull" (Orwell, 1949/1992, p. 26).

In reviewing Rule's *Privacy in Peril* (2007) and Solove's *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (2007), Vaidhyanathan praises both scholars for "avoid[ing] describing mass surveillance as a 'Panopticon'. That too is refreshing, as that standard model and theory of surveillance has exhausted its utility" (2008, p. 7). While forced to acknowledge his field's unsuccessful attempt to move beyond the panoptic model entirely, Lyon posits its usefulness as complementary at best. The model is fundamentally flawed[5], he argues, and may provide only "a diversion, a distraction from much more important issues that we miss at our peril through an obsessive fixation with the prison diagram" (Lyon, 2006, p. 9). The prison diagram offers a model which understands only coercion, and cannot account for willing participation, active agency and desire of individual subjects, complicit (wittingly or unwittingly) in their own disenfranchisement. Here the concept of hegemony can help us usefully complicate such reductive models. Ultimately, then, the panoptic model offers a too-simplistic, too-reductive understanding of both agency, ideological interpellation, and social determination. This was a primary reason the panoptic model met early and sustained resistance in the field of surveillance studies. Moreover, it was Foucault himself, in *Discipline and Punish* (1995), who argued that modern social control was in already in transition, across the social formation, from panoptic and other "disciplinary" regimes of surveillance and control to a new and

[5] See Lyon's introduction to *Theorizing Surveillance: The Panopticon and Beyond* (2006) for a brief overview of the emergence of critical resistance to the panoptic model in the field of surveillance studies.

radically decentered forms coterminous with the rise of emerging information technologies.

Another problem represented by thinking the privacy crisis through the panoptic lens is that in using an Orwellian frame to describe contemporary technocultural arrangements we may find ourselves aligned with mechanistic models of social control. Mechanistic models elevate technology as the primary or sole determinant social force, placing technology at the center of social change. This implies that to understand technology, we need to begin with the technological object itself, which either will have inevitable, linear, and unvarying effects to which we have no real ability to respond (a relation of simple causality), or a varying though finite range of possible effects to which we may only react after the fact (a relation of symptomatic causality). Neither approach offers the possibility of intervention, especially on or before the emergence of the technologies themselves. Non-mechanistic models, on the other hand, foreground the context surrounding the object, and reject the notion of technology as either simple agent or effect. Slack (1984) delineates two primary non-mechanistic models, both of which recognize the co-constitutive nature of technology and culture: "expressive causality" and "articulation and assemblage." However, while expressive causality recognizes the effects of the whole of a structure on the elements which constitute it, it posits the latter phenomena as the expression of the intrinsic essence of the former. In this framework, society "evolves" according to an essential and controlling single logic, with the cultural and social manifestations reflective of that essence. This allows journalists to draw overly simplistic conclusions about the relation between ideology, and cultural, technological, political, and economic forces, and thus to imagine and report reduced possibilities for political resistance. For Rule (2007), for example, the erosion of privacy is the simple expression of the nature of such technological systems: "[T]he capacities of computing systems to absorb, analyze, transmit and use personal data are bound gradually to find their ultimate expression, until no personal data is safe from incorporation" and the only defense against this technological juggernaut, according to Rule, is a system of laws and policies which might constrain it, "laws and policies that 'just say no' to endless extensions of institutional surveillance" (p. xv). But this type of thinking assumes too linear a model. Instead, by understanding culture and technology in our present historical conjuncture as related through processes of articulation—and especially disarticulation and rearticulation—we are able to address the question of how the relation of culture and technology might be otherwise.

Ultimately, in framing privacy violation as the story of resistance to the various apparatuses of a Big Brother (whether corporation or state), one is decidedly not telling the story of agency as a property of systems. One is telling the story of heroic individuals, and not of negotiation and prolonged hegemonic struggle in which individuals are persuaded to consent to trade personal privacy for convenience and

security. The Panoptic/Orwellian model of social control, and the commonsensical allusion to Big Brother which has come to be a shorthand for it, encourages only a linear determinist vision of power as coercion, rather than a vision of power as the property of articulations which come together in the seductive dreams of citizen-consumers. "The era when factories and troops were the decisive order-sustaining institution is (at least in our part of the world) over," writes Bauman (1998), "but so is, as well, panoptical power as the main vehicle of social integration, and normative regulation as the major strategy of order-maintenance. The great majority of people—men as well as women—are today integrated through seduction rather than policing, advertising rather than indoctrinating, need-creation rather than normative regulation" (p. 4). Put more simply, the surveillance society which emerges will not be, as is usually predicted, an Orwellian totalitarianism, but more Huxleyan, argues Schell (2010), "more like *Brave New World*, where technology controls us because it is so pleasurable."

The panoptic frame also supports the dominant bloc in offering a convenient straw man. The claims of Orwellian domination can be waved away persuasively by state and corporate actors—after all, most Americans do not fear being disappeared by a faceless Big Brother. Commonsensical analogies which attempt to understand our contemporary privacy crisis through the Orwellian lens are thus both understandable as a strategic response, and problematic in the extreme. While Orwell's description fails in its inability to offer a theory of ideology that accounts for agency and resistance, this is precisely the rhetorical power of the novel for critics—the widely acknowledged rhetorical power of Orwell's horrific tale which offers critics a trope/shorthand, already dense with cultural meaning, for explaining the dangers of unchecked surveillance. Orwell's dystopic society is so tightly integrated, so perfectly engineered, its technologies of surveillance and ideological domination so pervasive, that there exists no possibility for individual agency or resistance. From the first moments of the novel, Winston himself admits as much. "You might dodge successfully for a while, even for years, but sooner or later they were bound to get you" (Orwell, 1949/1992, p. 21). As readers of the novel we witness the utter destruction of his human identity, and are interpellated to experience the powerlessness of a subjection under panoptic surveillance.

Unfortunately, the real power in our contemporary surveillance regime comes not from a dominant coercive, visible but unverifiable panoptic surveillance, but surreptitious surveillance which tirelessly and secretly measures the digital footprint of a majority of citizens. This action-adventure narrative in which individuals are compared to Orwell's everyman protagonist serves the government in transforming a complex articulation of forces and architectures into a monolithic "Big Brother" who cannot easily be practically 'grasped' for political action, but who can conveniently be discursively waved away, and in fact, often repackaged as a form of individual agency.

Big Brother, through its invocation of the panoptic model, thus represents a distraction, agrees Boyne (2000), which severely mitigates critics ability to think with articulation about the troubling, emerging surveillance regimes: "The idea of a disciplinary, Panoptical society came to constitute the default background of much social and cultural analysis through the 1980s and into the 1990s. Analyses of the historical development and current functioning of private organizations, whose reception was reinforced by a cultural imaginary feeding off conspiracy theoretic journalism and a wave of paranoia entertainments emerging from the film industry, came to focus on the operation and significance of surveillance and control mechanisms, while on the other hand, discussions of social policy and the welfare state have, for the most part, taken the necessity of surveillance and information so much for granted that it is hardly even discussed" (p. 293). "The tendency," agrees Frau-Meigs, "to see privacy as protection from intrusive government, with much less emphasis on intrusive commercial third parties, goes together with the ingrained belief that the individual, construed as a code user, is empowered to resist in the face of enormous superstructures like corporations and institutions…The shift from secrecy towards personal control and autonomy is presented as a means of asserting one's identity and individualism" (2010, p. 94). The dominant bloc has a vested interest in encouraging the narrative of the rational individual everyman, for two reasons: It opposes the real complexity of the social structures which constitute dataveillance practices of the state; it helps sell products by interpellating users as active agents, empowered by the technologies on offer to them by commercial vendors.

The ubiquity of Big Brother in the popular media thus represents a perfect example of how an elaborate or nuanced account, theory, or philosophy—i.e., the fully developed work of literary political philosophy, flawed though it may be, represented by *Nineteen Eighty-Four*—enters, in reduced form our cultural fund of common sense as an explanatory trope. Orwell's brilliantly complex rendering of interlocking political forces, though problematic in its reliance on the panoptic model, is simply reduced metonymically to "Big Brother," as it moves into common sense, mobilizing a technologically determinist, economistic, or classically Marxist, narrative of individual agency, and centralized social control, in which a lone everyman somehow becomes conscious of the illusory ideological domination of the all-powerful state and resists it individually. As Gramsci's work suggests, political control in advanced western societies is most effective when it relies on building consensus. The Orwellian fable, then, as a fable in which all political agency is entirely circumscribed within the state, and of course is foreclosed *a priori*, tends to express an ideological position in which political action is at best Sisyphean. After all, "You can't fight city hall," common sense reassures us.

2.5 Privacy in Film

Above, I describe a general process regarding the news media's role in drawing from and depositing to a general fund of common sense. That cultural fund is constituted as well in and across the various discourses and genres of the popular media. Filmic discourse contributes to it in a somewhat different but equally important way. Technologically-themed fiction films often function by engendering what, in *Becoming Biosubjects* (Gerlach, Hamilton, Sullivan, & Walton, 2011) Gerlach et al. term a "social science fiction" (p. 4). These discursive frames from fiction and popular culture come to oppose current scientific and social realities of technology by offering us "frames and narratives within which we locate unfamiliar, underdeveloped, or as yet unknown[6]…technologies. The future possibilities of these technologies are folded seamlessly into their present description. In this way, the technology is mystified and ultimately reified, making it less amenable to critical analysis" (Gerlach et al., 2011, p. 4). Especially in popular entertainments (e.g. blockbusters, star-vehicles, award-winning films), this may significantly strengthen the power of the dominant ideologies which underwrite commonsensical, received views of technology, helping define for the general public the past, current, and potential future role of technology in society, and in the process mitigate possibilities for the re-articulation of particular conjunctures. "For scientists, social science fictions empower and protect their claims, their expertise, and their social function…for the public, social science fictions translate otherwise inaccessible knowledge into a set of social ramifications that can be recognized and negotiated" (Gerlach et al., 2011, p. 21). The practice of articulation represents the opposite impulse: "It aims to give people an understanding of the contingency of the present. If the present context did not have to be this way, if it was not guaranteed in advance, then it could have been otherwise, and it can be something different in the future" (Grossberg, 2010, p. 57). The enactment of reification with social science fictions obviates and/or obscures such possibilities, arguing that "The choice is not, then, whether we should have or use this technology, but rather, how to deal with its effects, as the social science fictional framing has rendered it already present" (Gerlach et al., 2011, p. 4). With regard to surveillance and privacy, argue Gerlach, et al., social science fictions exist in complementary relation to the political and legal work of implementing surveillance technologies and changing laws surrounding personal privacy, helping "ease the entry of this new surveillance technology into society" (Gerlach et al., 2011, p. 29). If we are able to think technology, culture, politics, and the economy together, we are empowered to see more clearly the relation between ideological and material practices.

---

[6] Their exact phrase is "unknown genetic technologies" (p. 4). I have omitted the word "genetic," which is indicative only of their particular technological focus, and doesn't alter the truth of their observation about technological narratives in general.

As an example of this fictional framing work, I want to examine a pair of films which, read in tandem, demonstrate the mobilization of the social science fiction I describe above, i.e., the lone everyman fights the monolithic state or corporation that invades his privacy and abrogates his rights through surveillance: Francis Ford Coppola's *The Conversation* (1974) and Tony Scott's *Enemy of the State* (1998). *The Conversation*, stars Gene Hackman as Harry Caul, a surveillance expert who stumbles onto a conspiracy to murder a corporate executive known as "The Director" (Robert Duvall). An acknowledged expert in his field Caul has devolved into an anti-social paranoiac because of professional guilt. His surname, 'Caul', denoting the protective membrane surrounding a fetus and symbolized by a translucent rain slicker he wears everywhere, represents his need to protect his privacy through insulation and isolation. While performing a surveillance operation for The Director (his ostensible client) he learns of a possible murder plot against his surveillance targets which forces him to struggle with his complicity in facilitating similar past murders. Although he initially withholds the surveillance tapes from The Director, they are eventually stolen by the director's assistant. However, Caul ultimately learns that his work was used purposefully to bait The Director and ultimately facilitate his murder by the surveillance targets he thought he was protecting. At the end of the film, Caul receives a threatening call from the murderers, who warn: "We know that you know, Mr. Caul. For your own sake, don't get involved any further. We'll be listening to you." The erasure of any and all safe space for Caul is foreshadowed earlier in the film when he guiltily admits that for his surveillance targets, "There's no protection. I follow them wherever they go. And I can hear them." Caul proceeds to tear up his apartment searching for surveillance devices. Ultimately unable to find one, he resigns himself to a chair amidst the ruin of his apartment and does the only thing left to him—play his saxophone, the only 'noise' left to mask his perpetually surveilled signal. It is the iconic image of a lost man—a surveillance expert who is no longer protected by his technical skills from a world making radical advances in surveillance with which he cannot keep pace.

Nominated for three Academy Awards, and the winner of the 1974 Cannes Film Festival's Palme d'Or, *The Conversation* represented a timely comment on the Watergate scandal, just two years prior, in which the Nixon administration was found to have broken into the Democratic National Headquarters in the Watergate complex in order to photograph documents and install audio surveillance devices. The film's success is arguably due, at least in part, to its ability to make public sense of events that led inexorably to the first presidential resignation in history. Drawing on the contextual irony of the contribution of Nixon's own surreptitious audio recordings to that resignation, it depicted surveillance in ultimately simple terms, as an unwieldy tool opening society to egregious abuses of power.

Nearly a quarter century later, *Enemy of the State* can be read as an response to the predictions made in *The Conversation* about the impending surveillance society. The film tells the story of everyman Robert "Bobby" Clayton Dean (Will Smith), a prominent Washington D.C. labor lawyer. When Dean inadvertently intercepts a zip disk containing footage of the secret assassination of U.S. Congressman Phillip Hammersley (Jason Robards), he finds himself the target of a rogue operation run by NSA Director-hopeful Thomas Reynolds (Jon Voight) who is determined to recover the evidence. It is in fact Reynolds himself who has sanctioned the assassination of Hammersley when he refuses to help pass the pending Telecommunications Security and Privacy Act. Terror mounts as Reynolds secretly employs the powerful means of the National Security Agency (NSA), apparently at his ready command to surveil, torture, and murder, in order to obtain the incriminating disk. While Dean's former lover is murdered by NSA operatives, the director's most powerful weapon is shown to be the data-matching algorithms which not only allow him to access Dean's various digital records, but to alter them. "Let's get into his life," rages Reynolds. "I want to know about his wife; I want to know about his parents; I want to know about his gambling problem; his urine samples; his porno rentals; I want to use every means possible to get what we need." Dean is soon on the run as a murder suspect, without money or other resources. There he encounters former NSA operative Edward Lyle (Gene Hackman), who very reluctantly agrees to help him fight the system by turning the NSA's surveillance tactics against itself.

Although *Enemy of the State* is not a direct sequel to *The Conversation*, it functions in a similar capacity, intertextually invoking a continuity between what are in fact two separate Hackman characters in two separate films.[7] This intertextuality can be seen in the similar way Scott references Coppola's characters. Like Caul from *Conversation*, Lyle from *Enemy* is a paranoid, anti-social surveillance expert paying an emotional debt of guilt; both Caul and Lyle work in nearly identical hidden warehouse labs; both films employ nearly identical scenes, including the signature scene from *The Conversation*, in which multiple agents work together to surveil a couple in a public plaza; when the NSA pulls Lyle's digital dossier, the photo shown is of Hackman's Caul from *Conversation*. In this way, both films work intertextually

[7] In a chapter from *Race Men* (1998), Hazel Carby outlines the way in which the many roles of actor Danny Glover, understood in aggregate, constitute the signifying practices of a racist politics in mainstream Hollywood film. "In [Glover's] person Hollywood, in addition to producing the black male as an outcast who threatens to undermine the very foundations of America, adopts the black man as a sympathetic cypher, a means for white men to find meaning within themselves and discover the true meaning of their existence" (p. 190). Although not the place for it here, a similar study might be made of the ideological functions performed by the equally iconic Hackman across his various film roles.

to produce a powerful and diachronic map that makes claims about the changing technical infrastructure effecting new possibilities for surveillance, and the contemporary meaning of privacy.

What is most fascinating about *Enemy of the State* is that when read as a single film, Lyle assumes the role of guide to Dean. When the films are read together, however, it becomes apparent that, when Hackman's characters are read in contiguity, they describe the evoulution of an orientation to technology—one which supports the fundamental contemporary changes and challenges to privacy. We watch as Caul/Lyle (linked semiotically through common characterization of Gene Hackman) learns to accept, re-inhabit, and master an emerging surveillance state. Caul's journey leads him, in the first film, to attempt and fail at isolation/insulation as a strategy for privacy protection. In the second film, forced by Dean to use his surveillance skills to take on the NSA, he is forced to realize that the 'surveillance society' is a juggernaut that cannot be the stopped, and that the only real protection one has is to master the techniques and work within the system.

Unlike Coppola's film, *Enemy of the State* is not a visually subtle film. Made a quarter century later, it assaults the audience with footage of the myriad surveillance technologies on offer today[8] (e.g., networked satellites, GPS tracking devices, digital dossiers, etc.) through Scott's trademark frenetic camera style. In the opening credits alone, we are bombarded with a series of jump-cuts to images of surveillance by short-circuit television, keyhole satellites, foot, car and helicopter pursuit, all of which depict the state's electronically enhanced pursuit and apprehension of citizens. Surveillance technology, it tells us in these images of 'criminals' pursued and decisively apprehended, is an unstoppable force which cannot be evaded. Drawing on a particular commonsensical received understanding of technology, the film thus dramatizes the argument that the surveillance society has arrived. The dramatic foot and car chases, gun-play, and explosions in the film proper only underscore what each character affirms for us in dialogue. For example, just before his assassination, Hammersley warns Reynolds: "[The Telecommunications Security and Privacy Act] is not the first step to the surveillance society; it *is* the surveillance society!" To which Reynolds replies "Liberal hysteria!...This is the richest, most powerful nation on earth, and therefore the most hated. And you and I know what the average citizen does not: that we are at war twenty-four hours of every day. Do I have to itemize the number of American lives we've saved in the past twelve months alone with judicious use of surveillance intelligence?" The 'liberal' position is offered here only as a straw man—easily dismissed by Reynolds' assassination of Hammersley which follows only moments later and, thanks to inadvertent surveillance, is captured on tape. Later in

[8] Though the movie was made a decade and a half ago, many of the surveillance techniques it depicts are still of current concern today.

the film, Reynolds explains: "Privacy's been dead for 30 years because we can't risk it." Mimicking Orwell's Winston Smith,[9] though with opposite intent, he concludes: "The only privacy that's left is the inside of your head and maybe that's enough." If the viewer doubts the villain's word that the surveillance society is upon us, it is nevertheless affirmed by other characters in the film we are interpellated to trust. It is Lyle, for example, who affirms "[the government's] been in bed with the entire telecommunications industry since the 40s. The old days we had to tap a wire to your phone line. Now a call is bouncing off a satellite, they just snatch 'em right out of the air." And in another scene, Dean's wife affirms for the viewer: "I told you Bobby! I told you they had the capability!"

As the film ends the televised words of a U.S. senator revise Juvenal's words to offer up what might be understood as a primary argument of the film: "We knew that we had to monitor our enemies. We also have come to realize that we need to monitor the people who are monitoring them." The senator's words suggest an infinite regression of continually more powerful technological means for surveillance. At this point, the film effects the full thrust of its argument to accept the presence of the surveillance state as necessary political protection: Lyle suddenly hijacks Dean's TV with a camera feed of Dean sitting on his own couch. Dean is troubled for the briefest moment as he realizes he's still being surveilled. The image of him is then immediately replaced by a fond message from Lyle scrawled on the sand of a tropical beach he's escaped to: "Wish you were here." Dean smiles then because he knows that Lyle is 'watching out' for him—he is safe thanks to the (continuing, constant and vigilant) heroic actions of a technical superman protecting him through the very surveillance technologies that had so vexed him before. Dean and Caul, the alternating-complementary protagonists with whom the viewer is called to identify through the movie's powerful rhetoric, have learned to work the system they cannot escape. The ideological effect is chilling, in some sense mirroring the final words of *Nineteen Eighty-Four*: "But it was all right, everything was all right, the struggle was finished. He had won the victory over himself. He loved Big Brother" (Orwell, 1949/1992, p. 245). The ultimate question becomes not whether surveillance is necessary—that question has been answered for us in the strongest rhetorical pathos—but how to regulate and live within it.

2.5 Privacy in Video Games

Lastly, I want to turn to an example of the way this action-adventure narrative of privacy and surveillance has been successfully deployed in contemporary digital- or

---

[9] "Asleep or awake, working or eating, indoors or out of doors, in the bath or in the bed—no escape. *Nothing was your own except the few cubic centimeters inside your skull* [emphasis added]" (Orwell, 1949/1992, p. 26).

electronic video games. Since the release of the first commercial video game console in 1966, video games have risen to become a major component of the entertainment industry, with *Forbes* estimating that the global video game industry may reach $82 billion this year (Gaudiosi, 2012). Not only are they a bulwark of the entertainment economy, they are culturally pervasive, engendering devoted fan communities, film adaptions, national conventions, and other forms of cultural engagement. According to the Entertainment Software Association (ESA), 58% of Americans play video games. The average gamer, who has been playing for well over a decade, is thirty years old ("Industry facts"). Demonstrably, filmic narrative has become a well-established criterion of value for players, designers, and critics of top-selling video games.[10] If the claim holds regarding a film's ability to ideologically interpellate a viewer, it must hold all the stronger for a modality in which the interpellated subject is hailed to more fully inhabit the subject position of the narrative by interactively shaping it. Many video games whose plots revolve around science-fiction scenarios in which a significant element of the plot involves computer technology have a hacking mechanic in which players complete challenges designed to represent breaking into everything from locked chests to digital networked computer architectures. A majority of games involve this mechanic, requiring players to routinely violate privacy in order to complete game objectives. This mechanic represents the enactment of a social science fiction in which surveillance is ideologically reframed as a tool enhancing the subject's agency. "Surveillance is more than a tool in the maintenance of social order; it is also a fantasy of power…In other words, surveillance is increasingly a social science fiction, another form of imaginary, in which, at the push of a button, anything can be made visible and knowable…From this perspective, people are not under surveillance, but rather coded information about them is collected. As a result, the struggle between control and resistance becomes less important than a logic of virtualization" (Gerlach et al., 2011, p. 31).

Lastly, then, I will examine the video game *Watch Dogs* (2013), in which players are encouraged to see individuals as "coded information" which can "at the push of a button"—both the virtual button of the mobile device carried by the character in-game, and the button on the real-life game controller held by the player—"be made visible and knowable" by hacking into their cloud-based digital dossiers. In an interview with IGN, one of the lead developers of *Watch Dogs*, Jonathan Morin, describes the transformation of subject to digital-virtual object in this way: "A lot of

---

[10] While there has been some debate among those who theorize interactive electronic entertainments as to whether the ludic or narrative dimensions of video games are of greater cultural and critical import, it has generally come to be recognized, especially with the launch of the latest next generation consoles, that narrative (and specifically filmic) qualities are an integral part of the ludic dimension of games—that is, they are best theorized together.

games will go and invite the player to just explore the environment. Us, we're kind of letting you explore human beings as well…Aiden Pierce looks at [an individual] around him in a different way…you can tap into [a person's] life…[to] find new side-quests."

Watch Dogs is a highly cinematic, open-world, third-person action-adventure game set in a virtually-rendered Chicago of the near-future. Well in advance of its release, the game has won multiple awards, taking "Biggest Surprise," "Most Anticipated" and "Game of the Show" awards at the industry-leading 2012 Electronic Entertainment Expo. The game also won "Best PC Game," "Best New Franchise," and "Biggest Surprise" by popular gaming organization IGN. The success of the game is based in part on its ability to tell the currently dominant story of surveillance in the namespace. Beyond the game's "obviously polished play mechanics" and "optimized graphics…[which] had us sitting slack jawed," the game's power was in its ability to address the problematic of privacy, according to a review in *Gaming Excellence*: "[I]t came down to a storyline that is bathed in real world possibility and the terrifying implications of a society that is so interconnected digitally, and the damage and possibilities of one man gaining control of the entire system" (Game of the Show, para. 1). The game tells the story of Aiden Pearce—his name puns on the words *aiding* and *pierce*, bespeaking his ability to penetrate the city's surveillance to help those in need—a surveillance-obsessed vigilante and technical superman (analogous to Hackman's Lyle character, above) who can hack a city-wide network called the "Central Operating System." In order to detect and punish criminals, Pearce must hack into the lives of most of the characters who inhabit this world by using a hand-held mobile device to biometrically scan them in order to learn intimate personal details about their health, finances, relationships, employment, etc. Aiden can also use his mobile device to hack the city's entire data and communication interface, tapping into individuals' cell phones, and CCTV network—in fact he can effectively control any electronic device in the landscape (cranes, roadblocks, elevated trains, etc.). Moreover, his hacking device leverages Big Data (combining massive datasets and sophisticated predictive algorithms) to predict whether other non-player characters are *likely* to commit a crime.

According to Morin, the game represents a response to perhaps multiple problematics of the namespace, but certainly privacy and control, albeit one that unwittingly underwrites the politics of the dominant bloc.

> One thing that's interesting is that people understand what we're talking about…A lot of people have been asking us where *Watchdogs* comes from? What's the concept? Well, it's typically beer-discussions about Facebook and information and what's happening in the world, right? A human being is always reacting to technology in different

> ways. Like today it's a new way of people to express themselves publicly. Some people don't like that. Like it gets harder to govern a given society when people have access to information that much. So we're talking about those things and instead of talking about being a victim of that, we started to ask ourselves wouldn't it be cool to be that guy? The guy who can tap into the network of information and to reverse engineer that conversation.

What's striking, yet predictable, is the game's answer to that question. Based on the assumption that political agency resides in individuals, political resistance is equated with vigilantism. It's a solution that maps perfectly to the affordances of the virtual video game world, at least as it is being imagined in the most popular and best-selling games. These games draw the same narrative of hero/anti-hero, bravely fighting an antagonistic, typically monolithic, omniscient, omnipotent system alone: "I wasn't always this guy," growls Pearce in the game trailer, "In this city, no one can hide from me. No one. They crossed a line. And for that, I will make them pay. I'll turn their city against them. They think I'm a man out of control. But I've never had so much control." Rather than depict a narrative in which characters work to radically re-articulate the economic, cultural, political, and technological forces at work in their fictional world, *Watch Dogs* depicts a world in which one cannot imagine, nor demand, the type of society in which unfair surveillance practices are outlawed. Aiden Pearce's hope for political resistance lies in becoming an outlaw, assuming in the process the dominant politics which created such a disempowering regime in the first place. "The tendency to see privacy as protection from intrusive government, with much less emphasis on intrusive commercial third parties, goes together with the ingrained belief that the individual, construed as a code user, is empowered to resist in the face of enormous superstructures like corporations and institutions…The shift from secrecy toward personal control and autonomy is presented as a means of asserting one's identity and individualism" (Frau-Meigs, 2010,p. 94). In this way, *Watchdogs* represents a social science fiction based on the same narrative in the two films above, and in the Orwellian novel which informs much news media coverage of the privacy crisis—a narrative which through limiting the complexity of our thinking about the privacy crisis, limits our ability to address it in a meaningful political way.

In this chapter, I have argued that the signifying practices of popular media demand to be interrogated as a primary locus of ideological struggle in the namespace, particularly with regard to one particularly tenacious model describing the relation between surveillance, privacy, and social control. I align with Vaidhyanathan in demanding "better terms, models, metaphors, and strategies to control our personal information" (2008, p. 3) suggesting that privacy research involve not only legal scholarship, but social science and media scholarship, as well. Such work demands a way that is both theoretically rigorous, but that mitigates or avoids altogether the

typical impenetrability, for lay people, of the esoteric vocabulary and other alienating discursive conventions of academic theory. The commonality in each of these media with regard to privacy and surveillance is a definition of power and agency as a thing to be won, rather than a property of systems, arising through articulations. Power is held by the all-powerful state or corporations, and resisted only by maverick individuals who work within its architectures, protocols, and ideologies, etc. In the next two chapters I examine more closely the commercial and state actors who both benefit from and drive the narratives, such as those described above.

Chapter 3. Privacy and Security in the Surveillance State

3.1 Societies of Control

In the previous chapter I discussed one of the ways in which popular media ideologically underwrites the hegemony of a dominant political bloc of powerful state and corporate actors which benefits from an increasing transparency that allows each to access the personal information of citizens and consumers. I examined the preponderance of a particular model of social control based on Bentham's panopticon which is used to frame a majority of privacy debates in popular media. The overwhelming ubiquity of this narrative represents a tendency to portray the present privacy crisis in commonsensical, individual-oriented terms, and tends to foreground the state and the corporations as monolithic Big Brother entities. This narrative obscures the complex social, political, and economic forces at work in the diminution of privacy and other civil rights. Narratives of a more convenient and pleasurable world in which social transparency ensures security and convenience have come to dominate more nuanced narratives in which strong informational privacy is more than a quaint, antiquated value.

One of the most important ways we can challenge this vision, and the hegemony of the security state it underwrites, is to replace this reductive model of social control with a more nuanced model that can account for the articulation of both private and public actors. For Vaidhyanathan (2008), in addition to the fact that observable surveillance has not demonstrably shown to discipline the behavior of individuals in a non-totalitarian state, the central problem with panoptic thinking is that it cannot account for the modes of control offered by the emergence of surveillance regimes powered by Web 2.0 and cloud computing, in which those surveilled often have limited or no awareness of the extent of state, and especially commercial, surveillance. This serves the interests of the dominant bloc, commercial and state actors who want citizen-consumers to increasingly share more and more personal information in order to better name and map them through the data generated by the choices manifest in their digital footprint. Commercial actors use that data to sell them more products. Governments use that data to discover those who would subvert and resist state control (p. 10).

Vaidhyanathan's description of a mode of control driven by transparency and mobility invokes one of the most pervasive and important challenges to panoptic thinking—Gilles Deleuze's 1992 essay "Postscript on Societies of Control." The essay focuses on the problematic represented in the rise of cybernetic regimes in which, through ever more powerful technological, economic, socio-cultural, and political means, governments and corporations construct elaborate systems of information management through which to surveil citizen-consumers in ways that facilitate a

dispersed new system of social control. "We don't have to stray into science fiction to find a control mechanism that can fix the position of any element at any given moment.…The key thing is that we're at the beginning of something new….the widespread progressive introduction of a new system of domination" (Deleuze 1997, pp. 181-2). Deleuze works forward from Foucault's genealogical work on power and social control in *Discipline and Punish*: *The Birth of the Prison* (1975), in which Foucault describes the modern shift from sovereign societies to the disciplinary societies of the eighteenth and nineteenth centuries. In disciplinary societies, Foucault argues, individuals moved relatively contiguously and linearly from one social site to the next—the family, school, factory, military, hospital, and perhaps prison. These disciplinary sites worked to create and control individuals through ideological enclosure. In each site the individual was named and categorized, disciplined by a set of knowledges and expectations, molded by broadly standardized ideological and behavioral models, and punished when he or she violated site norms. The disciplinary society relied on ubiquitous and manifest surveillance to interpellate individuals to conform to these ideological molds.

According to Deleuze, although Foucault never names the form of social control to supplant disciplinary societies, disciplinary forms represent for him fading forms which the emerging technological assemblages of our age indicate we are already moving beyond. Deleuze suggests that with the rise of digital communication networks and cybernetic structures of control of the mid-twentieth century we are moving toward a new paradigm of social control he terms the "control society." Unlike disciplinary societies, control societies represent a radical blurring of the sites of ideological subject formation into a kind of dynamic, ubiquitous, mobile singularity. The control society relies on wide, now global, networks of digital computers to collect, store, and analyze massive datasets. The coercive drive under disciplinary societies to force individuals to conform to a particular mold is replaced by the ability of the pattern-recognition algorithm to create highly flexible systems of control through real-time analysis and modulation: "We're moving toward control societies that no longer operate by confining people but through continuous control and instant communication" (1997, p. 174). Individuals in the control society become dividualized into data-points which can be monitored in real-time, producing the cybernetic loop with influences or constrains human behavior algorithmically and without human intervention.

In Deleuzian terms, then, the namespace represents a regime of social control through the pervasion of a surveillance system powerful enough to discover and/or assign a unique 'name' for each element in its network. "We no longer find ourselves dealing with the mass/individual pair. Individuals have become 'dividual's', and masses, samples, data, markets, or 'banks'" (1992, p. 5). Its ability to map and control publics is no longer based primarily on enclosure and physical surveillance, but on the

new form of surreptitious surveillance—*dataveillance*. As the global Web pervades ever more completely the daily lives of individuals, policies, practices, and protocols emerge which leverage the unique data points of each unique actor in ways that may also constrain and discipline its behavior. As Zadie Smith reminds us, interfaces validate and invalidate certain responses, disciplining members culturally about the most important and popular concerns, feelings, and discursive means for sharing them. She describes the control implicit in interfaces in "Generation Why," her meditation on the Facebook phenomenon: "What is your relationship status? (Choose one. There can be only one answer. People need to know.) Do you have a 'life'? (Prove it. Post pictures.) Do you like the right sort of things? (Make a list. Things to like will include: movies, music, books and television, but not architecture, ideas, or plants.)" (2010, page 2, para. 8). Deleuze's control society are constituted in and by such interfaces.

Thus, although the transparency and instant social connectivity powered by 'Big Data' may often provide certain forms of security and convenience, it also enables a powerful new mode of social control. Big Data describes the collection, storage, and analytical processing of data sets so massive and complex that special software, storage facilities, processing power, and technical infrastructures must be developed to handle them. In 2012, the White House announced a Big Data Research and Development Initiative comprising a $200 million budget across six federal departments and agencies. According to the White House, the initiative will help "accelerate the pace of discovery in science and engineering, strengthen our national security, and transform teaching and learning" (Kalil, 2012, para. 1). Big Data-driven dataveillance also drives the commercial sector's promotion of a culture of ambient findability, in which consumers are encouraged to share their personal information nearly everywhere and at all times. This shift is manifest in the success of myriad cybernetic consumer products such as the Nike FuelBand, the Jawbone UP, and the FitBit. These products capture, store, analyze and provide feedback on a host of biological data such as daily movement patterns, sleep patterns, and caloric intake. Customer data is stored on commercial servers where consumers can visualize their own activity graphically. With access to consumer data, however, these companies can continually refine their own sales and marketing for these and other products. The central rule and requirement of those institutions, practices, patterns, protocols, etc., which articulate to shape the namespace is the algorithmic assignation and/or discovery of identities in real-time. This is underwritten in part by the trend toward the elimination of an anonymous Web, as many Web services providers have instituted the requirement that all users use their real name on their networks. Commercial Web services providers often do so, in part, in order to map each actor's real identity to an extensive collection of data points, which allows them to match those users with a host of products and services offered by their partners. While government privacy protections have been diminishing with the rise of the security state—citizens are still

protected from many types of government surveillance—there remain very few laws or policies which offer more than nugatory protections against commercial actors. For this very reason, commercial dataveillance practices continue to be leveraged by the state to enhance its own surveillance capabilities. I examine these commercial actors in the next chapter. In this chapter I focus my examination at the juridico-political level of the social formation, addressing the state's struggle for political hegemony as it learns to wield this new mode of control.

Before continuing, I must clarify precisely what I mean by "state actors." At a broad level of abstraction, the U.S. government may be understood as unified by a shared interest in its own continuity, security, and prosperity. According to the *Routledge Encylopedia of International Political Economy* (2001), a state generally "mobilizes populations in defence of its realm; regulates, monitors, and polices conduct within civil society; intervenes (more or less intensively) within the economy, and regulates (and, in some instances, controls) the flow of information within the public sphere" (Hay, p. 1469). In practice, however, the three branches which make up the U.S. government articulate to each other in a complex system, as the popular refrain goes, of checks and balances. Within each of these levels, and articulated to them, exists a relatively heterogeneous assemblage of state actors, including various juridical, political, and military offices, institutions, and other organizations who often compete for budgetary and other resources. In practice, then, these various actors may often have conflicting priorities and agendas. The state actors I refer to herein is constituted in part by a specific articulation of powerful government interests, particularly drawn from within the Executive Branch and the U.S. Intelligence Agencies, who are dedicated to a policy of total information awareness in support of a surveillance regime that undergirds a nascent and likely growing security state.[1] The president's role as Commander-in-chief represents a powerful point of articulation joining the Executive Branch to the military and various intelligence agencies, unifying these state actors with regard to law and policy on foreign and domestic security. While this political fraction may be variously opposed by actors in the judiciary, legislature, and even by other actors in the Executive, military and intelligence communities, nevertheless, it is those state actors across the three branches who support the rise of the security state that I refer to, somewhat reductively, as "state actors," or the "state" in this dissertation. In the sense that I employ it here, then, the state can be

[1] To the question of whether the U.S. might ramp down its aggressive stance on security in light of massive U.S. budget shortfalls and the essential defeat of Al Quaeda forces, Secretary of Homeland Security Janet Napolitano is reported as answering, simply, "no," calling the 9-11 attacks "the signal of a change in the environment that we have to deal with, I think, throughout the foreseeable future" (Lake, 2011, para. 4).

understood as a particularly powerful line of force in the articulation of the namespace.

This dominant bloc of state actors approached political hegemony most closely in the years immediately following the 9-11 terrorist attack by asserting moral and intellectual leadership over a subaltern social fraction constituted by citizen-consumers and other actors who were persuaded to consent to the diminution of various civil rights, including privacy, in exchange for an immediate guarantee of security. As the 9-11 attacks represented a strong kairotic moment for cementing public fears of terrorism, the historical conjuncture centering around the attacks thus produced a temporary settlement of forces in which consent was easily obtained by a terrified public. The USA PATRIOT Act[2] was passed with few reservations in a moment of expanding hegemony, mitigating, and often overriding, nearly half a century of privacy protections. The Act was passed a month after the 9-11 attacks by a margin of 357-66 in the House and 68-1 in the senate. Speaking at the Center for American Progress Action Fund, Senator Ron Wyden (D-OR), one of only ten senators to vote against the reauthorization of the PATRIOT Act in 2006, describes the effects of the Act as "the creation of an always expanding, omnipresent surveillance state that now chips away needlessly at the liberties and freedoms our founding fathers established for all of us" (Wyden, 2013, para. 11). As the work of Wyden and other outspoken privacy partisans indicate, changing domestic and international contexts over the last decade have transformed the Act's cultural and political meaning for a broad majority of the public (the subordinate social fraction). Those individuals and organizations who are increasingly alarmed over the state's surveillance overreach are increasingly vocal in resisting it. Because the PATRIOT Act continues to stand as a major node in the namespace conjuncture, rearticulating the namespace requires understanding not only the Act itself, but the conjunctural forces through which it emerged.

3.2 The Snowden Revelations

By the middle of 2013, the privacy problematic had developed to high intensity after revelations by whistleblower Edward Snowden emerged demonstrating that the government had been spying on American citizens for a number of years. Working for Booz Allen Hamilton as an infrastructure analyst for the NSA, Snowden had access to a large number of classified NSA materials, many of which he revealed to *Guardian* reporter Glenn Greenwald. Greenwald thereafter published several groundbreaking articles exposing the extent and type of surveillance being conducted

---

[2] The USA PATRIOT Act is an acronym that stands for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001."

on American citizens through the government's 'partnership' with private corporations, as well as their efforts to undermine internet encryption standards. Greenwald's first article detailed the workings of the NSA's PRISM program through which the state 'legally' obtained both metadata[3] and content from email, chat, VOIP telephony, and various files (text files, photographs, etc.) from as many as nine telecommunications providers which service the majority of communication needs for the world, including Google, Facebook, Microsoft, Apple, Yahoo, Verizon, T-Mobile, and AOL (Greenwald & MacAskill, 2013). In an interview with Glen Greenwald and documentarian Laura Poitras, Snowden explains the scope of the NSA's ability to collect nearly everything a user may do on the internet. According to Snowden, the NSA does not, practically, limit itself to the surveillance of foreign individuals, but collects all communications that cross U.S. networks. This represents a large majority of the world's internet traffic. Through access to a variety of surveillance systems, such as Boundless Informant ("a global auditing system for the NSA's intercept and collections system") and PRISM (a system providing the NSA "direct access to the back-ends of all the systems you use to communication and store data"), claims Snowden, nearly "any analyst at any time can target anyone, any selector, anywhere" (Greenwald, MacAskill, & Poitras, 2013). Snowden's disclosure of the state's ability to read the content of assumed-private communications contradicts accounts by government officials, including President Obama, who affirmed that the data surveilled was metadata only, and Director of National Intelligence James Clapper, who, during his testimony to the U.S. Select Committee on Intelligence in March, 2013, replied in the negative when asked by Senator Wyden: "Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?"[4] On June 6, after the Snowden leaks, Clapper released a statement admitting that his statement before Congress had been "erroneous" (Ungar, 2013). In addition to its PRISM program, however, further documents published in the *Washington Post* at the end of October reveal that through software codenamed MUSCULAR, the NSA and British GCHQ in fact continue to copy millions of records directly from fiber optic cables transmitting data between Yahoo and Google and their respective data centers. As authors Gellman and Soltani note, FISC judge John Bates ruled illegal under FISA and in violation of the Fourth Amendment a

---

[3] Metadata is essentially data which describes data. Telephony metadata could include call pairs (the phone numbers of caller and receiver), caller location, date and time, duration of call, data amount, cost, etc. Internet metadata could include the computer type, applications installed, browser used, IP address, and any information stored in cookies. Such metadata constitutes a digital dossier for each individual, and under current laws, can often be repurposed, given, sold, or traded to third parties without consumers' consent or awareness.

[4] Clapper's exact response was: "No sir. Not wittingly. There are cases where they could inadvertently perhaps collect, but not wittingly" (Ungar, 2013, para. 2).

similar but smaller surveillance operation which copied records from cables also located in the U.S. (Gellman & Soltani, 2013).

Even more troubling than revelations that the U.S. has been hacking the servers of commercial actors were revelations that the NSA has been working with commercial actors to build security vulnerabilities into commercial software products themselves (Moyer, 2013). Soon after the PRISM revelations, in a joint article by *The Guardian, The New York Times,* and *ProPublica*, it was reported that the U.S. intelligence community has been pursuing a long term strategy to undermine stable encryption (one of the few technologies ensuring the private and secure storage and transmission of data on the internet). Through its membership in the National Institute of Standards and Technology (NIST), the NSA was able to wrangle its way to being the de facto author for the encryption standard—inserting its own 'back door' vulnerabilities in the process. The standard it de facto authored has been engaged by the International Organization for Standardization (ISO), an umbrella organization comprised of 114 standards organizations. It was stated matter-of-factly in the NSA presentation that "For the past decade, NSA has led an aggressive, multi-pronged effort to break widely used internet encryption technologies," and that cryptanalytic abilities of the intelligence community are now strong enough to penetrate encryption standards formerly thought to be impenetrable. The NSA presentation further revealed that, based on the 2013 budget request, under the heading "Sigint enabling," the encryption-breaking program budget dwarfed the PRISM program, estimated at $20 million, by ten times, averaging approximately $250 million each year.[5] This funded a variety of operations including an effort to break into 4G mobile devices and the investigation of possibilities for hacking the servers of Yahoo, Facebook, Microsoft, and Google (Naughton, 2013). As noted above, the threat of the NSA hacking Google and Yahoo is no longer a *potential* threat. It was also revealed that while the NSA's Commercial Solutions Center offered companies a resource for testing the security of their products, they leveraged their working relation with these clients to discover ways to insert vulnerabilities into their products. Through this close collaboration with private partners and other intelligence agencies, such as Britain's Government Communications Headquarters (GCHQ), the NSA has thus taken a number of steps to weaken digital privacy, including compromising and modifying codebases in ways that, according to acknowledged security expert Bruce Schneier, may render encryption altogether meaningless (Talbot, 2013). "I think the most significant revelation," observed Greenwald in his honorific speech for Edward Snowden during the 2013 Whistleblower Awards, "is that the objective of the United States and its closest allies in the U.K., Canada, New Zealand, and Australia is the elimination of privacy globally, the idea that there will be no ability on the part of any

[5] It's noteworthy that the U.S. intelligence budget has grown from $30 billion before the 9-11 attacks, to $80 billion, less than a decade later (Naughton, 2013).

human beings to communicate with one another electronically without it being monitored, collected, analyzed, and stored by the United States Government."

Hours after the release of Snowden's documents in *The Guardian*, President Obama held a press conference in which he acknowledged public privacy concerns and outlined four proposals to reform the NSA's surveillance activities, promising to work with Congress to reform section 215 of the PATRIOT Act in order to develop greater transparency, oversight, and constraints on the use of government authority. Declaring "we can and must be more transparent," the president promised to: launch a website to promote transparency; direct the intelligence community to find ways to remain as transparent as practicable; direct the Justice Department to publicize the legal rationale for section 215 of the PATRIOT Act; ensure that the NSA is "taking steps" to increase oversight through the appointment a Civil Liberties and Privacy Officer. This and other public outreach attempts by the Executive ostensibly demonstrate at least some concern with recovering political legitimacy in the eyes of a scandalized public ("President Obama Holds").

The state's response was far more intransigent and cavalier when in 2005 a surveillance program analogous to the PRISM program was first revealed to the public by retired AT&T employee Mark Klein. Klein reported that his former employer had allowed the NSA to install a network traffic shunt on west coast communication hubs, including San Diego, San Jose, Los Angeles and Seattle,[6] which could assist in secretly capturing communications for millions of Americans. This surveillance began as early as 2001, according to undisputed documentation provided in *Hepting v. AT&T* (2006). According to Klein, this breach involved the construction of a special NSA-secured room in which the agency installed a Narus STA 6400 network traffic analyzer[7] that allowed the NSA to split the network traffic stream, diverting millions of records to its own servers without judicial oversight or approval ("NSA Spying"). In early 2006, seven anonymous executives from the communication industry independently verified that the NSA had indeed enlisted the cooperation of not only AT&T, but Sprint and MCI (now Verizon). The ACLU

---

[6] Snowden has since asserted the inclusion of many more hubs, nationwide.
[7] The Narus corporate website describes their line of cyber-security products somewhat ominously as "Cyber 3.0: Rise of the Machines," invoking the title of the third film in the *Terminator* franchise, *Terminator 3: Rise of the Machines* (2003). "To adapt to the future of cyber, we have to rely on machines to make fast, incisive, critical decisions. Narus cyber analytics solutions apply machine-based algorithms at the atomic metadata level. They fuse enormous volumes of data and continuously learn from new data dynamics for deeper, richer knowledge that provides contextualized, definite answers that are useful for human analysts" (Narus Solutions).

publicly decried the government overreach in no uncertain terms: "Regardless of the scale of this spying, we are facing a historic moment: the President of the United States has claimed a sweeping wartime power to brush aside the clear limits on his power set by our Constitution and laws—a chilling assertion of presidential power that has not been seen since Richard Nixon" (NSA Spying on Americans is Illegal).

The Bush administration defended the legality of its anti-terrorism programs unapologetically, arguing that the events of 9-11 had represented an act of war, and cited the Authorization for Use of Military Force (AUMF) enacted by Congress immediately following the attacks, authorizing the president to engage any and all methods in the defense of Americans and pursuit of the terrorists. The AUMF's brief and relatively vague language gave the president sweeping powers. Specifically, the president was "authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons." The most candid account of the government's emerging politics of security was voiced by Vice President Cheney. Speaking on *Meet the Press* in the immediate aftermath of the attacks, he explained: "We also have to work, though, sort of the dark side, if you will. We've got to spend time in the shadows in the intelligence world. A lot of what needs to be done here will have to be done quietly, without any discussion, using sources and methods that are available to our intelligence agencies, if we're going to be successful. That's the world these folks operate in, and so it's going to be vital for us to use any means at our disposal, basically, to achieve our objective" (qtd. in Calderone & Froomkin, 2012). In practice, "use of force" has translated in part into a surveillance policy so broad that, if Snowden's revelations are true, the long held prohibition against NSA and CIA surveillance of U.S. citizens may have tacitly and secretly been abandoned. The AUMF continues in effect today, undergirding the state's efforts to enhance and grow its surveillance capabilities. A number of bills, including the AUMF, the Protect America Act, and FISA Amendments Act, and the PATRIOT Act, articulate to strongly empower the state to resist all but the strongest challenges to its authority to surveil with near-impunity. For example, in the case of *Hepting,* although the lower courts ruled in the plaintiff's favor in 2006, it was overturned in 2009 when a federal judge ruled that the telecommunications companies were immune from prosecution under the 2008 FISA Amendments Act (FISAAA) signed into law by President G. W. Bush. Among other sweeping powers, the FISAAA grants the Attorney General the ability to dismiss such cases by simply 'certifying' that surveillance was legal or authorized by the president (EFF's Case).

3.3 Total Information Awareness

While the 9-11 attacks precipitated a number of radical changes underwriting the diminution of civil rights, the expansion of the powers of the military and the executive branch begins far earlier than 2001, according to Shane Harris, author of *The Watchers: The Rise of America's Surveillance State* (2010). While the dragnet surveillance of Americans revealed by Snowden represents the continuation of a surveillance initiative that had begun immediately after the 9-11 attacks, the instantiation of a conservative, hawkish, politics of security has been at least several decades in the making, argues Harris. It does not represent what Gramsci would term a *war of manoeuvre* (a sudden, decisive stroke by which a dominant force overwhelmingly subdues an opposing force), but rather a *war of position* (a steady, concerted and protracted ideological and structural positioning of successive economic, political, cultural, and technological transformations). The politics of security, the emergent surveillance state, and the privacy crisis we now face begins, he argues, in October, 1983 with the terrorist attack on the Marine Amphibious Unit at the Beirut International airport, in which 241 marines were killed. Upon subsequent investigation, it was revealed that several intelligence agencies were separately aware of over 100 pieces of intelligence that, had they been combined, might have helped to prevent the attack. In responding to this crisis, President Reagan's Deputy National Security Advisor and Chairman of the National Security Council's Crisis Pre-planning Group, Vice Admiral John Poindexter, argued for combining the intelligence maintained by the various agencies to create an enormous security database that could help analysts predict and prevent aggressive anti-state activity. After several felony convictions[8] relating to his participation in the Iran-Contra Affair, Poindexter retired from public life and military service in 1987. However, the events of 9-11 eventually led to Poindexter's return to public service, and to the fulfillment of his belief in the phrase that would be the motto of the government security organization he was appointed to lead: "*scientia est potentia*."[9]

Appointed by president Bush in January 2002, Poindexter served as the director of DARPA's Information Awareness Office (IAO) for nearly two years, during which he architected the "Total Information Awareness" program, a program designed to leverage the power of networked digital computers to monitor, collect, link, and analyze massive amounts of both transactional (e.g., travel records, phone call metadata) and biometric data[10] (e.g., fingerprints, face and gait signatures), including

---

[8] Poindexter's convictions were overturned on appeal.

[9] "Knowledge is power."

[10] The types of biometric data which a computer can analyze has become truly staggering, including, height, weight, gender, race, myriad facial characteristics,

data both publicly available (data freely provided on social networks, documents in the public record) and privately available through either purchase[11] or state-commercial agreements (data combined from various national security agency files, medical records, financial records, travel records, and communications such as email, chat, VOIP, etc.). The project also became an umbrella integrating many of the surveillance-related IAO and DARPA projects including: Genoa and Genoa II (developing information decision systems for utilizing big data to make real time assessments for intelligence analysts); Genisys (developing electronic tools for linking heterogeneous data sources together to create massive data-banks); Evidence Extraction and Link Discovery and Wargaming the Asymmetric Environment (developing automated tools for extrapolating links between and patterns for predicting likely terrorist suspects across multiple public and private databases); Translingual Information Detection, Extraction and Summarization (developing tools enabling the interpretive and critical processing of human language by machine algorithm); Human Identification-at-a-Distance (developing tools to recognize human facial and gait biometric signatures); Bio-Surveillance (developing tools to detect in real-time the presence of biological pathogens). However, the program's goals generated strong concerns about government overreach even after its name was changed in 2003 to "Terrorist Information Awareness" to appease public concern. Congress publicly defunded the program in August of that year (Information Awareness Office).

Although the TIA program itself was defunded and the IAO closed, at least two core components of the TIA program were transferred to the office of Advanced Research Development Activity (ARDA), later known as the Disruptive Technology Office (DTO) and known today as the office of Intelligence Advanced Research Projects Activity (IARPA). Thanks to a provision in the Defense Department Appropriations Act of 2003, the TIA program could be legally broken into its constituent components, and these transferred to other programs (Harris 2006). The IARPA continues today to develop several of these core surveillance technologies, including tools for collecting, mining, and analyzing enormous datasets of individuals' information. The programs that worried the public and led Congress to defund the TIA have thus continued unabated and in secret during the last decade under different names (Information Awareness Office). For this reason, though the official TIA program has technically been defunded, I use the term Total Information Awareness as an umbrella term describing the intelligence community's continuing

---

physiognomy, fingerprints, capillary patterns, handwriting, voice characteristics, keystroke dynamics, and social behavior.

[11] A report by the GAO as early as 2006 noted that the Justice Department and the Department of Homeland Security spent approximately $30 million on purchasing private records ("agencies not protecting privacy").

reliance on Big Data as the bedrock of a new model of domestic and international surveillance for ensuring national security and domestic (and to some degree international) social control. As Nissenbaum (2010) observes, the unquestioning faith in Big Data analytics to resolve national security questions and enact social order is likely to produce a worrying spiral of information aggregation: "This faith in information, envisioned as an asset of enormous value, creates a virtually unquenchable thirst that can only be slaked by more information, fueling information-seeking behaviors of great ingenuity backed by determined and tenacious hoarding of its lodes" (p. 44). Exacerbating that spiral has been the government's inability to adequately process the massiveness of the massive datasets it collects and stores, according to Harris. The sheer amount of data has encouraged the state to develop a long range policy which includes, on one level, capturing as much data as it can, while simultaneously working on breaking and undermining encryption standards and developing the software analytics to eventually penetrate the encryptions and protections on the mass of communications they have stored:

> [The entire intelligence apparatus] has been geared toward collection. The technology to connect all these dots does not exist. There is no Google for all the systems that house these different kinds of data…It has become the default position of the intelligence community to collect as much information as possible for the broad purposes of defending against terrorism and other national security threats and to put off the more complicated task of trying to make sense of it. And in this arrangement, privacy and privacy protection has become a secondary concern. (Harris, 2012)

The result of this concerted effort to leverage the power of dataveillance toward a policy of total information awareness can be seen, then, in the construction of the NSA's Utah Data Center, a massive data storage and analysis facility located in the relatively remote Bluffdale, Utah. The Bluffdale facility is "in some measure, the realization of the 'total information awareness' program created during the first term of the Bush administration," writes James Bamford (2012, para. 5). Experts estimate the center will hold anywhere from several exabytes to a yottabyte[12] of information—space it will use to store information obtained from myriad inputs including surveillance satellites, overseas surveillance posts, and those public and private data sources described above and in the following chapter.

The Utah Data Center is the direct descendant of the intelligence program codenamed "Stellar Wind," authorized under the President's Surveillance Program (PSP) enacted by G. W. Bush in late 2001. The majority of the enhanced powers

---

[12] The largest memory standard yet proposed—one septillion bytes.

granted by the PSP remain classified, however it is publicly known that the PSP allowed the NSA to bypass the FISA courts and conduct warrantless electronic surveillance as long as certain legal and factual standards were met. While these enhanced powers remain classified today, revealed Bamford, a report by the Offices of Inspector General of the Department of Defense issued in 2009 had revealed a pattern of evasion and misrepresentation on the part of the Bush administration and the NSA in the prosecution of the program that caused serious concern for a number of senior Department of Justice officials[13], namely: The initial legal assessment of the program was performed by a single DOJ attorney (John Yoo) with no oversight; attorney Yoo's legal interpretation was based on an incomplete understanding (likely from lack of access) to classified activities enumerated in the documents released to him; when informed by Attorney General Comey of "serious issues" raised by the PSP, the President simply obviated the standard practice of having the Attorney General certify his reauthorization, choosing to use White House Counsel Alberto Gonzales, instead. Tellingly, when those classified PSP activities termed the "Terrorist Surveillance Program" by the administration later were moved under the jurisdiction of the Foreign Intelligence Surveillance Court (FISC), President Bush chose to allow the program to expire—only to essentially replace it with the equally sweeping and problematic *Protect American Act* of 2007, which I describe below (Fine, 2010).

The details of Stellar Wind were publicly revealed by whistleblower William Binney, a senior NSA cryptanalyst and one of the chief architects of the agency's digital surveillance infrastructure. Binney resigned in October, 2001 after more than thirty years with the agency on the grounds that the NSA's data collection practices were unconstitutional. With the enactment of PSP, explains Binney in his sworn affidavit for *Hepting v. NSA,* "[The domestic privacy protections of the Foreign Intelligence Surveillance Act] ceased to be an operative concern and the individual liberties preserved in the U.S. Constitution were no longer a consideration…I resigned from the NSA in late 2001. I could not stay after the NSA began purposefully violating the Constitution" (2012). Based on his experience, the enormous size of the proposed Utah Data Center (over 1 million square feet), and Klein's testimony regarding the existence of the NSA's "Narus" rooms, Binney concludes that the NSA continues to engage in the indiscriminant data collection associated with dragnet warrantless wiretapping of both international and domestic citizens, including storing all personal communication. The bulk collection of communication under Stellar Wind was discontinued in 2011, according to Obama administration officials, but the existence of the Bluffdale facility, and of programs like PRISM which feed it, continue to contradict claims of improvemed privacy protections by the state, and intensify the

[13] In fact, several senior Department of Justice and FBI officials planned to resign in protest of the Bush Administration's overreach, including Attorney General Comey.

problematic of privacy. "We are, like, that far [holding up thumb and forefinger] from a turnkey totalitarian state" worries Binney (qtd. in Bamford).

Harris' argument is supported by similar conclusions drawn by political activist Noam Chomsky in *Media Control: The Spectacular Achievements of Propaganda* (2002), who draws strikingly similar connections indicating the ideological continuity between the Reagan, G. H. W. Bush, and G.W. Bush administrations through the continuing political influence of a common core of political actors. Chomsky too, argues that "the war on terrorism was not declared on September 11; rather it was redeclared [sic], using the same rhetoric as the first declaration twenty years earlier" when Reagan described Islamic terrorism as the new enemy of the state (p. 70). The ideological continuity of Poindexter's role in the Reagan and Bush administrations has been made clear. However, several other key personnel solidified and carried forward the ideological stance that we now recognize as the continuity between Reagan's foreign policy agenda and the Bush Doctrine (which I describe below). Donald Rumsfeld, for example—special envoy to the middle east under Reagan, was appointed Secretary of Defense under G. W. Bush, helping to press a doctrine of regime-change in the middle-east. John Negroponte, who supervised U.S. operations in Honduras under Reagan, was appointed Director of National Intelligence under Bush. And perhaps most importantly, Dick Cheney, who served as Vice President under G.W. Bush and was a strong voice in "selling" the revived "war on terror" after 9-11, had in fact served as Secretary of Defense under G. H. W. Bush, Reagan's Vice President. The tight articulation of these particular individuals over several administrations speaks to the continuity of a security politics that has been growing, as both Harris and Chomsky see it, for decades.

Harris' analysis of how the Total Information Awareness program came to undergird the mission of national security is astute work. His examination of the origins and effects of the Total Information Awareness program, and its descendants in state-sponsored programs, helps explain the extant structures of surveillance and control today. I argue for the need to perform a similarly historicized rendition of the contemporary privacy problematic, in which a dominant bloc of state and corporate actors have attempted to woo a subaltern social fraction over the nature and value of privacy. The contemporary privacy problematic in fact draws it shape from shifting economic and technological formations roughly coterminous with the Nixon administrations. This lesser privacy problematic reached its zenith in the first year of the second Nixon administration, during which a group represented by members in the Executive and the intelligence community similarly betrayed its mandate to protect the civil liberties of the American people by employing a new and powerful surveillance paradigm against its political enemies. The discoveries of the Nixon Administration's overreach helped fuel an examination of the nascent dataveillance practices in the commercial sector, albeit with mixed results. Beginning with the

Nixonian conjuncture may help us to understand our own contemporary conjuncture and perhaps even dismantle, or at least rearticulate in positive ways, the namespace.

3.4 The Nascent Privacy Problematic

The historical context surrounding the Watergate scandal had already seen a rising public concern with privacy, and the emergence of networked digital computing contributed to an incipient focus on privacy. The Warren court (1953-1969) was strongly focused on the issue of privacy. As Lane (2011) notes, the term appears in 88 decisions in the 166 years leading up to Chief Justice Earl Warren's 1953 appointment to the high court, but has been featured in 642 opinions since, with 107 decisions during the fifteen-year Warren Court (p. 156). It is generally acknowledged to have solidified the constitutional right to decisional privacy through the landmark case *Griswold v. Connecticut* (1965).[14] The liberal Warren Court also produced or influenced many of the subsequent legislative and judicial milestones in defending and strengthening privacy rights. As I mentioned in the first chapter, William Prosser's 1960 article, "Privacy," drew together existing case law into a framework of torts that helped establish privacy as a modern right. The *Freedom of Information Act* of 1966 (FOIA) ensured greater government transparency by allowing citizens to request authorized access to previously unreleased government documents. The landmark decision *Katz v. United States* (1967) was central in guaranteeing individuals a reasonable expectation of privacy, and in centering privacy around individuals rather than places.[15] Alan Westin's seminal article on privacy argued to extend this from the protection of one's 'person' to information captured about one. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the "Wiretap Act") added judicial oversight for wiretapping and required that surveilled parties be notified after the expiration of the wiretap order.

With regard to consumer privacy, the *Fair Credit Reporting Act* of 1970 was meant to address the fact that credit agencies had been operating behind the scenes, mining customer data with no oversight and reselling the information to third parties—credit companies could supply information to any state agency, commercial organization, or

---

[14] *Griswold v. Connecticut* (1965), in which a Connecticut statute prohibiting the distribution of contraceptives was struck down, was a landmark case for decisional privacy. It stands as precedent for another landmark decision for personal privacy, *Roe v. Wade* (1973), in which a right to privacy was guaranteed under the Due Process Clause of the Fourteenth Amendment.

[15] "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection…But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected" (p. 347).

individual they considered credible (Lane, p. 152). The act anticipated the Code of Fair Information Practices outlined formally in the Department of Health, Education and Welfare's Advisory Committee on Automated Personal Data Systems report "Records, Computers, and the Rights of Citizens" (1973), which recommended a standard code governing data collection for all federal agencies, prohibiting the collection of personal information in secret databases, allowing individuals to discover the nature and uses of the data collected, disallowing the use of data outside of the contexts and uses for which it was collected, requiring organizations collecting data to ensure its reliability and, where possible, prevent its misuse, and allowing individuals to amend any incorrect or personally-identifying information. The Code of Fair Information Practices was used as a template for the Privacy Act of 1974, adding limits to the types of information an organization may collect and the manner in which it may collect it, as well as limits on the internal uses of information within and between organizations. The Act emerged in response to the increasing use by state and corporate actors of computer databases to automate and expedite the process of capturing, storing, and analyzing large amounts of data for large numbers of individuals. The Act standardized the Code for government agencies, prohibiting federal agencies from sharing information about individuals with other agencies without individuals' express written approval, and granted individuals the right to inspect and amend their own records were they not accurate, relevant, timely, or complete.

However, much like the Snowden revelations, it may have ultimately been the "rampant civil rights and privacy abuses of the Nixon administration," writes Lane (2011), that seemed to mobilize widespread public awareness of the extent of state and commercial actors' technological capability for surveillance (p. 189). The public examination of privacy practices in fact began during the last days of Nixon's own administration. In order to appease the public uproar over the Watergate break-ins, President Nixon appointed Vice President Ford the Chair of the Domestic Council Committee on the Right of Privacy (DCCRP), charging him with investigating and pursuing privacy safeguards against the emergence of computer databanking. By the end of its four-month mandate, the committee had produced few results, although it had quashed a $100 million project by the General Services Administration (GSA) to build FEDNET—a network of mainframes linking all federal databases through a single interface. After Nixon's resignation, President Ford promised publicly, "There will be no illegal tapping, eavesdropping, bugging, or break-ins in my administration. There will be hot pursuit of tough laws to prevent illegal invasions of privacy in both government and private activities" (qtd. in Lane, p. 190). However, when one considers the strength of purpose and the continuing attempt, in one form or another, to engender these various mega-databanks—FEDNET, the National Data Center, Poindexter's proposed intelligence leviathan, and the recently operational NSA facility in Bluffdale, Utah—it becomes clear just how unwaveringly, over the last half-

century, the government has moved toward a security policy founded on a network architecture of total information awareness.

Watergate helped publicly politicize the issue of privacy and spurred Congress, over the next several decades, to continue to pursue both privacy protections and government oversight in this area, solidifying, albeit in a statutory hodge podge, the value of various forms of personal privacy, particularly informational privacy in digital modalities. The Watergate scandal prompted a number of oversight committees to investigate the government's reach with regard to surveillance. The United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (commonly, the "Church Committee") thoroughly investigated the practices of the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), and the National Security Agency (NSA). The Church Committee found that the national intelligence agencies had engaged in break-ins, wiretapping, spying such as opening and recording in bulk the mail of U.S. citizens, and even attempting the assassination of several foreign government leaders. The Privacy Protection Study Committee (PPSC) established as mandated by the *Privacy Act* of 1974 confirmed the public's concern over the rising power of the state through its leveraging of information provided by the credit reporting agencies was entrenched and, as Lane puts it, "bordered on the incestuous" (2011, p. 197). Most credit reporting agencies, it discovered, handed over data requested by the federal government freely and without warrants.

"In retrospect" suggests Rule (2007), "the Watergate scandal, and the public mood it triggered, represented the high-water mark of privacy concern in American public opinion" (p. 50). Privacy law, practices, and policies have struggled valiantly since then to adequately address the speed of technological innovation. Ann Toth, Vice President of Policy and Head of Privacy for Yahoo, suggests that in our contemporary technology-rich environment, many state and commercial actors have adopted a implicit policy of 'code first and apologize later'. Relying on either the public's technological ignorance or a policy of plausible deniability, many companies may introduce new products and services which may not be well-scoped for privacy. "Fundamentally, the challenge has been [that]…technology gallops along at a pretty fast clip and legal institutions and government and law enforcement are sometimes taking advantage of the fact that we haven't really figured it out yet…And I think we're constantly trying to catch up with the pace of technology" (Glaser, 2011). Often, where antiquated laws have been updated or amended, those amendments have not adequately addressed the core problems constituted by the shifting technological modalities and socio-cultural conventions of the information and communication media landscape.

For example, the Video Privacy Protection Act (VPPA) of 1988, established after the video rental records of Supreme Court nominee Robert Bork were released publicly, provides strong protections for one very particular digital medium. The act makes it illegal for commercial video tape providers to knowingly disclose the personally identifiable information (PII) of their customers without that customer's written consent, or a warrant, subpoena, or court order. Regarding the purchase or rental of video tapes, PII may not be used in court, and must be destroyed as soon as possible by any third party vendor—no later than one year after its inception. Unfortunately, the medium of VHS and the distribution model (VHS rental stores) protected under the VPPA are essentially obsolete, replaced by new digital formats such as DVD rental and cloud-based video delivery services (e.g., Amazon, Hulu, Netflix, VUDU). The VPAA has not been updated to address the emergence of these media or distribution channels. Protections against data sharing and data-decontextualization that would guarantee users more than merely nominal control over their data have been consistently undermined and challenged by state and corporate actors. In contrasting these practices and prohibitions against the norms, practices, and laws at work in the current conjuncture with regard to informational privacy, it becomes clear that a mere decade later, the privacy problematic emerges in nascent form in the Nixon conjuncture, the shift to what would eventually become the DARPA's Total Information Awareness program had already begun.

The discoveries of the Church Committee of the government's surveillance overreach and burgeoning powers of the military and the Executive led to the enactment of the Foreign Intelligence Surveillance Act of 1978. The Act was designed to strike a balance between protecting the U.S. from serious anti-state aggression (e.g., terrorist attacks), as well as protecting the rights of U.S. citizens from warrantless surveillance through establishing government oversight. The Foreign Intelligence Security Act was passed in partial response to the abuse of various protestors, including civil rights advocates and those protesting the Vietnam War, by the FBI's COINTELPRO program (1956-1971), which surveilled and harassed 'subversive' groups—those deemed by the FBI to be politically left of the current regime (Rule, 2007). However, the act granted the state extraordinary powers—establishing the Foreign Intelligence Surveillance Court (FISC), a secret federal court established to grant warrants for the surveillance of agents of foreign powers, as well as U.S. citizens or permanent residents suspected of espionage or terrorist activity. FISA also allowed the president to authorize warrantless physical or electronic surveillance of up to one year of any non-U.S. individual, and up to 72 hours for any U.S. individual, in cases where that individual was a party to foreign communication.

While FISA was designed to strike a balance between individuals' right to privacy and the state's ability to protect citizens, amendments to the law and the introduction of other laws have extended its already problematic framework to seriously endanger

privacy and other civil rights. The introduction of the AUMF, the PATRIOT Act and its reauthorizations, the President's Surveillance Program, the Protect American Act, and the FISA Amendments Act have mitigated the effectiveness or obviated outright much of the legislation engendered in response to the Watergate scandal. "With the passage of the PATRIOT Act," suggests Lane (2011). "the Bush administration succeeded in undermining nearly all of the scant privacy protections adopted by Congress over the last forty years" including Title III of the Omnibus Crime Control and Safe Streets Act of 1968, the Electronic Communications Privacy Act of 1986, the Computer Fraud and Abuse Act of 1986, the Foreign Intelligence Surveillance Act of 1978, the Family Education Rights and Privacy Act of 1974, the Immigration and Nationality Act of 1952, the Right to Financial Privacy Act of 1978, and the Fair Credit Reporting Act of 1970 (p. 248). For example, the PATRIOT Act broadened the definition of what constituted foreign intelligence investigation, amending FISA such that the court was no longer required to approve detailed surveillance plans. In processing the PATRIOT Act, the government relies on legal opinions which help with the interpretation of the law-as-written. To date, however, those interpretations have remained classified. Senators Mark Udall and Ron Wyden, who have security clearance to have read the interpretations, have argued that current interpretations allow for radically different prosecution of the law and widen surveillance freedoms beyond the intentions represented by the original intent of the law. The original author of The PATRIOT Act, Representative Jim Sensenbrenner (R-Wisconsin), has also stated publicly that he believes the law, as enacted, does not strike the responsible balance between protection and liberty it was original intended to (Kravets, 2011).

Some of the more expansive provisions allowed by the PATRIOT Act were the following: It authorized the use of roving wiretaps and further validated the already questionable practice of pen register and trap-and-trace surveillance; it removed the burden on law enforcement to verify that the person speaking on a wire-tapped line was the person for whom the tap was authorized; it obviated the requirement that agents requesting a FISA warrant describe in detail their surveillance rationale—agents are now required only to declare that records are "sought for an investigation to protect against international terrorism"; it allowed intelligence agents to request a FISA warrant for tangible items (e.g., books, documents, and other personal records) from business, medical, and educational institutions (including public and academic libraries); it provided for the use of National Security Letters, FBI administrative subpoenas which do not require probable cause, a warrant or approval of the FISC, and which bar those served from disclosing that fact of their disclosure to anyone—including legal counsel.

There were specific privacy provisions in place in the Patriot Act, including the requirement that government agencies who had violated privacy be held directly

accountable, that citizens be able to file for damages when their privacy rights were violated, and that Inspector General of the Department of Justice be required to designate an official to monitor complaints from employee of the Justice Department over privacy and other civil liberties violations. The law also contained sixteen sunset provision which specified an end-date for some of the law's most potentially abusive provisions. When the Act was reauthorized by President Bush in March, 2006, it contained only a single improvement to civil liberties, the inclusion that parties prohibited from disclosing their receipt of a National Security Letter request be subject to judicial review. The request could only be made a year after service of the initial request, and the onus of proof lay on the served party to prove the government had acted in bad faith. The sunset provisions were ultimately struck altogether, codifying and extending those provisions which were most troublesome (Wyden, Guthrie, Dickas, & Perkins, 2006, p. 341).

These powers were extended further through the *Protect American Act* (PAA) of 2007 which radically increased the state's power to surveil with near impunity. Specifically, the Act: grants the Attorney General and the Director of National Intelligence the power to wiretap any communication which begins or ends in a foreign country wherein a "significant purpose" of the activity is certified by the state as the surveillance of *primarily* foreign agents, *reasonably believed* to be outside the United States; it grants the state the right to demand data from telecommunications providers, and grants civil immunity to those providers retroactive to 2001.[16]

3.5 Twenty-first Century Statecraft

While the sweeping powers granted in the PSP, AUMF, PAA, and PATRIOT Act were enacted during the presidency of George W. Bush (2001-2009), they have not been significantly repealed or amended during the Obama Administration. While the Obama administration and the G. W. Bush administration which preceded it ostensibly rest on fundamentally different ideologies, there is much they share with regard to privacy policy. The Bush Doctrine emerged ostensibly in response to the 9-11 attacks, although as Harris and Chomsky argue, above, the neo-conservative

---

[16] *Smith v. Maryland* (1979) established the 'Third Party Doctrine', which holds that telecommunications providers such as telephone and internet providers are 'third parties' and, as such, are not responsible for protecting the privacy of users who had shared their information voluntarily. This decision has been used as a precedent to establish the common practice that allows communication service providers to hand over our data to fourth parties, including the government. Third Party Doctrine has been successfully challenged however. In United States v. Warshak, the Sixth Court of Appeals ruled that individuals do have a reasonable expectation of privacy for electronic communications stored or processed by third parties (Reitman, 2012).

ideology of particular actors from the Reagan administration can be seen to emerge full-throated in the foreign policy of the G. W. Bush administration. The core elements of the Bush Doctrine are putatively understood to be expressed in the administration's *National Security Strategy of the United States* (2002). The essence of the Bush Doctrine can be read in the following statement: "It is an enduring American principle that [the protection of Americans and American interests] obligates the government to *anticipate* and *counter threats*, using all elements of national power, *before the threats can do grave damage*" (p. 18). Variously termed "democratic globalism," and "messianic universalism," the bedrock of this doctrine is a U.S. exceptionalism in which U.S. security, prosperity, and the fulfillment of other U.S. interests require the unilateral use of political and especially military power to facilitate the expansion of western democracy and, where possible, regime change. The doctrine conflates a policy of preventative military counter-terrorism with the geo-political expansionism through the promotion of U.S. values in strategic regions, particularly the Middle East (Monten 2005). It favors preventive war and, with the discursive invention of "the war on terror," arguably perpetual war (or perhaps, better, military conflict). While the state enjoyed a moment of hegemony after 9-11, thanks in large part to the galvanizing horror of the attacks, and the decisive leadership of the administration, the Bush Doctrine should be understood as a move away from a politics of hegemony, from Gramsci's *war of position*, toward a politics of direct intervention and coercion, Gramsci's *war of manoeuvre*, or what Monten describes as a move from "exemplarism," in which the U.S. leads through its ability to sustain multilateral international relations which are productive of U.S. interests, toward "vindicationalism," in which the president, declaring himself "the decider,"[17] embraced singularly unilateral policies. As we see above, the Bush administration's relative abandonment of due process after 9-11, with regard to civil and other rights, represented a sea change for privacy. Whereas privacy had historically existed in a more careful balance between the state's compelling interests in security and individuals' rights, privacy under the Bush Doctrine (and the Reagan-era politics of security which inform it), exists in a binary opposition with security. Privacy is a thing to be sacrificed in the name of security. By the end of the second term of the Bush presidency, the moment of total, expansive hegemony produced by the 9-11 attacks and which helped to engender the sweeping changes to privacy and other civil liberties was fundamentally transformed. The practices defined by and enacted through the Bush Doctrine helped to squander the administration's role as moral and intellectual arbiter of domestic and international policy.

---

[17] In 2006, President G. W. Bush termed himself "the decider" in an interview wherein he defended his choice to unilaterally reject the public outcry to replace Donald Rumsfeld as Secretary of Defense: "I hear the voices and I read the front page and I hear the speculation. But I'm the decider, and I decide what's best" (Stolberg, 2006, para. 5).

As a concerted departure from the Bush Doctrine, The Obama Doctrine can be seen as an attempt to return to the politics of hegemony, favoring multilateralism, and declaring its intent to wield moral and intellectual leadership in both domestic and international political theatres. The Obama Doctrine does not eschew the concept of American Exceptionalism outright, however, but seeks to reclaim it and persuade the domestic and international community that an exceptional America need not be conflated with a mitilarist, expansionist geopolitics. President Obama has sought to defend his approach to exceptionalism as a balance: "I see no contradiction between believing that America has a continued extraordinary role in leading the world towards peace and prosperity and recognizing that that leadership is incumbent, depends on, our ability to create partnerships because we can't solve these problems alone" (qtd. in Dish, 2010). Unlike the Bush Doctrine, the Obama Doctrine is not a fully formalized statement, but can be extrapolated from the administration's discursive positioning in a number of key speeches by the president and other key administrative officials, through the enactment of particular policies and practices, and finally through the laws, policies, and practices enacted, extended, or repealed by the president and the individuals who serve under him.

An important early document in that formulation is a 2007 essay by then-candidate Barack Obama in *Foreign Affairs* magazine, entitled "Renewing American Leadership," in which the president outlined a policy which represented a rejection of several of the foundations of the Bush doctrine. The U.S. must, he argued, protect domestic and international civil rights, embrace multilateralism and pursue improved domestic and foreign relations through a more transparent and conciliatory foreign policy. The U.S. must "by deed and example, [lead and lift] the world," so that America is "again called to provide visionary leadership" (2007, p. 2). In order to lead, the U.S. must "[end] the practices of shipping away prisoners in the dead of night to be tortured in far-off countries, of detaining thousands without trial, of maintaining a network of secret prisons to jail people beyond the reach of law" (p. 2). "This is our moment, the essay concludes, "to renew the trust and faith of our people—and all people—in an America that battles immediate evils, promotes an ultimate good, and leads the world once more" (p. 2). In the essay he specifically addresses the role of intelligence in counter-terrorism work, arguing that any successful strategy must leverage radical advances in technology and explore new practices and approaches capable of addressing the differences in the geopolitical landscape after 9-11. This includes the development of "technologies and practices that enable us to efficiently collect and share information within and across our intelligence agencies" (p. 2). Strikingly, the Obama administration shares with the Bush (and arguably Reagan) administration(s) the goal of a unified intelligence network—albeit for fundamentally different reasons. The creation of this new hegemony relies not primarily on offensive military might, but on the construction of a namespace which will allow it to build

American security through Big Data. It hopes to balances security and liberty (albeit prioritizing security) by leveraging a policy of total information awareness to provide more granular control through a variety of tactics, meant to demonstrate restraint and leadership on the geopolitical stage: working more closely and multi-laterally with the United Nations with regard to international conflicts; replacing large-scale military intervention with targeted drone strikes; closing a number of CIA-run prisons in Europe; ending the conflicts in Iraq and Afghanistan and effecting a stable transition; ending the policy of perpetual war, specifically the "War on Terror." The goal of total information awareness is the lynch pin, the *sine qua non* of this foreign policy shift to a limited, defensive but proactive leadership on the global stage. If we read the Obama administration's foreign policy (i.e., the Obama Doctrine) as an articulation, it shares many nodes with the Bush Doctrine, but disarticulates from it its strong neo-conservative ideology, rearticulating a weaker form of American exceptionalism. However, if it rejects a policy of perpetual ground war, the embrace of total information awareness may simply mean the articulation of a perpetual, and largely secret cyber-war.

Two additional important statements constituting the Obama Doctrine and indicative of the importance of the security/privacy binary are represented by two speeches given by Secretary of State Hilary Clinton immediately following the leaks of classified U.S. information by Julian Assange through the Wikileaks website. In Clinton's speeches, first at the Newseum, and weeks later at George Washington University, she delivers the Obama administration's interpretation on the relation of information technologies to the development of secure democracies, as well as its understanding of the relation of economic and political security balanced against privacy and other civil liberties. She suggests that foreign policy in the twenty-first century must acknowledge that cybernetic forms of economic and political control are paramount to national security and economic success. She argues for a transparency that can encourage a global democracy, through the freedom of information and of digital assembly provided by an 'open' internet. She claims the internet as a distinctly American space, granting the United States the right and responsibility to police it. "[A]s the birthplace for so many of these technologies, including the internet itself, we have a responsibility to see them used for good. To do that, we need to develop our capacity for what we call, at the State Department, twenty-first century statecraft" (Clinton, 2010). While governments should protect the "privacy of citizens who engage in non-violent political speech" and who "use the internet for peaceful political purposes," this free flow of information does not pertain to groups such as Al Qaeda who use the internet to "promote the mass murder of innocent people across the world." The internet, she argues, should be used as a tool to track down terrorists who engage in such hate speech. This involves the outreach and funding of academia, industries and NGOs to create a "standing effort that will harness the power of connection technologies and apply them to our diplomatic goals" (Clinton, 2010).

Like the Bush administration, then, the Obama administration has defended the surveillance programs in place, arguing that privacy and security represent a relation that must be delicately balanced—albeit heavily balanced in favor of security. In an interview with Charlie Rose, the president defended his foreign and domestic intelligence policies: "My job is to both protect the American people and to protect the American way of life, which includes privacy" (Obama, 2013). The legal safeguards now in place, he argues, must strike the appropriate balance between security and privacy, particularly with regard to what the administration regards as a growing threat of cyber-attack, which Defense Secretary Robert Gates called a "huge future threat…[and] a considerable current threat" (Montalbano, 2010, para. 2). Clinton's earlier speeches display this same rhetoric of balance: "Without security, liberty is fragile. Without liberty, security is oppressive. The challenge is finding the proper measure: enough security to enable our freedoms, but not so much or so little as to endanger them." While Secretary Clinton describes a perfect balance between liberty and security, Obama's understanding of this balance has demonstrably changed since assuming presidency. For example, in 2005, while still a senator, Obama resoundingly critiqued the government's surveillance overreach with regard to the secretive nature of FISA. Citing the inability of citizens to have substantive legal recourse to challenge overbroad "fishing expeditions" represented by the FBI's National Security Letters, he called intrusive government surveillance "just plain wrong" (Wheaton, Kim, & Cascarano, 2013). In 2007, then-candidate Obama critiqued the Bush administration for erecting a false choice between liberty and security, promising to:

> provide our intelligence and law enforcement agencies with the tools they need to track and take out the terrorists without undermining our constitution and our freedom. That means no more illegal wiretapping of American citizens. No more national security letters to spy on citizens who are not suspected of a crime. No more tracking citizens who do nothing more than protest a misguided war. No more ignoring the law when it is inconvenient…This administration acts like violating civil liberties is the way to enhance our security. It is not. There are no shortcuts to protecting America. (Wheaton et al., 2013)

President Obama's actions demonstrate a different ideological position and a different rhetoric. National security letters have not abated, and in fact have kept pace with the Bush administration's numbers. On average, each year from 2008 to 2013, approximately 19,000 national security letters were delivered seeking information on nearly 8,200 individuals. In response to the privacy criticisms, and particularly the Snowden revelations, Obama claims to have modified the legal framework in ways that redress the shortcomings he earlier outlined in the Bush administration's

approach, and lessen the overreach of the government. However, his stance now reveals the same binary approach to privacy and security he critiqued so stridently in 2005:

> I think it's important to recognize that you can't have a hundred percent security, and then also have a hundred percent privacy and zero inconvenience. We're gonna have to make some choices as a society.…I think, on balance, we have established a process and a procedure that the American people should feel comfortable about. But again, these programs are subject to congressional oversight and congressional reauthorization and congressional debate. And if there are members of Congress who feel differently, then they should speak up. And we're happy to have that debate. (Wheaton et al., 2013)

However, having indicted six government officials so far for leaking sensitive information—already twice the total of all previous administrations, the Obama administration has been accused of pursuing a policy of retribution for administrative leaks so aggressive it has produced a chilling effect on the press. Moreover, promises made by the Obama campaign to promote government transparency, outlined in several reform agenda documents, were removed two days after Snowden leaked government documents. Among the language removed was the following quote, which clearly contradicts the administration's policy on whistleblowers:

> Often the best source of information about waste, fraud, and abuse in government is an existing government employee committed to public integrity and willing to speak out. Such acts of courage and patriotism, which can sometimes save lives and often save taxpayer dollars, should be encouraged rather than stifled. We need to empower federal employees as watchdogs of wrongdoing and partners in performance. (Butler, 2013, para. 6)

And, after it was discovered that the Department of Justice had obtained at least two months of phone records of various journalists at the Associated Press without suspicion of specific crimes, White House Press Secretary Jay Carney was asked by ABC White House Correspondent Jake Tapper how the administration's stance on transparency could possibly "square with the fact that this administration has been so aggressively trying to stop aggressive journalism in the United States by using The Espionage Act to take whistleblowers to court" (Calderone & Froomkin, 2012, para. 24). President Obama later responded "I am troubled by the possibility that leak investigation may chill the investigative journalism that holds government accountable. Journalists should not be at legal risks for doing their jobs" (Remarks by President at National Defense University, 2013). Comparing his rhetoric to empirical

evidence, however, the *New York Times* editorial board responded with a vote of no confidence, claiming that the Obama administration had "now lost all credibility on this issue," and calling the government "reckless in its assignment of unnecessary and overbroad surveillance powers" (Editorial Board, 2013).

In his 2013 interview with Charlie Rose, Obama declared: "What I can say unequivocally, is that if you are a U.S. person, the NSA cannot listen to your telephone, and the NSA cannot target your emails, and have not, by law and by rule, unless they go to a court and obtain a warrant and seek probable cause. The same way it's always been."[18] However, as I demonstrate above, the history of privacy legislation does not stand on a solid body of tradition but more properly represents a struggle between dominant and subordinate political blocs in which privacy plays a greater and lesser role by turns. "We don't have to sacrifice our freedom in order to achieve security," argued President Obama. "That's a false choice. That doesn't mean that there are not trade-offs involved in any given program, any given action that we take. So *all of us make a decision* [emphasis added] that we go through a whole of security at airports. That's a trade-off that we make" (italics mine). But when the president refers to "all of us," he seems to imply a consensus that belies both the truth of the public privacy crisis, and the truth of the broad powers enacted in the name of the Executive Branch after the events of 9-11. By framing the distinction between national security and civil liberties in terms of priorities, Obama is clear about the fact that security trumps liberty. When Rose asserts, "[Y]ou've certainly indicated…that the number one responsibility of a president is national security, to keep the American people safe," the president responds, "[security] is my number one priority because if I don't get that right, obviously, we don't get anything right." However, like the Bush era rhetoric it mimics, the notion that without security there might be no liberty must be understood as a similarly false choice. The ideology at work in this statement is one which continues to support the security state. Remembering the lessons of Orwell's *Nineteen Eighty-Four* (1949), we might ask just how secure protagonist Winston Smith felt without liberty?

---

[18] After President Obama's stalwart refusal to acknowledge more extensive, and certainly unconstitutional surveillance programs—the existence of which continue to leak through Edward Snowden's revelations in the popular media—it is indeed telling to hear him cavalierly describe the evasions necessary to government leaders and high-level officials in the service of national interests. When Rose asks about the Chinese president's response to accusations of corporate espionage, President Obama responds, "You know, when you're having a conversation like this [accusing a foreign leader of cyber-spying], I don't think you ever expect a Chinese leader to say, 'You know, you're right. You caught us red-handed. We're stealing all your stuff and every day we try to figure out how we can get into Apple."

Just as it took the Watergate scandal to inform the public of the surveillance practices of the current administration, the Snowden revelations have encouraged both state and commercial actors to address privacy issues. "I think it's clear that some of the conversations this has generated, some of the debate, actually needed to happen," Director of National Intelligence James Clapper told a defense and intelligence contractor trade group. "If there's a good side to this, maybe that's it." (Ackerman, 2013, para. 6). In September, 2013 FISC Judge Dennis Saylor has ruled that the White House must declassify and release by early October any legal opinions relating to section 215 of the PATRIOT Act written after May 2011 reasoning that the release would contribute to a public debate engendered by Snowden's release of information regarding specific practice of the FISA Court.

The Snowden revelations have also had an effect on global geopolitics. Several countries have raised objections to U.S. surveillance practices. Brazilian president Dilma Rousseff canceled her visit to the White House based on the discovery that the U.S. had been spying on her emails and the emails of other top PETROBRAS officials, which, she argued, amounted to nothing less than industrial espionage. Rousseff has since announced plans to build an undersea fiber-optic cable to obviate the problem of surveillance of Brazilians' data, the majority of which pass transits U.S. jurisdiction, and requiring commercial actors such as Google and Facebook to store data on servers located on Brazilian soil. Additionally, Brazil's state-owned postal service Correios has begun work on an encrypted national email system which would also eliminate the possibility of U.S. snooping (More in Sorrow Than Anger). The EU justice commissioner Viviane Reding wrote to US Attorney General Eric Holder over concerns that US espionage might have serious global consequences. *The New York Times* published an open letter from Russian President Vladimir Putin to the American public and its leaders in which he critiqued the Obama administration's embrace of American exceptionalism, and Ecuadorian President Rafael Correa compared Obama's embrace of exceptionalism to the ideological stance of the Nazi party during the Second World War (Ecuador's Correa). In October, Brazil joined Germany in drafting a U.N. resolution supporting privacy in digital spaces. The resolution will declare deep concern over "human rights violations and abuses that may result from the conduct of any surveillance of communications…[including] extraterritorial surveillance of communications, their interception, as well as the collection of personal data, in particular massive surveillance, interception and data collection" (Brazil and Germany). And finally, most recently it was discovered that the NSA had tapped German Chancellor Angela Merkel's phone for more than a decade—well before Merkel was elected to the office of Chancellor—with full knowledge of the president, reports say (US bugged).

A number of commercial actors have also spoken out against the state's surveillance practices and the legal framework which prevents them from speaking publicly about

requests for customer data. To date, a coalition of 85 companies has launched the Web site petition Stop Watching Us, demanding: congressional inquiry into the NSA revelations, congressional reform of Section 215 of the PATRIOT Act, revision of the FISAA, the creation of an investigative committee which might recommend legal and regulatory reform on U.S. surveillance practices, and the holding accountable of those public officials responsible for enacting and prosecuting these policies. Yahoo CEO Marissa Mayer has complained publicly that she worried about incarceration or being labeled a 'traitor' if she failed to comply with government requests and Facebook CEO Mark Zuckerberg has, likewise, publicly distanced himself from the government, arguing that it failed to balance protection of citizens' freedoms, the economy, and the rights of commercial actors. Speaking at the 2013 TechCrunch Disrupt Conference, Zuckerberg said "Frankly, I think the government blew it" (Geron, 2013, para. 1). Google, Yahoo, Facebook and Microsoft have all filed suit against the Foreign Intelligence Surveillance Court demanding to be released from the gag order imposed on all recipients of National Security Letters. Umbrella privacy organization Privacy International has asked the Organisation for Economic Co-operation and Development to investigate top telecoms, including Level 3, British Telecom, Verizon, Vodafone Cable, Viatel, and Interoute to disclose the nature and extent of their cooperation in releasing consumer data to GCHQ (Telecom Firms). Six of the larger telecoms, including AOL, Apple, Facebook, Google, Microsoft, and Yahoo have authored a letter in support of the The USA Freedom Act, legislation introduced by Senate Judiciary Committee Chairman Patrick Leahy and PATRIOT Act author Representative Jim Sensenbrenner, aimed at reining in the U.S. intelligence community's sweeping surveillance powers by requiring greater transparency and substantial reforms for FISA, particularly enabling service providers to report more information about the number of requests for data they receive.

The pressure to address the government's overreach on surveillance and other civil liberties by government actors, commercial actors, privacy partisans, and a concerned public only strengthen the hegemonic crisis faced by the current administration (of which I have more to say in chapter five) and engender strong possibilities for challenging the construction of the namespace and the total information awareness that underwrites it. The Obama Doctrine represents a move toward rejecting coercive tactics, reestablishing political hegemony through gaining the consent of the public to accede to the state's intellectual and moral authority. Leveraging the administration's demand for the subordinate bloc's consent may help an informed public and press to challenge the administration, as it did during the Watergate scandal, to do better by its citizens. Lane (2011) has argued that just like the Food and Drug Administration, the Federal Trade Commission, the Federal Radio Commission, the Aviation Administration, and the Environmental Protection Agency, the issue of privacy protection demands federalization (p. 257). It may be the case that only through a

standardized bureaucratic apparatus with the power to make policy for both state and commercial actors—and especially to enforce it—will the rearticulation of the namespace (i.e., the disarticulation of the ideology of total information awareness as a viable mode of domestic and international control) be possible.

In this chapter, I have argued that the rise of the security state relies on the policies and protocols of total information awareness at the level of the state. In the next chapter, I address the hegemony of a culture of total transparency which has been widely adopted by the public through its embrace of that product sold by commercial actors, an 'ambient findability', which may in fact represent the most tendential line of force in the articulation of the namespace.

Chapter 4. Privacy and Convenience in the Information Economy

4.1 Ambient Findability

In the previous chapter, I examined the articulation of actors from the Executive, military, and intelligence branches of the U.S. federal government which actively pursues the policies and practices of large-scale dataveillance as an intelligence strategy originally termed *total information awareness*. In this chapter, I examine articulating dataveillance practices, policies, and protocols in the commercial sector, described in aggregate by one of its proponents as *ambient findability.* The constituent practices, policies, and protocols which constitute the economico-cultural ideology of ambient findability must be understood as both analogous to those practices which constitute the state's total information awareness, and as significantly underwriting it. While the practices and policies of state and commercial dataveillance regimes differ, each relies on the social acceptance of a dual proposition: The transformations to communication practices, and social life, wrought by the ubiquity of networked digital communication technologies provide greater security and convenience, guaranteeing citizen-consumers 'safer' and 'better' lives; the guarantee of greater security and convenience must be purchased by the acceptance of less personal privacy in citizen-consumers' relations with state and corporate actors. Observes Yahoo's Head of Privacy Ann Toth, "Data collection online, the collection and use of that information, gives enormous benefit to consumers. Right now advertising makes the internet free and consumers want a free internet. I think that's pretty clear" (Glaser, 2011). The powerful line of force articulating these state and corporate interests in mining the data of consumers produces the contemporary conjuncture I term the "namespace." As we saw in the last chapter, the namespace doubly serves the state, which can leverage commercial dataveillance practices (both legally and illegally) to supplement their own dataveillance practices. In this chapter, I examine the commercial dataveillance practices, the corollary rise of an information economy, and the new marketing and advertising paradigm which supports it.

In the commercial sector, then, the public's acceptance of large-scale dataveillance relies in part on the popularity of ambient findability, the dominant ideology in a "fast emerging world where we can find anyone or anything from anywhere at anytime," according to Peter Morville (2005, p. 6). What I am calling the namespace represents for Morville "an inflection point in the evolution of findability" as the public and private sectors leverage ubiquitous computing technologies to generate myriad, massive (frequently interconnected) databases filled with the largest digital collection of knowledge in human history—to include as well the public and personal data of consumer-citizens. In Morville's eponymous O'Reilly title, *Ambient Findability,* the Web 2.0 phenomenon is held aloft as an essentially unmitigated social good. The increasing ubiquity and availability of consumer data is cited as a cause for "hope and

inspiration" and is indicative of "the reality of progress" (p. 6). For Morville, ambient findability describes the confluence of the technological, economic, cultural, and psychological to create a vast digital information enclosure (p. 6) that empowers the individuals with radical new literacies, as well as economic and social opportunities: "Most importantly," he exhorts the reader, "findability invests freedom in the individual" (p. 6-7). Requiring the tracking and recording of individuals' digital footprint, ambient findability ostensibly offers a trade-off; it offers to meet and even predict their needs by offering them custom-tailored experiences. "The promise of personalization is simple…the benefits to the user are clear. No more searching" (p. 115).

However, after a similar promise made by Google CEO Eric Schmidt at the 2010 IFA Conference in Berlin, Schmidt drew harsh criticism by Consumer Watchdog over his failure to consider the consequences to privacy in the future role he imagined for Google: "We can suggest what you should do next, what you care about," argued Schmidt. "Imagine: we know where you are, we know what you like" (Tsotsis, 2010, para. 6). At the 2010 Washington Ideas Forum, he phrased the same statement somewhat differently, adding: "With your permission you give us more information about you, about your friends, and we can improve the quality of our searches. We don't need you to type at all. We know where you are. We know where you've been. We can more or less know what you're thinking about" (Thompson, 2010). This allows the ostensibly benevolent Google to match your digital footprint to your interests in real-time—particularly those interests which collectively define you as a consumer.

Ambient findability clearly presents more than simple convenience, then, it represents an architecture of control which constrains and influences behavior as much as it maps it. In Deleuze's "Postscript on the Societies of Control," he describes the architecture of control engendered by a simple identification card. "Felix Guattari has imagined a city where one would be able to leave one's apartment, one's street, one's neighborhood, thanks to one's (dividual) electronic card that raises a given barrier; but the card could just as easily be rejected on a given day or between certain hours; what counts is not the barrier but the computer that tracks each person's position—licit or illicit—and effects a universal modulation" (1992, p. 7). Imagine that card held nearly every personally identifying aspect of your identity. Some nascent version of that universal modulation is already in place through the protocological architectures of control developed by the major players in the telecommunications industry. In fact, the major social networks and telecommunications providers inhabiting the web are responsible for the development of the code and protocols transforming the Web

today. In *HTML5: Up and Running* (2010), Mark Pilgrim[1], a developer advocate for Google, suggests that a slight diminution of privacy represents the price we must pay for the transparency and access of an HTML5-fueled ambient findability which will pay broad social, cultural, and economic dividends in the long run. "It's your job to provide as much data as possible," he argues, "Let the rest of the world decide what to do with it. They might surprise you!" (Pilgrim, 2010). "The winners in an HTML5 world, agrees Brett McLaughlin in *What is HTML5?* (2011) "are those who stop fearing being stolen from, and actually start handing out their candy to every kid on the block" (McLaughlin, 2011). And in fact, the inventor of HTML, Sir Tim Berners-Lee, weighs in on the side of openness for economic reasons: "Lots of governments make money by selling data….When you look at so many things, I mean what was the return-on-investment of the Web? You can't put a number on it, but everybody thinks, oh, so many things we couldn't have done without it. Same with all this data. When you put it out there, it just makes life so much easier for people. Their life just picks up, you know? It goes faster. It goes more efficiently, the country goes better…It's difficult to do the math, but when people have done it, it's been often very persuasive that really, making the data available for free is very much, economically, the best thing to do" (Berners-Lee, 2011).

Arguably, the advent of social networking has greatly contributed to the public embrace of ambient findability as a cultural good, reshaping our digital communications with other individuals, organizations, and the government in a large number of ways—many of which we have yet to fathom. For example, "We write," argues Morville, "not just to communicate, but to enhance our own personal findability" (p. 142).[2] Perhaps one of the most perfect expressions—an ideological

---

[1] Ironically, without ceremony or explanation, on October 4, 2011, Mark Pilgrim has "withdrawn from digital life," as Eric Meyer put it, deleting his Github, Google+, Reddit, and Twitter accounts. The only explanation, to date, have been universal agreement to respect his apparent wish for privacy. This was affirmed by a final cryptic tweet by Jason Scott, which read: "Mark Pilgrim is alive/annoyed we called the police. Please stand down and give the man privacy and space, and thanks everyone for caring. The communication was specifically verified, it was him, and that's that. That was the single hardest decision I've had to make this year" (qtd. in "Searching").

[2] While it would be difficult, in the face of the popularity of social networking, to deny the last claim, it does not follow that desires by younger "netizens" to share their lives in online spaces, are necessarily informed decisions. As Frau-Meigs warns, "Young people have no recollection of the tyranny of public opinion nor of the public pressure for social conformity…nor do they fathom the risks that homesteading on the cyber-frontier could lead to cyber-lynching, as reputation building can derail into denunciation and defamation" (p. 91).

paean, really—of ambient findability can be found in a recent Sprint commercial for the iPhone 5, entitled "I am unlimited: Picture Perfect," in which the concept of a 'network' is portrayed in images as the natural interconnection between universe, planet, ecosystem, organism, and computer technology. The commercial means to invoke the values of harmony and human freedom as the narrator triumphantly intones: "The miraculous is everywhere. In our homes, our minds; we can share every second in data dressed as pixels. A billion roaming photojournalists uploading the human experience and it is spectacular. So why would you cap that? My iPhone 5 can see every point of view, every panorama, the entire gallery of humanity. I need to upload all of it. I need—no, I have the right—to be unlimited!" Here, the ability to share our every personal detail online is not a duty, but a right—ideologically linked to, and arguably conflated with, the concept of human freedom and liberty. The grand narrative represented in this single commercial is in fact strikingly ubiquitous in the popular media. Because privacy is weighted against compelling social goods, because it is contextual, decided by the publics it defines, the voices of the those with the strongest interest in promoting it must be the loudest. The continual public statements on privacy by those promoting ambient findability can thus be seen as motivated by the need to continually reinforce the message of ambient findability as a social good. When asked by interviewer Leslie Stahl if he is "trying to turn everything we do on the web into a social function," Facebook CEO Mark Zuckerberg answers: "I think that we're really gonna see this huge shift where a lot of industry is and products are gonna get remade to be social." In such statements, Zuckerberg inhabits the voice of the expert commenting upon a social phenomenon that he in fact helps to architect through the creation of digital code and protocol, cultural and economic practices through the interface of Facebook (and all of the more than 100,000 Web sites it interfaces with). Social networking, we are told continuously by these 'expert' service providers, means that to be a truly 'social' animal means to share everything online.

Although the growth of social networking has slowed to roughly 4% in the three years since 2010, overall media market penetration on average has risen from approximately 45% to 65% in the last five years. The internet and other mobile digital forms of media lead television, radio, and print media across all demographics (Universal-McCann, 2012, pp. 16-20). Globally, the average consumer owns an average of four devices capable of connecting to the internet. While almost 80% of these consumers owned a personal computer, 44% owned smart phones and 14% owned a tablet (Universal-McCann, 2012, pp. 57-62). Public privacy concerns have also risen by several percentage points. "Our research shows that concerns about sharing personal data online [sic] is real and building" (Universal-McCann, 2012, p. 29). One study found that in the USA, Spain, the U.K., Canada, Poland, and Japan, privacy was more important than the opportunity to network socially. However, Brazil, China, India, Mexico, and South Korea demonstrated the opposite trend

(Universal-McCann, 2012, p. 33) with the ability to network socially outweighing the possibility of privacy violation.

Without invoking the argument that social networking represents a technocultural juggernaut that cannot be stopped, we must acknowledge the cultural pervasion and, in fact, the very real benefit of social networking, of transparency, and of social connectivity broadly. As I mentioned in my first chapter, and Morozov's challenge notwithstanding, the Arab Spring can be seen as one positive effect of the collective intelligence and political activism that emerges when communities of people connect virtually. Certainly, people use social networking Web sites and applications for a growing range of social, cultural, economic, and political purposes, including organizing their schedules, making personal and professional contacts, shopping, consuming news and entertainment, self-publishing, engaging in political debate, engaging in religious practice, and a host of other activities newly shifting to digital spaces. Many people spend large amounts of time updating their online presence (62%) and updating their status (52%) (Universal-McCann, 2012, p. 30). Sites like Alice.com are harbingers of the new economics of this age of social networking. Alice.com allows consumers who volunteer their personal information and consumption habits in return for which manufacturers supply these consumers with cheaper and often free products about which they share their information (Gerzema & D'Antonio, 2011). However, these ostensibly free services are 'purchased' through the information we provide in order to 'sign on' to their Web sites (through the necessary step of creating a site profile, the information contained in which immediately becomes the property of the parent site) to accept their services. In order to discover the degree to which our personal information has been monetized on the Web, The Disconnect Web site, which offers tools and tips for protecting individual privacy while Web browsing, offers a tool to estimate the monetary value of the information provided on an individual's Facebook page.[3] This sale of personally identifying information to data brokers and/or the in-house use of that information, both of which are typically used to drive targeted advertising to the user, constitutes the bedrock of the information economy that has, as yet, emerged as the only demonstrably successful means (besides direct billing) for monetizing Web service to date.

4.2 The Information Economy

While lines of direct causal determination would be impossible to draw, the articulation of emergent digital communication technologies, changing interpersonal communication habits, changing domestic and global economic practices, and

[3] As reported in the *Huffington Post*, staffers who used the tool reported a range from $143.27 to $394.63 (Palis, 2012).

changing geo-politics have produced a namespace constituted in and by dataveillance. In the commercial telecommunications sector, this has been coterminous with the rise of what many theorists term an information economy (Langenderfer & Miyazaki, 2009). The importance of the revenue stream generated by the information economy to the larger U.S. economy was recently underscored by President Obama, who mentioned both social network mega-corporations Google and Facebook in his 2011 State of the Union address, as milestones of American invention and ingenuity: "Thirty years ago we couldn't know that something called the internet would lead to an economic revolution…We're the nation that put cars in driveways and computers in offices, the nation of Edison and the Wright brothers, of Google and Facebook. In America, innovation doesn't just change our lives, it is how we make our living." In the speech, the president ties the success of Google and Facebook to nothing less than the economic revitalization of the American economy. The state's commitment to the development of ambient findability (and it own analog—total information awareness) months earlier in a speech given by Secretary of State Clinton at the newseum. The speech, entitled "Remarks on Internet Freedom," (Clinton, 2010) also vaguely tied digital connectivity to economic prosperity: "A connection to global information networks is like an on-ramp to modernity…There are 4 billion cell phones in use today. Many of them are in the hands of market vendors, rickshaw drivers, and others who've historically lacked access to education and opportunity. Information networks have become a great leveler, and we should use them together to help lift people out of poverty and give them a freedom from want."

For the state, the promise of ambient findability represents not only a strengthening of the commercial sector (as greater numbers of individuals engage in internet commerce), but also offers the promise of massive data stores that the state may tap with near impunity. There remain relatively few laws structuring data collection and protecting personal privacy in the private sector. And since 9-11, the government has increased its purchase of consumer information for law enforcement purposes. Individual credit accounts make up the backbone of the contemporary digital dossier. Rule (2007) calls the U.S. credit reporting system, a $4.6 billion industry, constituted by the near-monopoly of a small number of companies including Experian, Equifax, and TransUnion, "a manifestation of surveillance virtuosity unsurpassed by any other system, government or private" (p. 97). The online advertising industry estimated at $36 billion for 2011 and has continued to rise steadily and is estimated by the *Wall Street Journal* to reach $67 billion by 2016 ("Finding Value"). The advertising model on the internet and for each of the larger social networks is targeted advertising. It was, in fact, Google that developed targeted advertising, reshaping the entire internet economy in the process.

This emerging online economy, worries Mark Andrejivic, "increasingly seeks to exploit the work of being watched," as consumers are "recruited to participate in the

labor of being watched to an unprecedented degree by subjecting the details of their daily lives to increasingly pervasive and comprehensive forms of high-tech monitoring" (2002). These new forms of sharing might best be understood to represent Deleuzian forms of social control through continual modulation of the self. "The power in question is not the static domination of a sovereign Big Brother, but that of a self-stimulating incitement to productivity: the multiplication of desiring subjects and subjects' desires in accordance with the rationalization of consumption" (p. 231). Andrejivic describes a primary driver behind the new information economy as a form of labor derived from the ability of service providers to monitor consumers through the technological power and sheer ubiquity of ICTs, and through the appeal of convenient and ostensibly "free" services. But customization also allows for customized pricing. As with customer loyalty cards, the number and type of a consumer's purchases are tracked. Providing a service provider with information about which products are *most* purchased, likely provides them with information about which products should *cost the most*. "The process of naming everything in the universe turns out to be a prelude to enfolding it into a monitored totality subject to the manipulations and ministrations of marketers…an omniscient gaze for the purposes of convenience and profit" (pp. 102-103).

The Federal Trade Commission (FTC) is one state organization responsible for protecting consumer interests. In its report Protecting Consumer Privacy in an Era of Rapid Change (2010), the FTC called for powerful "do not track" mechanisms to be built into Web browsers. FTC Commissioner Julie Brill, addressing mounting privacy concerns at the 2011 Berkeley Browser Privacy Mechanisms Roundtable, outlined the importance of adopting a new model of privacy protection that can account for the ways in which changes in the amount and uses of data has changed the way consumers use technology and the importance of the industry's ability to address these changes with alacrity and openness. We have moved, she argues, from a *notice and choice* model which placed the burden on consumers to choose from among what were often myriad confusing, sometimes obfuscating, incomprehensible choices, to what she calls a *harm-based* model which was "reactive" and is only useful in addressing breaches in privacy, such as security breaches and identity theft, after the fact. The harm-based model, she notes, also fails to recognize breaches which are difficult to quantify in terms of monetary damages, such as social stigma or embarrassment. The state of consumer privacy protection today is represented by the following realities: Collection of consumer data is ubiquitous, both on and offline; consumers remain ill-informed and ill-prepared to make informed choices about data collection; privacy emerges as an overarching concern for consumers, yet targeted advertising is responsible for many of the received benefits to consumers; the distinction between personally identifiable and non-personally identifiable information is blurring as technological systems, organizations, and individuals articulate in ways that may inadvertently violate the privacy of individuals.

The FTC report attempts to develop a set of best practices (heavily leveraging the Fair Information Practice principles developed in the 1970s) to address these realities, including: Promoting privacy by design—the principle that a concern for consumer privacy should drive the design of systems not offered as afterthoughts; aligning levels of security are commensurate with data sensitivity; ensuring the collection of data is restricted to only those data required; ensuring that those data retained only as long as needed. Consumer choice should be effected, it argues, through mechanisms which uses simplified language while remaining informative and meaningful to consumers. The interface/mechanisms of privacy should be judged by five indicia: Ease of use; effectivity and enforcibility; universality of industry participation; consumer ability to opt out of data collection; and interface persistence of consumer choice with regard to data collection. Brill ended with a warning to the browser industry suggesting that a self-regulatory response to these requirements would be sufficient if advertising industry shows that it is willing to honor consumer choices. "It's still [the FTC's] position that if the industry does not act quickly and sufficiently, we will ask congress to take up this issue." In response to the FTC's report, Google, Mozilla, Apple, and Microsoft have added Do Not Track functionality into their browsers. Unfortunately, however, the FTC has no power to enforce these recommendations among data brokerages. Internet privacy issues are generally taken up by the FTC which is empowered act only when a citizen has been defrauded by a service provider.

4.3 Data Brokerages

Hagel and Rayport (1997), predicted a privacy backlash would accompany the ramping up of data mining of consumers. However, they suggested that rather than being strictly concerned about their privacy being violated, consumers might be more concerned by a lack of remuneration for their information. They coined the term "infomediaries" to represent the emerging data brokers who might help consumers aggregate their own data, and negotiate on their behalf for payment for their information. "Businesses have generally assumed," they write, "that information is a resource waiting to be claimed, like land in the western United States during the great land rush of the mid-nineteenth century" (p. 53). One company, the now defunct Lumeria, Inc., proposed to do this by building a unified uber-profile that would drive targeted marketing by reimbursing the consumer for the info they provided. The platform would allow users to monitor and correct their own data. Lumeria would take a small commission, for which it would store and manage the data transactions, as well as facilitate legal action when third parties violated consumers' privacy.

Infomediaries have not emerged as a private service designed to protect consumers. Unfortunately, instead, we have hundreds of what Nissenbaum terms "omnibus information providers," or more commonly in popular parlance, simply "data

brokerages." Affirming Hagel and Rayport's description of consumers as a resource to be mined, Nissenbaum sees the burgeoning array of data brokerages as "evidence of a spiraling feedback loop: the availability of vast repositories of digitized records of personal information spurs demand in all walks of life, demand spurs further supply, and so on" (p. 49). Data brokerages provide their clients (typically advertisers, and/or law enforcement agencies) personal, professional, and financial information, aggregated from a wide range of sources, about millions of individuals. The Dataium data brokerage, for example, can tie a consumer's real life identity to his or her browsing profile it builds from analyzing the links he or she clicks on. Applying advanced analytics to that data, Dataium builds a user profile which it sells to advertisers or vendors who gain additional knowledge, and thus leverage, over the consumer in order to influence their behavior.

The *Wall Street Journal* surveyed the top 1000 most popular websites and found that at least 75% used such tracking software. Among the largest data brokerages, ChoicePoint is known to work closely with government agencies, frequently selling consumer data to intelligence and law enforcement agencies. Choicepoint's security record is not spotless, however. In 2006, the company reached a $15 million settlement with the FTC after it was discovered that it mistakenly sold information to a crime ring of identity thieves (Campanelli, 2006). The most important way that data brokerages function (often entirely surreptitiously—you will likely not have heard the name of most of the brokerages such as Axciom) is through embedding cookies, small data files, on user computers. Retargeting, remarketing, or remessaging, is an analytics service that uses the cookies they store on users' machines in the following way: Once a user visits a site with a retargeting "pixel," a very small bit of code which writes a browser cookie into one's device upon simply visiting the Web page. That cookie can be read by and thus provide information from, any company or organization whose Web site a consumer visits which has contracted with the same data brokerage (and thus whose retargeting pixel they have embedded in their Web page, as well). The result is that a network of companies share visitor data through the cookies that share your information when you visit a partnering site in that network. Google uses their personalized retargeting pixel to drive their adwords service for sites that participate in their Adsense brokerage. Microsoft performs "remessaging" for sites that participate in the Microsoft Media Network. Retargeting/remessaging is a powerful way for consumers to return their product to visibility, then, even after you've navigated away from the original company or organization's Web page. Remarketing/remessaging has been traditionally difficult on mobile devices which do not accept cookies. One company, Drawbridge, is developing an solution which employs statistical analysis to map anonymous location signals to various devices owned by the same user. By triangulating a user's mobile device identities based on location and usage patterns which correlates behavior across

devices, the company purports to be able to identify unique individuals with a high degree of precision and thus directly target that user with ads on their mobile devices.

As the information economy has matured, the next logical step toward being able to market greater number of goods directly to individual consumers has been the move by these telecommunications and other Web service providers to require their customers to use or associate their real names in their Web surfing. The famous *New Yorker* cartoon depicting a dog using the internet and smugly declaring to another dog "On the Internet, nobody knows you're a dog," no longer rings true. Research by the *Wall Street Journal* has shown that during the login process on 70 popular websites, at least a quarter of the time information about the user was passed along to third-parties (Valentino-Devries, 2010). Google and Facebook have both recently shifted, requiring the association of users' real names, ostensibly in the name of greater convenience. It cannot be denied, however, this such a move also serves to cement further the practice of the creation of consumer digital dossiers which can increase the fidelity of the targeted marketing analytics engines.

4.4 Social Networking

Thus, while explicit acts of surveillance are troubling, the more insidious and troubling challenge to traditional notions of privacy is present in the particular formation of a culture of ambient findability pervading the social formation. A major driver in shaping this cultural phenomenon, are the telecommunications service providers—especially those centered around providing social networking services. In fact, renewed interest in privacy may be due in part to the constant swirl of negative publicity surrounding a continuing series of privacy violations to users of their products and services. The two most important examples, here, are the Facebook and Google corporations, in no small part because of the sheer scale of the societal way in which they contribute to the transformation of the lived social reality of hundreds of millions of people around the globe.

Since the launch of Facebook in 2004, the social networking site has become one of the largest companies in the United States, estimated at $100 billion dollars. In under a decade, the popular social networking website has garnered nearly three-quarters of a billion users worldwide and continues to see steady, rapid growth during 2011, with profits estimated at $4.2 billion, nearly double that of 2010 ("Facebook IPO"). Google is likewise a story of rapid growth and financial success. The global multinational has grown into a telecommunications leviathan, absorbing other smaller tech companies and now encompassing nearly all digital communication services, essentially reinventing advertising, email, television, radio.

Both Facebook and Google have had major complaints by both Privacy Partisan and watchdog organizations as well as governmental inquiries. Facebook's history of privacy violations is so egregious that it has come to define, for many, its very mission. Facebook violations of user privacy were first uncovered in an expose by the *Wall Street Journal* in 2010. At one point, all of the 10 most popular apps transmitted user data to third parties without users' awareness or permission (Steel & Fowler, 2010, para. 6). In 2011, ten of the largest advocacy groups signed an open letter to Facebook CEO Zuckerberg requesting radical changes in its opaque and unstable privacy policy: The American Civil Liberties Union of Northern California, Center for Democracy and Technology, Center for
Digital Democracy, Consumer Action, Consumer Watchdog, Electronic Frontier Foundation, Electronic Privacy Information Center, Privacy Activism, Privacy Lives, and Privacy Rights Clearinghouse. In May of 2011, the Electronic Privacy Information Center filed a complaint with the FTC against Facebook on grounds that its privacy policies are both too opaque and protean for consumers. It has violated German privacy laws by mining Facebook's users' contact lists to send unsolicited emails inviting participation in Facebook to user's contacts. After purchasing the popular photo-sharing service Instagram in 2012, Facebook suddenly changed the terms of service to allow the sale of users' uploaded images to third-parties; they were forced to reverse the policy when users complained.

Google, too, has had its share of privacy critiques. Google has violated the privacy laws of several countries, including the United Kingdom, the United States, Canada, Australia, Spain, South Korea, and Germany and is reportedly facing investigations in more than 20 countries worldwide after the wifi-equipped cars it employs for its Street View application inadvertently captured information from user's unsecured wireless networks (Halliday, 2011). Prompted by Google's transformation of its email into a more social networking application called Buzz in 2010. While Facebook's privacy violations reach three-quarters of a billion people globally, it remains confined to a single application. As influential as Facebook is, Google's power and influence is rapidly and easily outstripped it. Google's privacy violations dwarf Facebook's because it reaches into and across a potentially much broader media spectrum. Like Facebook, it has had its share of privacy snafus—none of which have gone unnoticed in the media and popular press. The Former CEO of Google Eric Schmidt is infamous for his cavalier and vaguely threatening pronouncements on Google's plans for eliminating not only an irrelevant notion of privacy, but of consumer choice. "[O]ne idea is that more and more searches are done on your behalf without you needing to type. I actually think most people don't want Google to answer their questions. They want Google to tell them what they should be doing next " (Jenkins, Jr., 2010, para. 10). Hearkening back to 1984, Schmidt's suggestion chillingly echoes one of "the two great problems which the [Ingsoc] Party is concerned to solve…how to discover against his will, what another human being is thinking" (Orwell, 1949/1992, p. 159).

4.5 The Californian Ideology

"It is difficult to overlook," remarks Elliott Sperber in his article "The California Ideology Becomes Hegemonic," "that …[the] oligarchs of the Tech Industry begin to exert more control over national policy" (2013, p. 3). This is precisely what my research demonstrates in this chapter. In their now famous 1995 polemic "The Californian Ideology," Richard Barbrook and Andy Cameron critique the rise of what they see as a "global orthodoxy" that mixes cybernetics, free market economics, and counter-culture libertarianism empowered to obviate alternative futures which do not match its libertarian bent. The Californian ideologues argue for a "'Jeffersonian democracy' in cyberspace," which they draw under the sign and the aegis of the "hi-tech free market" (Barbrook & Cameron, 1996, p. 2). Juxtaposed against this claim, the explanation by Google founder Larry Page of Google's project to digitize the entire world's books seems telling: "Do you really want the whole world not to have access to human knowledge as contained in books? You've just got to think about that from a societal point of view."[4] The Californian ideology "reflects the disciplines of market economics and the freedoms of hippie artisanship. This bizarre hybrid is only made possible through a nearly universal belief in technological determinism…[through which] the new information technologies would realize their ideals" (Barbrook & Cameron, 1996, pp. 2-3). Influenced by the New Right, they argue, the New Left embraced a new form of liberalism—an economic liberalism which elevates the "liberty of individuals within the marketplace," (Barbrook & Cameron, 1996, p. 3) in which "each member of the 'virtual class' is promised the opportunity to become a successful hi-tech entrepreneur" (Barbrook & Cameron, 1996, p. 4). The Californian ideologues reject big government, and foreground the power of markets, as the only possible means to assure the "full flowering of individual liberty within the electronic circuits of Jeffersonian cyberspace"—a liberty available only to the "resourceful entrepeneurs who are the only people cool and courageous enough to take risks" (Barbrook & Cameron, 1996, p. 4). Written well-before the rise of Facebook and Google, "The Californian Ideology" provides a faithful picture of the ideology behind the emergence of ambient findability. "In many cyberpunk novels and films," they write, "this asocial libertarianism is expressed by the central character of the lone individual fighting for survival within a virtual world of information" (Barbrook & Cameron, 1996, p. 5). The hero of the narratives embraced by those who embody and enact the Californian ideology through their technocultural designs, thus appears analogous to the heroic character I describe in the second chapter. This narrative thus underwrites the radical changes to privacy

---

[4] The eventual digitization of all the world's books is a project Google is known to have begun without consulting a single publisher or other relevant authority on copyright or intellectual property.

going on around us by valorizing individual and heroic responses over responses based on an understanding of agency as a process of rearticulation of a variety of economic, cultural, political, and technological forces and phenomena. The cultural hegemony of an emerging impulse to openness, connectivity, mobility, and transparency (for consumers rather than state and commercial actors) articulates to the state's larger project of political hegemony, for many reasons, but certainly among them the Snowden revelations as well as the continuing disaffection with the privacy violations of the telecommunications and social networking providers, that hegemony is now in crisis.

Chapter 5. Rearticulating the Namespace

5.1 Hegemonic Crisis

Americans entering the second decade of the new millennium have come to live in a nascent surveillance society. The conjuncture I term the namespace is constituted in and through ideological and material forces in the form of discourses, economies, laws and policies, technical architectures, codes and protocols, and cultural practices that articulate to form a surveillance regime constituted in and through the articulation of ideologies of total information awareness and ambient findability. According to Frau-Meigs (2010), our "cyberist moment" represents a continuing historical shift toward invasive new forms of social control as we shift from an identity politics favoring acceptance and diversity in the 1980s, to a morality politics of control and regulation in the 1990s, to our present politics of security in the new millennium, during which we witness a regime of unprecedented surveillance coterminous with radical advances in computer technology and associated cultural and economic practices (p. 81).

In the new security state, particularly powerful public (government) and private (commercial) forces align under the sign of a new transparency, openness, and social connectivity which promises to engender new possibilities for personal and professional growth, economic prosperity, more democratic political participation, and national security. These same forces articulate in ways that enable new forms of privacy and other civil rights violations. The articulation of powerful state and commercial actors forms a dominant political bloc for which a major point of articulation has become a shared desire to reframe strong privacy protections as a quaint or irrelevant value—even one that impedes progress. A Diminution of privacy thus serves particular commercial actors by bolstering their ability to obtain and sell individual's personal data in what has become a multi-billion dollar information economy which has allowed many service providers to successfully monetize Web commerce. State actors subject this data to complex analytics for discerning and predicting patterns that might expose possible anti-state activity.

The articulation of this political bloc represented a powerful moment of temporary hegemony after the terrorist attacks of 9-11. However, hegemony is always a temporary settlement of the forces involved in ideological struggle. The namespace conjuncture is constituted in and by several lines of force that challenge the hegemony of the state-commercial bloc. According to Gramsci, when contradictions accumulate across a conjuncture, the dominant typicaly bloc experiences a *crisis of hegemony*, which represents a moment when the dominant bloc, has failed to successfully enact its political program/agenda or been forced to move along the gamut from consent to coercion (Hall et al., 1979). In moments of hegemonic crisis, no longer are the mechanisms that guarantee assent obscured and/or naturalized; rather, they are

spotlighted by an accumulation of contradictions that foreground the process of ideological struggle. At the height of the hegemonic crisis, the state "exhibits more plainly than it does in its routine manifestations what it is and what it must do to provide the 'cement' which holds a ruptured social formation together" (Hall et al., 1979, p. 217). The contradictions at work in the namespace include but are not limited to: the U.S. and global economic crises, spurred in part by the failure of major U.S. banks; the expense and toll in human lives of several (arguably failed) U.S. military campaigns; the revelations that the U.S. disregarded its own constitution and other international agreements in both imprisoning and torturing citizens without due process, and spying en masse on its own citizens; and the realization that commercial telecommunications service providers have directly or indirectly, through agreement and compulsion, supported the de facto creation of a global telecommunications surveillance regime.

This latter feature of the namespace represents one particularly strong and self-evident contradiction, which can be seen in the way state actors have tended in past decades to simply bypass or challenge (both legally and illegally) restrictions and prohibitions on particularly intrusive forms of surveillance—i.e., essentially annexing the commercial telecommunications industry as a wing of its security apparatus. The articulation of these contradictions belie the boon of the new security and convenience provided by dataveillance and has spurred the subaltern fraction to an acute if nascent political consciousness of the problematic of privacy. Certainly in the popular and academic media, the prominence of these contradictions has encouraged more critics to recognize the politics of the namespace as the relation of powerful interests both in the public and private sector. "Were Big Brother to come back in the 21st century, he would return as a public-private partnership," notes one *Guardian* reporter (Ash, 2013, para. 1). These media are increasingly beginning to recognize and foreground the binary of security/privacy in which privacy represents the subordinated value. A July, 2013 poll by *ABC News* and *The Washington Post* indicates that by a margin of 57%-39%, the public sees it more important to violate individual privacy than to protect it, in order to protect against the threat of terrorism. While still a significant majority, what is important to note is the degree to which that margin has been rapidly narrowing. The number of people who question government privacy invasion in the name of security is 10% points higher than in previous ABC/Post polls of 2003 and 2006. While 42% of those polled say the NSA surveillance is increasing security, 47% do not see it as contributing to Americans' security, with 5% seeing it as contributing negatively (Cohen & Balz, 2013). Because the hegemony of the dominant bloc relies on the consent of the subordinated bloc, and that consent seems to be significantly diminishing, the moment is thus ripe to contribute to the counter-hegemonic struggle to rearticulate the namespace in ways that strengthen privacy and other civil rights, to explore the alternatives to an information economy in which consumers are commoditized and mined for their

personal information, and to resist those calls for a state organized around a surveillance-driven security politics.

As an example of the dynamic and contingent nature of struggle that characterizes the uneasy settlement of political hegemony, and of the political opportunity available to the subordinated bloc in the process of re-articulation, I point to the contemporary example of the changing American Republican party. This example speaks to the possibility for political change in noting how the dominant bloc, in winning the consent of the subordinate bloc, must agree to certain concessions. The granting of such concessions is never simply nominal, notes Jones (2006), and always produces the possibility of instability and change within the dominant bloc itself. During the last two election cycles, the Republican Party has sought to attain a more expansive hegemony by articulating to itself a demographic of conservative, white, middle class, often evangelical Christian voters. During the 2004 election, the party actively continued to draw upon the conservative religious element it had come to understand and characterize as its base. This strategy, over two election cycles, from 2000-2008, represented more than simple capitulation, since to articulate a subordinate group to itself and thus win its consent, the dominant bloc must "thoroughly recreate itself," writes Jones: "A truly hegemonic group or class really must make large parts of its subalterns' worldview its own" (2006, p. 46). After articulating to elements of this conservative demographic, the Republican party thus found itself to some degree mediated by a populist political wing which described itself as the *Tea Party*. The Tea Party was able to successfully claim a large number of seats in the House of Representative. And, in fact, counted with their supporters, the Tea Party can be seen to represent a significant force in the Republican party. Through hegemonic struggle the Tea Party has worked to rearticulate the Republican party itself. As Williamson et al. note, this poses a problem for Republican moderates, in that Tea Party republicans have pushed the party so far to the right ideologically that non-Tea Party Republicans are now seen as closer to Democrats than to their Tea Party compatriots (Williamson, Skocpol, & Coggin, 2011). This example demonstrates the possibilities for political agency inherent in the hegemonic process, for although a bloc must struggle to carefully maintain its hegemony, that process has the capacity to transform the dominant bloc itself.

With regard to privacy, this presents a hope for directly engaging with the dominance of the dominant state-commercial bloc in the namespace. Privacy partisans must be able to leverage the intensity of the privacy crisis toward substantial political change, to harness the collective outrage expressed at the self-evident contradictions between what the U.S. proclaims as its economic, political and technological ideals and those it enacts. Such work begins through recognizing the dominant bloc's tenuous hold on the position of moral and intellectual leadership, discovering those points of articulation vulnerable to rearticulation, and working to shift those connections,

linkages, and alliances to a more positive and just effect. In this way, privacy partisans may open the dominant bloc to making concessions, and perhaps, like the Republican party, to significant rearticulation. Shane Harris (2010) suggests that, as we are significantly distanced from the events of 9-11, the type of security crisis which promotes jingoist nationalism and helps cement political hegemonies, now is the time to press for political change:

> I think that now in the relative calm before another attack is the time to start asking these hard questions about how we strike this balance…If there is another attack on the United States on the order of 9-11, this question about balancing security and liberty will become strictly academic. The government will come down decisively on the side of security because that's what it knows how to do. It will collect [private information] on a scale we've never seen. It will be clumsy. It will be driven by urgency and by fear. And then you will see, I believe, many of the infringements on individual liberty that many of us have only worried about to this point.

Below, I explore some of the ways that those interested in defending and strengthening privacy rights can begin to engage with privacy in the namespace, which I've only begun to map in this dissertation. I examine individual praxis—immediate action average citizen-consumers (those with no special training in the issues of privacy) might take in their own lives, through engaging directly with technical practices. I then move to the ways in which these same individuals might engage in collective praxis—working at a more conjunctural level in concerted political and economic ways. Finally, I suggest ways in which the contributions of academics and other professionals might develop an expert praxis, rearticulating the namespace conjuncture through education.

5.2 Individual Praxis

It does not necessitate adopting the myth of the solitary, rugged, everyman versus the monolithic social structure, which I describe in chapter two, to recognize that individuals can and should engage with the privacy crisis at the level of their everyday lives. One way to work individually for privacy, is to begin to educate oneself about privacy issues, being careful to contextualize the seductive but overly reductive narratives I describe therein. Books by what Hall et al. (1979) term *primary definers* are valuable, of course, in coming to understand the perspective of the dominant bloc. Like Google Chairman Eric Schmidt's book, which I describe in the second chapter, the work of privacy apologist Jeff Jarvis in *What Would Google Do?: Reverse-*

Engineering the Fastest Growing Company in the History of the World (2009)[1] and *Public Parts: How Sharing in the Digital Age Improves the Way We Work and Live* (2011) is instructive at least in the drawing the extreme boundary of resistance to stronger privacy rights. Juxtaposed together, each represents a clear example of the Californian ideology I describe in the previous chapter—an ideology easily challenged when we think with articulation. In this same vein, the dramatic irony in dystopic action films such as *The Conversation* (1974) and *Enemy of the State* (1998) may play a hortative role, warning us of the dangers of a transformed and diminished privacy right and calling us to action. However, intellectually we must recognize the influence of market, industry and other forces which work to simplify the narratives of popular media (and particularly action films). In the news media, reductive narratives can be recognized as those accounts which rely on trite metaphors and simplistic models of social control, which portray agency as the property of individual actors rather than the complex interplay between technological, cultural, political and economic forces, practices and ideologies. Reductive accounts are frequently instructive in single dimensions, sometimes providing important facts, but must be balanced against counterclaims, and ideally, juxtaposed against accounts that recognize the complex interplay of forces in any social determination. Narratives that moves us away from thinking with articulation, toward an heroic narrative of individual agency—one lone hero against a technological juggernaut—we must be careful to acknowledge the rhetorical pathos of these social science fictions and problematize them.

Kevin Roose (2013) details some of them in his *New York Magazine* article "The Surveillance-Free Day," in which he attempts to live surveillance-free for 24 hours while still engaging in the activities common to the urban dweller, such as shopping online, sending e-mail and tweeting, using his mobile phone, and taking public transportation. The sizable list of preparations required to obscure his digital footprint included hobbling wi-fi and transmission capability for most of his digital devices and turning off completely those digital devices which could not be stopped from transmitting data. To ensure his privacy while staying digitally connected, he downloaded an application called Wickr to encrypt and auto-erase texts and photos posted to the Web. He enrolled in a Web service called "HideMyAss," which provides a private Virtual Private Network (VPN) to obscure his browsing history and other network activity. Unable to use a credit card, which are legally tracked by corporations and the government, he used the anonymous digital currency Bitcoin. For encrypted email, he signed up for a free Hushmail account, and for Web surfing he opted to download Tor, a browser which encrypts its Web searches. Finally, and most absurdly, to combat surveillance by the network of CCTVs which pepper the

---

[1] Jarvis' title, in which the term "Google" is substituted for "Jesus," is apt—as his work generally demonstrates, he understands Google and its work as nothing short of messianic.

urban landscape, he constructed and wore a battery-powered baseball hat with infrared light bulbs meant to obscure his face from those cameras using infrared lenses. Of course individuals need not go to such lengths to ensure they have more privacy when using the myriad information and communication technologies in their lives. Educating oneself about the types and extent of the data being sent by the technologies you use, is a strong first step. It is also important for individuals to be aware of what options they may control in disabling or opting out of the intrusive tracking from government and telecommunications providers, and to investigate the protective privacy policies and settings on all major Web sites, apps, and services they use.

While no doubt a fascinating experiment, it is important to recognize the limited application of an approach like this. Working as an isolated individual who must construct his own anti-surveillance technology is impractical for all but a handful of the techno-savvy. His essay thus fails to contribute useful thinking about the possibilities of rearticulating the namespace itself, about how our vast technocultural assemblage *might be otherwise*. Roose does recognize the articulation of state and corporate interests and his own willing participation in the diminution of privacy: "Most of the surveillance I've encountered today isn't part of a vast conspiracy. In fact, a lot of it has been explicitly authorized by law, and by decisions I've made consciously. I've known for years that Google's algorithms scan my Gmail in-box in order to show me more targeted ads, and I've been aware for weeks that Facebook has cooperated with the NSA. And yet, even after learning about PRISM, I kept logging on, because I like having free, useful web services" (2013, para. 7). Ultimately, however, his article exemplifies the media's tendency to understand the privacy crisis through the lens of a panoptic model of surveillance, narrating for us his urban odyssey as the story of one man's struggle against monolithic surveillance forces, rather than a techno-cultural assemblage that we might politically engage with.

Informed by more nuanced accounts, individuals will be better prepared to engage directly with the information and communication technologies and practices in their own lives while contextualizing the degree to which individual action can be politically effective. For example, most individuals are too connected to their banks, telephones, computers and other networked electronic devices and services to move to a remote wilderness, eschewing all modern convenience for the sake of privacy. Such measures are both unattractive and simply impractical for the broad public whose social lives are constituted by an interconnectivity which is deeply mediated by ICTs. However, for those who wish to remain digitally interconnected while protecting their privacy, there are solutions. Under the current articulation of the namespace, individual praxis (of a more pragmatic and non-heroic nature), remains necessary to safeguard those privacy violations that are an immediate and preventable result of users' failure to learn to change the settings and defaults of technological switches,

settings, and practices established by the commercial actors who see consumers as resources to be mined.

5.3 Collective Praxis

However, as the recent revelations of the state's willingness to simply ignore legal and technological safeguards in their promotion of the security state, and thinking with articulation, we should recognize the need for a strong collective praxis, as well. We move beyond the everyday concerns of the individual into a broader political and economic action by engaging with larger social and political collectives. Because the state is not a monolithic material ideological structure, government actors can be seen and encouraged to support privacy reforms and resist government overreach—and this form of interaction remains a useful for of individual political praxis. For example, Senator Russ Feingold, chairman of the Senate Judiciary subcommittee on civil rights, has spoken out against government overreach in this area: "'Trust us' doesn't cut it when it comes to the government's power to obtain Americans' sensitive business records without a court order and without any suspicion that they are tied to terrorism or espionage" (Miga, 2007, para. 6). Senators Ron Wyden, Mark Udall, and 25 other senators have collectively plied the Obama administration to declassify and release information on the extent of the NSA surveillance. In September, 2013 senators Ron Wyden, Mark Udall, Richard Blumenthal, and Rand Paul crafted the Intelligence Overview and Surveillance Reform Act to end the warrantless dragnet collection of phone records of U.S. citizens. This bill would amend FISA Titles IV and V to prohibit the bulk collection of email and telephone records of U.S. citizens, respectively. It would amend a number of National Security Letter statutes to both prohibit the bulk application of National Security Letters, and to ensure greater transparency from the government in its use of National Security Letters. It would also reform Section 702 of the USA PATRIOT Act by eliminating the "back door searches" loophole (thus requiring the government to obtain warrants); prohibit the collection of ancillary information not specifically the communications of the investigation's target; specifically address and outlaw the practice of targeting the communication of foreign individuals in order to surveil a U.S. citizen(s) known to be in communication with that individual; place stronger limits on information collected unlawfully by the government; create an independent Constitutional Advocate who can balance the court through the imposition of an adversarial role; require the U.S. Attorney General to declassify those FISC rulings which represent significant interpretations of the law or the U.S. constitution; permit Constitutional challenges; permit citizens impacted by surveillance to petition the court for redress; permit private companies to reveal information about their disclosure of customer records and increase government reporting; authorize the Privacy and Civil Liberties Oversight Board (PCLOB) to subpoena and compel the testimony of government officials ("Domestic Surveillance Reform," 2013). By focusing on those elected

officials assigned to select committees which deal with privacy concerns, and those officials who have shown publicly they support privacy and mean to resist the emergence of the surveillance state, citizen-consumers may engage politically.

For individuals less familiar with the maze-like hierarchy of government influence, the assistance of privacy partisan groups is an effective way to navigate the maze of political activism. The privacy crisis has spurred the growth of the number of organizations that pursue policies of transparency and equity with regard to government and corporate actors, document and fight privacy violation, and attempt to theorize an emerging surveillance society, both in the U.S. and abroad. These organizations include: The American Civil Liberties Union, Center for Democracy and Technology, Center for Digital Democracy, Consumer Action, Consumer Watchdog, Electronic Frontier Foundation, Electronic Privacy Information Center, Privacy Activism, Privacy Lives, Big Brother Watch, Privacy Rights Clearinghouse, Global Information Liberty Campaign, and perhaps the largest organization, Privacy International, which emerged in 1990 as an umbrella organization of over 100 individuals and organizations from several countries, including Austria, Bulgaria, Belgium, Denmark, Finland, France, Hungary, the Netherlands, Spain, and Switzerland. These organizations, most of which are non-profit, non-government organizations, marshal personnel and resources to lobby Washington, write amicus briefs, and sue for greater privacy protections. Citizen-consumers can contribute to any group that encourages responsible uses of information technology, particularly those which foreground the importance of privacy and other civil liberties, through membership, which often provides an educative benefit, through financial donation, and/or through contributing their own expertise. By expertise, let me make clear I am not invoking the technical super-hacker who works surreptitiously within the system both to subvert code, and to reify the system itself. This was the dream of the cyberpunk ideology, which, as I note in my fourth chapter, underwrites the Californian Ideology's determinist understanding of the relation of technology to culture. The expert praxis I envision must represent an embrace of transparency, must abandon assumptions about technology and culture with regard to determination. Experts must leveraging knowledge, skills, and ethics before and during the creation of code, machine, and practice.

5.4 Expert Praxis

Expertise is one of the most powerful elements of political praxis. Gramsci recognized that hegemony is derived in part through the media's resourcing of members of the dominant bloc to stand as experts. The Web has opened out traditional circuits of discursive power to experts (and amateurs alike) who may now construct blogs and other analogs of traditional media. The Web has enabled greater sharing of expertise, even among those with fewer financial resources and access to media outlets, allowing

individuals to organize by leveraging the collective intelligence of entire communities. Contributing expertise in an open forum is one vital way to get involved politically. In order to engage with the experts of the dominant bloc—those who are first in setting the terms of the debate around privacy—the subordinate social fraction must encourage its own intellectuals to articulate to the namespace, as it is currently articulated, their own ideologies.

One example of such a forum is Groklaw.net, an award-winning blog which provided a space to join experts (and other interested and knowledgeable parties) in law to those in technological fields in discussion on subjects which benefitted from the open discourse between specialists in these two fields, engendering debates over free and open source software (FOSS), patents, and intellectual property, among others. Groklaw ran from 2003 to 2013, when it closed citing the revelation of the government's ability to monitor private emails with relative impunity. Such government powers, argued founder Pamela Jones, prohibited sensitive work that required confidentiality, abolished the basic human right to live free from constant surveillance, and represented de facto proof that the surveillance state was a fait acompli: "There is now no shield from forced exposure" (Jones, 2013, para. 29).

Several other privacy-centric sites have recently closed, citing the same reason. In a message that supplanted the company's homepage, encrypted email provider Lavabit (in the news recently as Edward Snowden's email provider) explained their reason for closing after ten years: "I have been forced to make a difficult decision: to become complicit in crimes against the American people or walk away from nearly ten years of hard work by shutting down Lavabit… I wish that I could legally share with you the events that led to my decision…the first amendment is supposed to guarantee me the freedom to speak out in situations like this. Unfortunately, Congress has passed laws that say otherwise" (Estes, 2013). Implied in this open letter is that Lavabit's owners have been legally bound under provisions in the PATRIOT Act from disclosing their receipt of a National Security Letter. While the decision of these sites to discontinue service was understandable, it only strengthens the hegemonic bloc by lessening the counter-hegemonic discourses and services available. The increase of counter-hegemonic discourses is more important than ever, under a burgeoning security state.

On the other hand, the destruction of company-held data before the state can claim it should not be seen as an act of cowardice, but an act of moral conscience. The closure of Lavabit was immediately succeeded by the stunning elimination of a major product line by company Silent Circle, a company which until recently offered a secure email service. After the Snowden revelations, and inspired by his courage, the company took a moral stand and eliminated its database of user information in the interest of privacy. CEO Michael Janke explains their rationale: "We knew that metadata was

just as dangerous as email content regardless of if the contents of an email are encrypted…We were literally sitting on a treasure trove of data that was highly valuable to many, many nations and intelligence agencies of the world. We made the pre-emptive decision to just scorched-earth it" (Gewirtz, 2013, para. 7).

Silent Circle's actions raise the question of civil disobedience. While it is often more than simply inconvenient for those Davids who take the brunt of retaliation by public and private Goliaths—Lavabit and Silent Circle abandoned entire revenue streams—this type of civil disobedience represents a relatively powerful form of political praxis. In the case of George Christian, executive director of a 27-member Connecticut library consortium, it was *successful* counter-hegemonic ideological struggle, when Christian, and other unnamed librarians, refused to comply with a national security letter to obtain patrons' computer records. Christian et al. were successfully defended by the ACLU, and ultimately were never required to turn over patrons' records, nor were they penalized by the government for their non-compliance. This points to the possibility of political resistance by collectives of expert individuals willing to fight together for privacy rights against unconstitutional government practice (Cowan, 2006).

5.5 War of Position

In *Moral Politics: What Conservatives Know That Liberals Don't* (1996), George Lakoff has argued for understanding the importance of the ideological dimension in political struggle. Lakoff suggests that after Goldwater's defeat in the 1964 U.S. presidential election—a solid blow to the social popularity of conservative ideology—conservatives embraced a new strategy for encouraging and strengthening a new generation of conservatives through rearticulating the educational and media landscape in their own interests. This strategy was built upon tapping wealthy conservative donors to endow academic chairs, institutes, and organizations for teaching conservative business practices. Independent conservative think tanks with total autonomy would also need to be created outside of academia, they realized. To develop rigor and respectability for their ideological program, conservatives would need to create publications, journals, magazines, and to purchase media outlets outright to help disseminate a conservative ideology directly. The limited hegemony of the conservatives is a direct effect of a concerted effort over nearly half a century—a forty-year "war of position" as Gramsci would describe it—in which conservatives have successfully re-articulated the political landscape through a process both infrastructural and ideological, both material and discursive. Among these various conservative factions (e.g., fundamentalist Christians, libertarians, fiscal conservatives, social conservatives, neo-conservatives, etc.) some are more powerful than others, but all are articulated together, Lakoff argues, under a single point of articulation: an ideological vision of the Christian God as a strict father-figure, and a clear understanding of just what that

ideology means and how it translates to political life. The problem for liberal progressives who want to resist this model, he suggests, is that, unlike the conservatives, they are not well-organized and cannot clearly elucidate and articulate just what their own ideology is and how it translates to political life.

The long-term ideological struggle Lakoff describes between conservatives and progressives, is—or should be—analogous to the ideological struggle between the dominant bloc, and subordinate social fraction which it seeks to articulate to itself, over privacy, civil rights, security, and surveillance in the contemporary namespace. In order to fundamentally rearticulate the namespace, I argue, involves finding and deploying means for dis-articulating and re-articulating the forces that empower the hegemonic bloc. Thinking with articulation helps us to recognize that the successful approach by the conservative bloc (i.e., rearticulating the political landscape through the educative function) might similarly succeed for privacy partisans through the creation of a bloc constituted in and by counter-hegemonic discourses, institutions, alliances, etc. This bloc should be made up of both academics and those from private industry.

The need for diverse expertise is clear, particularly at the juridico-political level wherein law and policy are enacted and enforced. As I argue in the third chapter, the repeal of the PATRIOT Act is a necessary first step to restoring the protections which it renders inert. That single step, however, must exemplify a larger concerted effort to unify an active political bloc to support the restoration of privacy and other civil rights. For example, the putative problem of the preponderance of insular, corporate-funded lobbyists must be adressed if counter-hegemonic struggle is to have an effect. Corporations frequently allocate staff resources to write amicus briefs and other educative materials for congressional and other policy bodies. Like the conservatives, progressives and privacy partisans must find ways to ensure their expertise and orientations inform the policies being engendered which serve the dominant politics. Policy decisions which are based on the intersection of technology and culture, for example, require a nuanced understanding of the interrelation of each. Steeves (2008), for example, found that the Canadian Supreme Court's failure to understand the complexity of privacy in online spaces may have "limit[ed] the court's ability to protect us from surveillance technologies that negatively affect our dignity, autonomy, and social freedom" (p. 334). Informed by a technological determinism which elevates technology as the central actor, and failing to consider the shifting social habits of a changing technocultural landscape, the court, she argues, failed to protect the privacy rights of Canadian citizens. The application of particular theories and methods of social science, agues Steeves, would allow courts to make more just decisions, informed by the strong analysis of complex social-technical systems and human behavior.

The same educative expertise must be leveraged to inform our own legal system. For example, speaking at the 2011 Fourth Circuit Judicial conference, Chief Justice John Roberts was asked about familiarity with, and any specific court policies on, social media and other Web technologies. Roberts replied:

> I don't think any of [the justices] have a Facebook page or "tweet," *whatever that is* [emphasis added]…The impact of the new technology on substantive law is really quite significant…But that too is nothing new. I mean you think of the Supreme Court's dealing with the wire tapping cases when wire taps were the new thing. The first decision says 'Well, of course that's not covered by the Fourth Amendment…then the court came to have some experience with it and reversed itself…It's one of the great things, again, with the law clerks. They come in and *they know how all this stuff works* and *what it means and they're a nice resource for kind of educating those of us who are a little behind the curve* [emphasis added].

Roberts' answer is troublesome in several respects. It seems to indicate he is both unfamiliar with and dismissive of the cultural, economic, and certainly political import of social networking. While it is true that rulings shift based on changing social, cultural, political and technological changes, and that the justices of the high court cannot be expected to be expert in subjects beyond the law, Roberts' response indicates that the court receives its understanding of the workings and significance of modern information and communication technologies serendipitously, from incoming law clerks, who are themselves no more likely to be critically prepared in this area. And in Roberts' case, such knowledge must be nugatory, since he disclaims any knowledge of Twitter, one of the world's largest social networking platforms—a platform involved for example, in the social transformations represented by the Arab Spring. Especially in light of the revelations of government surveillance of commercial communications providers I discuss in chapter three, it is difficult to imagine that Roberts has not been briefed about the significance of social networking to the U.S. government, and to the U.S. economy. Roberts' response thus points to a particular rhetorical exigency that might be addressed by the bloc of interdisciplinary experts I suggest above who are able to work with those in commercial and state sectors to inform those making U.S. policy and law.

One of the important ways in which we might build this expertise is by providing an inter- or cross-disciplinary education which can help students successfully negotiate the complexity of the contemporary namespace. While many young people often already have a relatively strong literacy in the practices of consumption and production of digital forms of culture, they may not have naturally internalized a critical approach to the complex literacies of the multiple ICTs which pervade their

daily lives, nor intuitively recognize the ways in which mainstream media producers serve the powerful interests of economic and political actors. Even for those who do, it's important to recognize, as I point out in chapter two, the ideological power of the technical and cultural architectures, protocols, and codes through which political reality is mediated and constructed for them. It is thus important to rethink traditional disciplinary curricula through the lens of articulation, in ways that might better demonstrate for students the importance, for example, of thinking culture, technology, law, politics, and ethics together, as deeply imbricated, deeply articulated. While I agree with Luke (2002) that "the challenge for new media pedagogy is to connect students' everyday interactions and experiences with media technologies, to classic questions of equity, privacy, fairness, openness, access, power, and so on—to give the students the critical vocabulary and tools to think with and to encourage them toward more active and principled media use and participation," to do this means engaging students at the point of mythologizing which typically accompanies any discussion of technoculture by "sustain[ing] the constructive affirmative energy of the myths, while pointing the way beyond simplistic hype," or what we might describe as engaging directly with the dominant codes on offer (p. 561). I provide an example of this type of work in my second chapter.

In order to truly engage with the discursive myths and social science fictions mediating our relation to new media, we must understand the role played by particular digital codes and the logical and material architectures and technologies which accompany them. To understand the meaning of the rise of networked computing, and associated socio-cultural phenomena such as social networking, involves understanding the Web as an articulation across the social formation, notes Langlois (2005), as "socially shaped and culturally distinct through a renewed focus on its technological characteristics" (p. 579). We do this by understanding it, she argues, as a conjuncture—an "assemblage of technocultural layers," both those which culturally contextualize and shape it, and the technical architectures which structure it.

> A starting point for examining the layers that constitute the Web is the analysis of the different cultural values that are encoded within the technical objects and processes that form the Web….[T]he protocols that make the Internet an open network are also the ones which allow for something like surveillance to exist. Furthermore, the actors in charge of defining the protocols and rules of the Internet communication can also be criticized for representing specific interests. (2005, pp. 575-576)

Frameworks such as articulation theory, actor-network theory, and others that approach the socio-political as conjuncturally determined provide a rich means of

understanding the way in which social and technical architectures, codes, and protocols structure and are structured by the emergence of networked digital computing, and are complicit in strengthening or weakening particular cultural and social values as well.

Cory Doctorow points to the way in which privacy articulates technology advances in networked computing to political and corporate interests of power in his 2008 speech to the American Library Association conference, entitled "Privacy: Is it time for a Revolution?"

> One of the kinds of laws we write is code—software code—when we build networked societies and systems, we end up evolving the political systems that will come out of them; they're interrelated and one grows out of the other naturally…So really when we start talking about a society in which people no longer get to choose the circumstances under which we disclose our information, we're talking about a society in which we all end up living under the thumb of a politburo, whether or not that's a politburo that's embodied by faceless bureaucrats or simply as the outgrowth of our technology, it's not a society that I think we should want to live in.

Technical systems which fail to acknowledge the importance of individual privacy, he concludes, cannot fail to produce political systems in which privacy is simply obviated as well. In the same vein, Bruce Schneier (2013), security expert and fellow at Harvard's Berkman Center for Society and the Internet has called publicly for the political intervention of expert praxis by engineers whom he urges to engage politically with the digital architecture by both monitoring and disclosing when they are called to act unethically by corporations or governments. "If you work with classified data and are truly brave, expose what you know. We need whistleblowers…There's safety in numbers, and this form of civil disobedience is the moral thing to do." He also exhorts engineers to promote open source designs which are less likely to be surreptitiously hacked by the government. "We need to demand that real technologists be involved in any key government decision making on these issues. We've had enough of lawyers and politicians not fully understanding technology; we need technologists at the table when we build tech policy." Of course the slight but necessary modulation of Schneier's important observation here is that technologists must enter into dialogue with those who make policy and law in a spirit of negotiation. Each perspective must inform the other. Both engineers and politicians must come to understand the ethical, moral, social, political, and cultural dimensions that in our contemporary moment have contributed to the emergence of the namespace.

5.6 Cultural Studies

Suggesting the articulation of a politically-active subordinate bloc constituted in and by experts who would leverage the diverse disciplinary knowledges, theoretical and methodological frameworks of the complementary fields of its members is nothing revolutionary. In fact it represents the historical impetus and the continuing promise of the field of cultural studies. Cultural studies has, since it's inception, been a critical project, navigating between the academy and society at large. Cultural studies is defined by its ethical commitment to make social and political change. It recognizes the opportunity to resource its work from within the 'elite' academy. However, because cultural processes do not map easily or perfectly onto methods of academic inquiry, for cultural studies theorists any critical project "has to be out, and away and into more dangerous places!" (Johnson, 1986, p. 43). Cultural studies negotiates these two demands through the productive tension between the interdisciplinary and counter-disciplinary impulses which define it. Cultural studies understands the conjuncture as the level at which the production of concrete knowledge is best employed for political struggle and change (Grossberg, 2010). This necessitates an interdisciplinary approach in the continual questioning of which objects are most relevant to study and which tools most effective for studying them. The theory of articulation is used to make that critical selection from an impossibly large and complex socio-historical context. No single discipline can profess the adequate tools and scope to map the diverse and heterogeneous elements that articulate to form a complex conjuncture such as the namespace. Cultural studies' methodological toolkit must be inter-disciplinary enough to borrow, responsibly and with due respect to carefully policed institutional and disciplinary boundaries, those theories, methods, and practices with which it can best make a study of particular phenomena in their relevant contexts.

Cultural studies must also be counter-disciplinary if it hopes to resist the canonical and curricular reification that accompanies institutionalization, allowing itself to remain flexible and viable as a practice by articulating to institutions and organizations outside the traditional structure of academia. In this way it hopes to remain "critical" and deeply committed to an examination of political, economic, social, and cultural flows of power articulated to *any* social or institutional structure, text, event, or cultural phenomenon it chooses to study. Lawrence Lessig's widely cited *Code: And Other Laws of Cyberspace 2.0* (Lessig, 2006) represents a strong example of conjuncturally-oriented, interdisciplinary work that understands the deeply imbricated nature of culture, technology, law, and politics. In *Code*, Lessig describes the way in which cybernetic architectures and protocols (metonymically, "code") are bound to the architecture of social design. Codes and protocols may be designed in ways that empower users by, for example, protecting informational and decisional privacy; they may also be designed, he warns, in ways that promote regimes

of surveillance and control by, for example, enforcing regimes of strict identification and a security culture of authorization. The latter road leads toward the namespace.

Contemporary legal scholar Julie Cohen, whose interdisciplinary work on privacy draws from several fields (among them cultural studies), describes the challenge and reward of such interdisciplinarity:

> We need to ask about the properties of the field and the properties of [the subject] and that requires insights from disciplines that law often doesn't pay attention to because they seem messy and alien, like cultural studies, science, technology, and society, [and] surveillance studies—they have 'strange' terminology, 'weird' jargon, 'no numbers', 'everything's a moving target'…so some work is required there, and it can be somewhat of a drag. But simple analytical framing is only a virtue if you're talking about something simple. So, I think we need to learn a new language to do information law and policy the right way.

With its focus on social flows of power, and its impulse to discover and deploy those frameworks and tools best suited to addressing the problematics of particular conjunctures, cultural studies and other interdisciplinary models of scholarship, offer us a powerful model of the intellectual networking that must happen across diverse fields if we are open to informed debate with those in the dominant bloc about the importance of privacy.

Because of its focus on conjunctures and social formations, the field of cultural studies provides a useful orientation for mapping outward to more global articulations and conjunctures. While the scope of this project limits my mapping, centering it on the articulation of American forces, phenomena, law, technology, etc., the burgeoning influence of globalism on economic, political, and technological realities demonstrate that concerns over privacy are far more global scope than I have been able to represent here. For example, I have not had space to explore the particular economic dimensions of the problematic, such as the commodity chain that articulates repressive foreign regimes to the U.S. surveillance technology companies that create and/or sell surveillance systems. Frameworks such as articulation thus allow us to imagine problematics like privacy as more complex than simply matters of law, business, or technology alone. As Nissenbaum and Solove both rightly point out, we must approach privacy contextually, in terms of concrete 'privacy problems'. I want to suggest, however, that this may ultimately mean moving beyond a focus on singular surveillance technologies and practices, toward a focus on the larger articulations and conjunctures to which these are undeniably linked.

While addressing the ways in which the TSA's policies of airport screening violate personal privacy is important, it should *found* a mapping work which prepares us to answer questions about intra- and international problematics. For example, how are the changes argued by the U.S. as necessary to rebalance security and privacy articulated to its role as a world police authority? How have U.S. policies perhaps promoted a global political climate in which terrorism becomes a political strategy against which it must continually contend? Questions about the problematic of privacy and the emergence of the namespace have, then, far larger reach than the question of whether U.S. intelligence agencies surveil individuals' email metadata in the war on terror. They are sizable political questions about national security and global geo-politics, such as what it means to abandon perpetual ground war for an inevitable perpetual cyber-war, hinted at in Obama's Presidential Policy Directive 20, in which are outlined "Offensive Cyber Effects Operations (OCEO)" which "offer unique and unconventional capabilities to advance US national objectives around the world with little or no warning…and with potential effects ranging from subtle to severely damaging" (Greenwald & MacAskill, 2013, para. 2). The problematic of privacy thus engenders for me the question of whether it is possible to imagine, let alone engineer, a world in which we're not in a technological arms race, a future which doesn't resemble a human face being stamped on by a boot.

References

Ackerman, S. (2013, September 13). FISA judge: Snowden's NSA disclosures triggered important spying debate. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/sep/13/edward-snowden-nsa-disclosures-judge

Acquisti, A., & Gross, R. (2009). Predicting Social Security numbers from public data. *Proceedings of the National Academy of Sciences, 106*(27), 10975–10980.

Alderman, E., & Kennedy, C. (1997). *The right to privacy.* New York: Vintage Books.

Allen, A. L. (1988). *Uneasy access: Privacy for women in a free society.* New Jersey: Rowman & Littlefield.

Althusser, L. (2005). *For Marx* (B. Brewster, Trans.). New York: Verso. (Original work published in English in 1969)

Andrejevic, M. (2002). The work of being watched: Interactive media and the exploitation of self-disclosure. *Critical Studies in Media Communication*, *19*(2), 230-248.

Arendt, H. (1998). *The human condition.* Chicago: University of Chicago Press. (Originally published in 1958).

Ash, T. G. (2013, June 27). If Big Brother came back, he'd be a public-private partnership. *The Guardian.* Retrieved from http://www.theguardian.com/commentisfree/2013/jun/27/big-brother-public-private-partnership-nsa

Assange, J. (2013, June 1). The banality of "Don't be evil." *The New York Times.* Retrieved from http://www.nytimes.com/2013/06/02/opinion/sunday/the-banality-of-googles-dont-be-evil.html

Bamford, J. (2012, March 15). The NSA is building the country's biggest spy center (watch what you say). *Wired.* Retrieved from http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/

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

Bauman, Z. (1998). On postmodern uses of sex. *Theory, Culture & Society, 15*(3), 19–33.

Bentham, J. (2011). *The panopticon writings* (M. Bozovic, Ed.). New York: Verso. (Original work published in English in 1791)

Bessie, A. (2010, December 5). Privacy is passe, so broadcast yourself (to Big Brother). *Truthout.* Retrieved from http://www.truthout.org/archive/item/93164-privacy-is-passe-so-broadcast-yourself-to-big-brother

Boyne, R. (2000). Post-panopticism. *Economy and Society, 29*(2), 285–307.

Brauch, H. G. (2011). Security threats, challenges, vulnerabilities and risks in US national security documents (1990–2010). *Coping with Global Environmental Change, Disasters and Security* (pp. 249–274). Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-17776-7_12

Butler, K. (2013, July 26). Obama promises disappear from transparency website. *UPI.* Retrieved from http://www.upi.com/Odd_News/Blog/2013/07/26/Obama-transparency-promises-disappear-from-transparency-website/4791374863492/

Calderone, M., & Froomkin, D. (2012, May 18). "Reporter's privilege" under fire from Obama administration amid broader war on leaks. *Huffington Post.* Retrieved from http://www.huffingtonpost.com/2012/05/18/reporters-privilege-obama-war-leaks-new-york-times_n_1527748.html

Campanelli, M. (2006, December 8). FTC launches redress program for ChoicePoint identity theft victims. *Direct Marketing News.* Retrieved from http://www.dmnews.com/ftc-launches-redress-program-for-choicepoint-identity-theft-victims/article/93773/

Carby, H. V. (2009). *Race men.* Boston: Harvard UP.

Cashmore, P. (2009, October 28). Privacy is dead, and social media holds the smoking gun. *CNN.* Retrieved from http://www.cnn.com/2009/OPINION/10/28/cashmore.online.privacy

Cashmore, P. (2012, January 23). Why 2012, despite privacy fears, isn't like Orwell's *1984. CNN.* Retrieved from http://www.cnn.com/2012/01/23/tech/social-media/web-1984-orwell-cashmore/index.html

Chen, K.-H., & Morley, D. (1996). *Stuart Hall: Critical dialogues in cultural studies.* New York: Routledge.

Chomsky, N. (2002). *Media control: The spectacular achievements of propaganda.* New York: Seven Stories Press.

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM, 31*(5), 498–512.

Clifton, B. (2012, October 4).Privacy, web analytics, Google and ketchup. *Measuring Success.* Retrieved from http://www.advanced-web-metrics.com/blog/2012/10/04/privacy-web-analytics-google-and-ketchup/

Clinton, H.R. (2010, January 21). Remarks on internet freedom. *The Newseum.* Retrieved from http://www.state.gov/secretary/rm/2010/01/135519.htm

Cohen, J. & Balz, D. (2013, July 23). Poll: Privacy concerns rise after NSA leaks. *The Washington Post.* Retrieved from http://articles.washingtonpost.com/2013-07-23/politics/40862490_1_edward-snowden-nsa-programs-privacy

Conti, G. (2008). *Googling security: How much does Google know about you?* Boston: Pearson Education.

Cooley, T. M. (1888). *A treatise on the law of torts or the wrongs which arise independent of contract.* Chicago: Callaghan & Co.

Coppola, F. F. (Director), & Coppola, F. F. (Producer). (1974). *The conversation* [Motion picture]. United States: American Zoetrope.

Couric, K. (2007, October 8). Notebook: Google and privacy. *CBS News.* Retrieved from http://www.cbsnews.com/video/watch/?id=2916062n&tag=api

Cowan, A. L. (2006, May 31). Four librarians finally break silence in records case. *The New York Times.* Retrieved from http://www.nytimes.com/2006/05/31/nyregion/31library.html?_r=0

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

Deleuze, G. (1997). *Negotiations: 1972-1990.* (M. Joughin, Trans.). Columbia UP.

Dice, M. (2011). *Big Brother: The Orwellian nightmare come true.* San Diego: The Resistance.

Dish, T. D. (2010, November 9). The big lie. *The Atlantic.* Retrieved from http://www.theatlantic.com/daily-dish/archive/2010/11/the-big-lie/180117/

DNI statement on recent unauthorized disclosures of classified information. (2013, June 6). *Director of National Intelligence* [website]. Retrieved from http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information

Domestic surveillance reform, senator Ron Wyden. (2013, September 25). [Press Conference]. Retrieved from http://www.wyden.senate.gov/news/video-and-audio/view/domestic-surveillance-reform-press-conference

Ecuador's Correa: Obama's exceptionalism talk reminiscent of Nazi rhetoric before WWII. (2013, October 6). *RT.* Retrieved from http://rt.com/news/correa-us-exceptionalism-dangerous-748/

EFF's case against AT&T. (n.d.). Electronic Frontier Foundation. Retrieved from https://www.eff.org/nsa/hepting

Elgin, B. (2011, December 13). Fresh air: The technology helping repressive regimes spy. *NPR.* Retrieved from http://www.npr.org/2011/12/14/143639670/the-technology-helping-repressive-regimes-spy

Estes, A.C. (2013, August 8). Edward Snowden's email provider shut down rather than comply with feds. *Gizmodo.* Retrieved from http://gizmodo.com/somebody-read-government-goons-shut-down-edward-snow-1070103469

Facebook IPO: Worth the price or next Internet bubble? NPR. (2012, January 30). *NPR.* Retrieved from http://www.npr.org/blogs/alltechconsidered/2012/01/31/146093231/facebook-ipo-worth-the-price-or-next-internet-bubble

Federal Trade Commission. (2010). Protecting consumer privacy in an era of rapid change—A proposed framework for businesses and policymakers. *Journal of Privacy and Confidentiality, 3*(1), 5. Retrieved from http://repository.cmu.edu/cgi/viewcontent.cgi?article=1068&context=jpc

Finding value in the growing online advertising industry. (2013, April 3). *MarketWatch.* Retrieved from http://www.marketwatch.com/story/finding-value-in-the-growing-online-advertising-industry-2013-04-03

Fine, G. A. (2010). Unclassified report on the president's surveillance program. Diane Publishing. Retrieved from https://www.fas.org/irp/eprint/psp.pdf

Foucault, M. (1995). *Discipline and punish : the birth of the prison* (2nd Vintage Books ed.). New York: Vintage Books. (Original work published in French in 1975)

Frau-Meigs, D. (2010). From secrecy 1.0 to privacy 2.0: Who controls what? *Revue française d'études américaines, 1*(123), 79–95.

Froomkin, D. (2005, November 7). Cheney's "dark side" is showing. *The Washington Post.* Retrieved from http://www.washington post.com/wp-dyn/content/blog/2005/11/07/BL2005110700793.html

Gahran, A. (2013, November 18). Courts drawing line against warrantless phone data searches? *CNN.* Retrieved from http://www.cnn.com/2010/TECH/mobile/12/02/location. privacy.gahran/

Gaming Excellence's best of E3 2012. (2012, June 19). *Gaming Excellence.* Retrieved from http://www.gamingexcellence.com/features/gamingexcellences-best-of-e3-2012

Gaudiosi, J. (2012, July 18). New reports forecast global video game industry will reach $82 billion by 2017. *Forbes.* Retrieved from http://www.forbes.com/sites/johngaudiosi/2012/07/18/new-reports-forecasts-global-video-game-industry-will-reach-82-billion-by-2017/

Gellman, B., & Soltani, A. (2013, November 1). 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_2.html

Gerlach, N., Hamilton, S. N., Sullivan, R., & Walton, P. L. (2011). *Becoming biosubjects: Bodies, systems, technologies.* Toronto: University of Toronto Press.

Geron, T. (2013, September 11). Mark Zuckerberg: U.S. government "blew it" on NSA issue. *Forbes.* Retrieved from http://www.forbes.com/sites/tomiogeron/2013/09/11/live-mark-zuckerberg-speaks-at-techcrunch-disrupt/

Gerzema, J., & D'Antonio, M. (2010). *Spend shift: How the post-crisis values revolution is changing the way we buy, sell, and live.* San Francisco: Wiley & Sons.

Gewirtz, D. (2013, August 13). The truth about why Silent Circle silenced their secure email service. ZDNet Government. Retrieved on November 18th, 2013 from http://www.zdnet.com/the-truth-about-why-silent-circle-silenced-their-secure-email-service-7000019300/

Gibney, A. (2013). *We steal secrets: The story of WikiLeaks* [Documentary]. United States: Focus World.

Glaser, M. (2011, February 10). 5 across: Online privacy and the 'do not track' debate. *PBS.* Retrieved from

http://www.pbs.org/mediashift/2011/02/5across-online-privacy-and-the-do-not-track-debate041/

Glenn Greenwald honorific speech for Edward Snowden. (2013, August 31). *RT.* Retrieved from http://www.youtube.com/watch?v=EPhghCkwk0E&feature=youtube_gdata_player

Goetz, T. (2011, June 19). Harnessing the power of feedback loops. *Wired.* Retrieved from http://www.wired.com/magazine/2011/06/ff_feedbackloop/

Gramsci, A. (1971). *Selections from the prison notebooks.* In Q. Hoare & G. N. Smith (Eds.). New York: International Publishers. (Original work published in Italian in 1934)

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

Greenwald, G., MacAskill, E., & Poitras, L. (2013, June 9). Edward Snowden: the whistleblower behind the NSA surveillance revelations. *The Guardian.* Retrieved from http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Griswold v. Connecticut, 381 U.S. 479 (1965).

Grossberg, L. (2010). *Cultural Studies in the future tense.* Durham: Duke UP.

Hagel, J., & Rayport, J. F. (1997). The coming battle for customer information. *McKinsey Quarterly,* 64-77.

Hall, S., Critcher, C., Jefferson, T., Clarke, J. N., & Roberts, B. (1978). *Policing the crisis: Mugging, the state, and law and order.* London: Macmillan.

Halliday, J. (2010, October 20). Google Street View broke Canada's privacy law with wi-fi capture. *The Guardian.* Retrieved from http://www.theguardian.com/technology/2010/oct/19/google-street-view-privacy-canada

Harris, S. (2010). *The watchers: The rise of America's surveillance state.* London: Penguin Books.

Harris, S. (2012, December 8). The watchers: The rise of America's surveillance state [Public Lecture.] *Cato Institute.* Retrieved from http://www.cato.org/events/watchers-rise-americas-surveillance-state

Hay, C. (2001). State theory. In Jones, R. J. B. (Ed.) *Routledge encyclopedia of international political economy: Entries P-Z.* New York: Taylor and Francis.

Hepting v. AT&T. 439 F. Supp. 2d (2006).

Horvitz, S., Asokan, S., & Tate, J. (2011, December 1). Trade in surveillance technology raises worries. *The Washington Post.* Retrieved from http://articles.washingtonpost .com/2011-12-01/world/35286192_1_surveillance-technology-first-trade-show-products

Industry facts. Entertainment Software Association. (n.d.). Retrieved from http://www.theesa.com/facts/

Information awareness office. (n.d.). *Wikipedia.* Retrieved from http://en.wikipedia.org/wiki/Information_Awareness_Office

Jarvis, J. (2009). What would Google do? Reverse-engineering the fastest growing company in the history of the world. New York: HarperCollins.

Jarvis, J. (2011a). *Public parts: How sharing in the digital age improves the way we work and live.* New York: Simon & Schuster.

Jarvis, J. (2011b, February 3). Your life torn open, essay three: Get over it. *Wired.* Retrieved from http://www.wired.co.uk/magazine/archive/2011/03/features/get-over-it

Jenkins, Jr., H. W. (2010, August 14). Google and the search for the future. *The Wall Street Journal.* Retrieved from http://online.wsj.com/news/articles/SB10001424052748704901104575423294099527212

Johnson, R. (1986). What is cultural studies anyway? *Social Text* (16), 38-80.

Jones, P. (2008, May 7). Forced exposure. *Groklaw* [Blog comment]. Retrieved from http://www.groklaw.net/article.php?story=20130818120421175

Jones, S. (2006). *Antonio Gramsci.* New York: Taylor & Francis.

Kalil, T. (2012, March 29). Big Data is a big deal. *Whitehouse.gov.* Retrieved from http://www.whitehouse.gov/blog/2012/03/29/big-data-big-deal

Katz v. United States, 389 U.S. 347 (1967).

Kelly, M. (2012, January 27). Google responds to privacy policy criticisms. *VentureBeat*. Retrieved from http://venturebeat.com/2012/01/27/google-privacy-policy-response

King, Jr., N., & Ballhaus, R. (2013, July 24). Approval of Obama, Congress falls in new poll. Retrieved from http://online.wsj.com/news/articles/SB10001424127887324144304578624112569717272

Kirn, W. (2010, October 15). Little Brother is watching. *The New York Times.* Retrieved from http://www.nytimes.com/2010/10/17/magazine/17FOB-WWLN-t.html

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences, 110*(15), 5802–5805.

Kravets, D. (2011, October 26). Patriot Act turns 10, with no signs of retirement. *Wired.* Retrieved from http://www.wired.com/threat level/2011/10/patriot-act-turns-ten/

Lake, E. (2011, September 8). Perpetual security state. *The Washington Times.* Retrieved from http://www.washingtontimes.com/news/2011/sep/8/perpetual-security-state/

Lakoff, G. (1996). *Moral politics: What conservatives know that liberals don't.* Chicago: University of Chicago Press.

Lane, F. S. (2011). *American privacy: The 400-year history of our most contested right.* Boston: Beacon Press.

Langenderfer, J., & Miyazaki, A. D. (2009). Privacy in the information economy. *Journal of Consumer Affairs, 43*(3), 380-388.

Langlois, G. (2005). Networks and layers: Technocultural encodings of the World Wide Web. *Canadian Journal of Communication, 30*(4), 565-583.

Lenz, T. O. (1997, Midsummer). "Rights talk" about privacy in state courts. *Albany Law Review, 60*(5), 1613-1631. Retrieved from http://go.galegroup.com/ps/i.do?id=GALE%7CA20442016&v=2.1&u=lom_mtu&it=r&p=AONE&sw=w&asid=97dfde6a056ecf15a737876efd3ccb7a

Luke, T. W. (2002). Power and political culture. In L. A. Lievrouw, & Livingstone, S. (Eds.), *Handbook of new media* (pp. 518–552). London: Sage.

Lessig, L. (2006). *Code v. 2.0: Code and other laws of cyberspace.* New York: Perseus Books.

Lyon, D. (2006). *Theorizing surveillance: The panopticon and beyond.* Portland: Willan Publishers.

Lyon, D. (2013). *The electronic eye: The rise of surveillance society.* Minneapolis: University of Minnesota Press.

Marmura, S. M. E. (2010). *Hegemony in the digital age: The Arab/Israeli conflict online.* Lexington: Lexington Books.

Marx, K. (1904). *A contribution to the critique of political economy.* Charles H. Kerr. (Original work published in German in 1859)

McGrath, J. E. (2004). *Loving Big Brother: Performance, privacy and surveillance space.* New York: Routledge.

McLaughlin, B. (2011). *What is HTML5?* O'Reilly. [Kindle Reader Version]. Retrieved from http://shop.oreilly.com/product/0636920021049.do

Miga, A. (2007, April 12) Librarian who resisted FBI says Patriot Act invades privacy. *The Washington Post.* Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2007/04/11/AR2007041102041.html

Miller, A. R. (1967, November). The national data center and personal privacy. *Atlantic*, 53-57.

Montalbano, E. (2010, November 18). U.S. warns of "huge" cyber threats. *InformationWeek.* Retrieved from http://www.informationweek.com/government/security/us-warns-of-huge-cyber-threats/228300167

Monten, J. (2005). The roots of the Bush doctrine: Power, nationalism, and democracy promotion in U.S. strategy. *International Security, 29*(4), 112–156.

More in sorrow than anger. (2013, September 18). *The Economist.* Retrieved November 20, 2013, from

http://www.economist.com/blogs/americasview/2013/09/brazil-and-united-states

Morin, J. (2013). *Watch Dogs* Interview with creative director Jonathan Morin on systemic subversion. *Dealspwn.* Retrieved from http://www.youtube.com/watch?v=qo7me0VT6nw&feature=youtube_gdata_player

Morville, P. (2005). *Ambient findability.* Sebastopol: O'Reilly Media.

Moyer, E. (2013, September 12). NSA disguised itself as Google to spy, say reports. *CNET News.* Retrieved from http://news.cnet.com/8301-13578_3-57602701-38/nsa-disguised-itself-as-google-to-spy-say-reports/

Narus Solutions: Cybersecurity technology for a dynamic world. (2003). *Narus.com.* Retrieved from http://www.narus.com/solutions/narus-solutions-overview

Naughton, J. (2013, September 15). After Edward Snowden's revelations, why trust US cloud providers? *The Guardian.* Retrieved from http://www.theguardian.com/technology/2013/sep/15/edward-snowden-nsa-cloud-computing

Negroponte, N. (1995). *Being digital.* New York: Vintage Books.

New York Times Editorial Board. (2013, June 6). President Obama's dragnet. *The New York Times.* Retrieved from http://www.nytimes.com/2013/06/07/opinion/president-obamas-dragnet.html

Nissenbaum, H. F. (2010). *Privacy in context: Technology, policy, and the integrity of social life.* Stanford: Stanford Law Books.

Nitrozac and Snaggy. (2009). Big Zucker is watching. *Joy of Tech.* Retrieved from http://www.joyoftech.com/joyoftech/joyarchives/1330.html

NSA spying on Americans is illegal. (n.d.). *NSAWatch.* Retrieved from http://www.nsawatch.org/nsa-illegal.html

NSA spying. (n.d.). *Electronic Frontier Foundation.* Retrieved from https://www.eff.org/nsa-spying

O'Reilly, T. (2005, October 1). Web 2.0: Compact definition? [Blog post]. Retrieved from http://radar.oreilly.com/2005/10/web-20-compact-definition.html

Obama, B. (2007, July 1). Renewing American leadership. *Foreign Affairs.* Retrieved from http://www.foreignaffairs.com/articles/62636/barack-obama/renewing-american-leadership

Obama, B. (2013, June 16). President Barack Obama [Interview by C. Rose]. Retrieved November 20, 2013, from http://www.charlierose.com/watch/60230424

Obama's remarks on NSA controversy. (2013, June 7). *WSJ Blogs: Washington Wire.* Retrieved from http://blogs.wsj.com/washwire/2013/06/07/transcript-what-obama-said-on-nsa-controversy/

Orwell, G. (1992). *Nineteen eighty-four.* London: Random House. (Original work published in English in 1949)

Palis, C. (2012, May 3). Facebook privacy options ignored by millions of users. *Huffington Post.* Retrieved from http://www.huffingtonpost.com/2012/05/03/facebook-privacy-consumer-reports_n_1473920.html

Pilgrim, M. (2010). *HTML5: Up and running.* Sebastopol: O'Reilly.

President Obama holds a press conference. (2013, August 9). *Whitehouse.gov.* Retrieved from http://www.whitehouse.gov/photos-and-video/video/2013/08/09/president-obama-holds-press-conference

Prosser, W. L. (1960). Privacy. *California Law Review,* 48, 383-423.

Reitman, R. (2012, December 6). Deep dive: Updating the Electronic Communications Privacy Act. *Electronic Frontier Foundation.* Retrieved from https://www.eff.org/deeplinks/2012/12/deep-dive-updating-electronic-communications-privacy-act

Remarks by the President at the National Defense University. (2013, May 23). *WhiteHouse.gov.* Retrieved from http://www.whitehouse.gov/the-press-office/2013/05/23/remarks-president-national-defense-university

Resmini, A., & Rosati, L. (2011). *Pervasive information architecture: Designing cross-channel user experiences.* Burlington: Morgan Kaufmann.

Riley, C. (2013, June 12). Sales of Orwell's *1984* spike after NSA leak. *CNN Money.* Retrieved from http://money.cnn.com/2013/06/12/news/1984-nsa-snowden/index.html

Risen, J., & Lichtblau, E. (2005, December 16). Bush lets U.S. spy on callers without courts. *The New York Times.* Retrieved from http://www.nytimes.com/2005/12/16/politics/16program.html

Roberts, D. (2013 June 28). Senators accuse government of using "secret law" to collect Americans' data. *The Guardian.* Retrieved from http://www.theguardian.com/world/2013/jun/28/senators-james-clapper-nsa-data-collection

Roe v. Wade, 410 U.S. 113 (1973).

Roose, K. (2013, July 29). The surveillance-free day: Part 1. *New York Magazine.* Retrieved from http://nymag.com/daily/intelligencer/2013/07/surveillance-free-day-part-i.html

Roose, K. (2013, July 29). The surveillance-free day: Part 2. *New York Magazine.* Retrieved from http://nymag.com/daily/intelligencer/2013/07/surveillance-free-day-part-ii.html

Rosen, J. (2010, July 21). The Web means the end of forgetting. *The New York Times.* Retrieved from http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html

Rotenberg, M. (2012, January 10). I know who you are and I saw what you did: Social networks and the death of privacy. *The Diane Rehm Show*. Retrieved from http://thedianerehmshow.org/shows/2012-01-10/i-know-who-you-are-and-i-saw-what-you-did-social-networks-and-death-privacy

Rothke, B. (2011, July 8). Definitive text on the topic [Comment/Review]. *Amazon.com.* Retrieved from http://www.amazon.com /Surveillance-Security-Risks-Wiretapping-Technologies-ebook/dp/B005ILKE0W/ref=sr_1_1?s=books&ie=UTF8&qid=1384803965&sr=1-1&keywords=surveillance+or+security

Rule, J. B. (2007). *Privacy in peril: How we are sacrificing a fundamental right in exchange for security and convenience.* Oxford: Oxford UP.

Schell, J. (2010, July 27). Visions of the gamepocalypse. *The Long Now Foundation*. Retrieved from http://longnow.org/seminars/02010/jul/27/visions-gamepocalypse

Schmidt, E., & Cohen, J. (2013). *The new digital age: Reshaping the future of people, nations and business. New* York: Alfred A. Knopf.

Schneier, B. (2013 September 5). The US government has betrayed the internet: We need to take it back. *The Guardian.* Retrieved from http://www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-internet-nsa-spying

Scott, T. (Director), & Bruckheimer, J. (Producer). (1998). *Enemy of the state* [Motion picture]. United States: Touchstone Pictures.

Searching for Mark Pilgrim. (2011, October 4). Thoughts from Eric. *Meyerweb.com.* Retrieved December 15, 2013, from http://meyerweb.com/eric/thoughts/2011/10/04/searching-for-mark-pilgrim/

Slack, J. D. (1984). *Communication technologies and society : Conceptions of causality and the politics of technological intervention.* Norwood: Ablex Publishing Corporation.

Slack, J. D., & Wise, J. M. (2005). *Culture + technology: A primer.* New York: Peter Lang.

Smith, Z. (2010, November 25). Generation why? *The New York Review of Books.* Retrieved from http://www.nybooks.com/articles/archives/2010/nov/25/generation-why/

Solove, D. J. (2008). *Understanding privacy.* Boston: Harvard UP.

Solove, D. J., Rotenberg, M., & Schwartz, P. M. (2006). *Privacy, information and technology.* Aspen: Aspen Publishers Online.

Sorkin, A. (Writer), & Director, B. D'Elia (Director). (1999, November 24). The short list [Television series episode]. In K. Harms (Producer), *The West Wing.* Los Angeles, CA: Warner Bros. Television.

Sperber, E. (2013, August 9). The Californian ideology becomes hegemonic. *CounterPunch.* Retrieved from http://www.counterpunch.org/2013/08/09/the-californian-ideology-becomes-hegemonic/

Spielberg, S. (Director), Curtis, B., de Bont, J., Molen, G.R. & Parkes, W. F. (Producers) (2002) *Minority report* [Motion Picture]. United States: Twentieth Century Fox.

Sprenger, P. Sun on privacy: Get over it. (1999, January 26). *Wired.* Retrieved from http://www.wired.com/politics/law/news/1999/01/17538

Steel, E., & Fowler, G. A. (2010, October 18). Facebook in privacy breach. *The Wall Street Journal.* Retrieved from http://online.wsj.com/news/articles/SB10001424052702304772804575558484075236968

Steeves, V. (2008). If the Supreme Court were on Facebook: Evaluating the reasonable expectation of privacy test from a social perspective. *Canadian Journal of Criminology and Criminal Justice 50*(3), 331-347.

Stolberg, S. G. (2006, December 24). The decider. *The New York Times.* Retrieved from http://www.nytimes.com/2006/12/24/weekinreview/24stolberg.html

Talbot, D. (2013, September 23). Bruce Schneier discusses the NSA documents. *MIT Technology Review.* Retrieved from http://www.technologyreview.com/news/519336/bruce-schneier-nsa-spying-is-making-us-less-safe/

Telecom firms under spying scrutiny. (2013, November 5). *BBC.* Retrieved from http://www.bbc.co.uk/news/technology-24819116

The national security strategy of the United States of America. (2009). Morgan James Publishers.

Thompson, D. (2010, October 1). Google's CEO: "The laws are written by lobbyists." *The Atlantic.* Retrieved from

http://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/

Tsotsis, A. (2010, September 7). Eric Schmidt: We know where you are, we know what you like. *TechCrunch.* Retrieved from http://techcrunch.com/2010/09/07/eric-schmidt-ifa/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Techcrunch+%28TechCrunch%29&utm_content=Google+Reader

Ungar, R. (2013, June 12). GOP rep. Peter King blows away the First Amendment to catch the bad guys. *Forbes.* Retrieved from http://www.forbes.com/sites/rickungar/2013/06/12/gop-rep-peter-king-blows-away-the-first-amendment-to-catch-the-bad-guys/2/

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107 –56. 115 Stat. 272 (2001). Retrieved from http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

Universal-McCann. (2012). *Wave 6: The business of social.* Retrieved from http://universalmccann.com.au/global/knowledge/view?Id=226

Vaidhyanathan, S. (2008). Naked in the nonopticon. *Chronicle Review, 54*(23), 7–10.

Valentino-Devries, J. (2010, July 31). What they know about you. *The Wall Street Journal.* Retrieved from

http://online.wsj.com/news/articles/SB10001424052748703999304575399041849931612

Wacks, R. (2010). *Privacy: A very short introduction.* Cambridge: Oxford UP.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220.

Watch Dogs. (2013). [XBOX software]. Montreal, Canada: Ubisoft Montreal.

Westin, A. F. (1967). *Privacy and freedom.* New York: Athenum.

Wheaton, S., Kim, A., & Cascarano, C. (2013, June 7). Obama on surveillance, then and now. Retrieved from http://www.nytimes.com/interactive/2013/06/08/us/politics/08obama-surveillance-history-video.html?_r=1&

Williams, R. (2001). *The long revolution.* Letchworth, Herts: Broadview Press. (Original work published in English in 1961)

Williams, R. (2011). *Keywords: A vocabulary of culture and society.* New York: Routledge.

Williamson, V., Skocpol, T., & Coggin, J. (2011). The Tea Party and the remaking of republican conservatism. Cambridge: Oxford UP.

Wyden, R. (2013, July 23). Remarks on the NSA's domestic surveillance programs at the Center for American Progress. *Whatthefolly.com* [transcript]. Retrieved from http://www.whatthefolly.com/2013/08/12/transcript-sen-ron-wydens-

remarks-on-the-nsas-domestic-surveillance-programs-at-the-center-for-american-progress-on-july-23-2013/

Wyden, R., Guthrie, C., Dickas, J., & Perkins, A. (2006). Law and policy efforts to balance security, privacy and civil liberties in post-9/11. *American Standard Law & Policy Review,* 17, 331. Retrieved from http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/stanlp17&section=21

Zamiatin, E. I. (1983). *We* (M. Ginsburg, Trans.). New York: Avon. (Original work published in Russian in 1924)

Appendix A

I have not used images, tables or charts, nor any intellectual property which I do not own or did not create. I have reviewed my dissertation thoroughly and all the references I include are allowed under the fair use clause under U.S. copyright law.