Transparent Lives and the Surveillance State: Policing, New Visibility, and Information Policy

Bryce Clayton Newell

A dissertation
submitted in partial fulfillment of the
requirements for the degree of

Doctor of Philosophy

University of Washington
2015

Reading Committee:
Adam D. Moore, Chair
Batya Friedman
Ryan Calo
Steve Herbert
Ricardo Gomez

Program Authorized to Offer Degree:
The Information School

University of Washington

Abstract

Transparent Lives and the Surveillance State: Policing, New Visibility, and Information Policy

Bryce Clayton Newell

Chair of the Supervisory Committee:
Adam D. Moore
The Information School

In this dissertation, I utilize conceptual and legal analyses to explore the tensions between personal information privacy and public access to information implicated by government surveillance and citizen-initiated inverse surveillance efforts designed to cast the gaze back at the government, and ask what implications these conclusions have for individual freedom (defined as the absence of domination). I focus on police use of body-worn cameras (BWCs) and automated license plate recognition (ALPR) technologies, on one hand, and citizen-initiated recordings of police officers and freedom of information (FOI) requests for data collected by police BWCs and ALPR systems, on the other. My analysis draws upon republican political theory, philosophical and legal theories of privacy and free speech, the concept of "policing's new visibility" (Goldsmith, 2010), and various other theories of surveillance and reciprocal/inverse surveillance within the surveillance studies literature. I conduct doctrinal and descriptive legal research into relevant privacy and disclosure laws applicable within

Washington State (USA); utilize legal and philosophical theories of privacy, freedom, and free speech to conduct an analysis of the values and value tensions implicated in these situations; and apply elements of Value Sensitive Design for similar conceptual and analytic purposes. Ultimately, I develop a theory of information policy that that accounts for tensions between personal information privacy rights and government disclosure of personally-identifiable information under state FOI law in Washington State, and I propose normative recommendations for improving law, public policy, and police department surveillance and disclosure policies related to these privacy and access concerns.

To Aprille

Thank you for your love and support during this process.

I am eternally grateful for who you are and for all you do for me and our family.

Acknowledgements

There have been many individuals who have impacted me and my work throughout the process of developing this dissertation, as well as to my larger project of becoming a scholar and educator. It is not possible to name and thank each of these individuals here (and I would likely inadvertently fail to include everyone who deserves to be in such a list), but I do want to specifically thank those individuals mentioned below:

My supervisor and Ph.D. committee chair, Adam D. Moore, for championing my application to the Ph.D. program and for continually challenging me to think more critically about the philosophical bases for—and my arguments regarding—privacy, free speech, and other rights and values that arise in and around my work, and for allowing me the space to follow my interests. The conceptual analysis and normative conclusions offered herein are much more defensible as a result.

Batya Friedman, for always being optimistic and positive about my research while also taking the time to give significant amounts of extremely valuable—and sometimes critical—feedback on my work as it developed. This work is much better because of her advice.

Ricardo Gomez, for the tremendous amount of time and effort he has expended to help me become a better researcher.

Steve Herbert, for always being willing to entertain questions and give helpful advice, and for always reminding me to consider the values associated with law enforcement and criminal justice that come into play in the context of my research.

Ryan Calo, for being willing to provide comments and feedback, and for pushing me to consider and integrate new areas of privacy scholarship—and questions about how these intersect—into my work.

Stephen Gardiner, for introducing me to the work of Philip Pettit and spending substantial time helping me to craft and refine my arguments around privacy through the lens of republican political theory.

I also want to acknowledge the following individuals for providing comments, suggestions, and advice on this work (and related papers) and in regards to my general pursuit to become an academic throughout these past years in graduate school: Anupam Chander, Rachel Cichowski, Floyd Feeney, Chris Heaney, Elizabeth Joh, Laura Lenhart, Alan Rubel, and Ingra Shellenberg, as well as the participants at the pre-conference workshop at the 2013 Information Ethics Roundtable and members of the Comparative Law and Society Studies (CLASS) Center at UW for all of their comments on earlier versions of parts of this project.

Thank you to Coke and Cindy Newell (my parents) for always supporting and encouraging me, and for starting me out in life in an environment that prioritized and emphasized the importance of education, expression, and creativity.

Thank you to Aprille Newell and our children, Annalesa, Caden, Aspen, and Oliver. I love each of you and am so incredibly grateful for your love and support—and for reminding me of what's really important in life each day when I come home from school or work.

And in memoriam of Keith Aoki, for being gracious and willing to supervise the development of my first published article while I was still a law student of his at UC Davis. That experience helped ignite my interest in scholarship and set me on the path that has led me to where I am today.

Table of Contents

1. Introduction

1.1. The nature and purpose of the study

The purpose of this dissertation is to explore the relationship between privacy and access to information implicated by government surveillance, citizen-initiated efforts to cast the gaze back at the government, and public record disclosure policies, and to ask what implications these conclusions have for individual freedom. More specifically, throughout this dissertation I focus on police use of body-worn cameras (BWCs) (Chapter 7) and automated license plate recognition (ALPR) technologies (Chapter 5), on one hand, and citizen-initiated recordings of police officers (Chapter 6) and freedom of information (FOI) requests for data collected by police BWCs and ALPR systems (Chapters 5 and 7), on the other. This exploration is necessarily tied to the concept of "new visibility" (Thompson, 2005) and the extension of that concept to "policing's new visibility" (Goldsmith, 2010), as well as various theories of surveillance and reciprocal/inverse surveillance within the surveillance studies literature. This examination also requires doctrinal legal analysis of relevant privacy and disclosure law, the utilization of legal and philosophical theories of privacy, freedom, and free speech, and an analysis of the values and value tensions implicated in these situations as well as the application of conceptual methodologies from Value Sensitive Design. By incorporating these various analytical methods, the proposed dissertation has been designed to allow me to develop a robust and defensible theory of information policy—one that that accounts for conflicts between personal information privacy rights and government disclosure of personally-identifiable information under state FOI law—and to propose normative recommendations for improving law, public policy, and police department surveillance and disclosure policies related to these privacy and access concerns.

Information policy, as defined by Braman (2011), "is comprised of laws, regulations, and doctrinal positions—and other decision making and practices with society-wide constitutive effects—involving information creation, processing, flows, access, and use." In line with this definition, this study's development of information policy will encompass the analysis of laws that regulate the collection/creation, use, and subsequent access to personal information generated through certain surveillance activities by the state (BWC and ALPR use) and its citizens (civilian video and FOI requests). With the aim of developing an original theory of information policy, the proposed dissertation will specifically examine how a neorepublican conception of freedom, of the type championed by Philip Pettit (1996; 1997; 2001; 2002; 2003; 2008; 2011; 2012) as the absence of the possibility of domination, can inform the way we think about the proper relationships between privacy, access, and security in public and private spaces, and to determine whether this neorepublican theory can adequately account for the legal and policy questions raised by the cases under consideration. My analysis will draw upon theoretical and empirical research in law, information science (including Value Sensitive Design), surveillance studies and criminology, and philosophy.

The proposed study is built around three real-life scenarios (the "cases") that demonstrate various forms of police and citizen visibility *vis-à-vis* each other:

Case 1 (chapter 5): The use of automated license plate reader (ALPR) technologies by law enforcement agencies and the resulting public disclosure of ALPR databases;

Case 2 (chapter 6): The role of civilian video and the right of citizens to record encounters with police officers (the so called "right to record"); and

Case 3 (chapter 7): Police use of body-worn cameras (BWCs) to document police-citizen interactions and the disclosure of the resulting footage under public records (FOI) laws.

The investigation of these cases will be restrained by jurisdictional criteria—specifically, to the experience and law applicable within Washington State (including federal and state constitutional law as well as state statutory and judicial case law related to privacy and public access to information). Washington State provides a particularly appropriate boundary for the cases because of a confluence of factors, including the breadth of the state's FOI law, provisions in the state's Privacy Act related to eavesdropping and regulating dash-camera camera use, and the fact that recent ALPR and body-camera footage disclosures within the state have raised questions about privacy versus disclosure into the public spotlight more than anywhere else in the country to date. Because the broad nature of Washington's Public Records Act and its recently confirmed precedence over state privacy law (see Fisher Broadcasting-Seattle TV LLC v. City of Seattle, 2014) has resulted in some unique and interesting consequences—including the release of largely un-redacted ALPR databases and BWC footage to members of the public—the Washington State experience is an ideal boundary within which to conduct an exploratory, descriptive, and policy-oriented *single-outcome study* of the three cases outlined above through the application of *within-case analysis*.[1] Additionally, the applicability of the Washington State's eavesdropping law, which requires all-party consent, to both citizen recordings and the use of BWCs as a means of limiting access to records, make those two phenomena relevant to the overall research project. To be sure, Washington is not alone in experiencing the ramifications of the adoption of ALPR and BWCs and with the proliferation of civilian video, but the conflicts between privacy and public disclosure have come to a head in Washington like in no other state to date. Additionally, focusing on Washington is particularly appropriate because it complements other empirical research I am currently conducting with two police departments in the state and, practically speaking, this restricted focus will enable me to provide more targeted normative recommendations to these agencies and to state lawmakers. However, this focus on Washington State (both the particulars of Washington law and the experiences that Washington agencies and residents have had with these issues) also limits the applicability of my specific findings to a broader set of cases or in other jurisdictions. Despite these limitations, I expect that my broader and generalized theoretical conclusions might have importance outside the confines of Washington itself.

---

[1] Gerring (2006) defines a single-outcome study as a case study design that is designed "to investigate a bounded unit in an attempt to elucidate a single outcome occurring within that unit" rather than the goal of discovering "something about a broader population of cases" (p. 707). A *within-case analysis* as part of the single-outcome study allows for the detailed explication of the case of special interest.

1.2. Overview of the problem

Civilian video, BWC video, and ALPR data can all be used to force transparency of police officer conduct, whether by providing audio-visual evidence of (mis)conduct or the ability to track and analyze officer movements over time. Ultimately, the interplay between the rights of citizens to record police in public/private spaces, police filming citizens on the streets and in their homes, and the visibility provided to both parties through analysis of information contained in ALPR databases, raise important questions about privacy, accountability, and transparency. When technology advances rapidly, law written in decades past often loses relevancy when applied to these newer developments. As surveillance methodologies become more sophisticated, less expensive, and mobile (wearable), states and individuals each have the power to collect increasingly large amounts of information about the activities of the other.

In the United States, the rights of citizens to document government action and access public records have a strong foundation in First Amendment principles, but states also have legitimate interests in collecting certain types of information to promote efficiency, public safety, and law enforcement. These interests are also regulated by constitutional law (e.g. the Fourth Amendment) and personal privacy interests, and often what personal information law and/or courts consider "public" or "private" is dependent on spatial and property-based considerations. As state surveillance continues to capture more and more potentially sensitive personal information about individual citizens (or non-citizen residents and others), broad FOI laws and other transparency initiatives may come into significant tension with individual privacy rights when they would require states to disclose sensitive personal information about individual citizens simply because the information happens to be included within a government record (see Solove, 2002).

Additionally, as police officers are outfitted with mobile surveillance devices, such as BWCs, which are not constrained by property or spatial limitations (i.e. they can be worn into private residences or anywhere else the officer chooses to be), the tensions between privacy, state surveillance, and public access become increasingly escalated. Sensitive personal information captured in video footage from officers' cameras has already begun to hit YouTube, Facebook, and other online repositories as a consequence of access-prioritizing FOI law in some states; and particularly in Washington State where these tensions have been felt more acutely in recent months. Breakdowns between law and policy, on one hand, and technological development, on the other, require us to rethink our information policy—that is, from a legal and regulatory standpoint, how should we balance information access and information control in a way that properly balances public access to records and democratic oversight with personal privacy and an effective criminal justice system?

Despite longstanding tensions between government power and citizen oversight, public record-keeping is a relatively recent phenomenon that largely emerged in the twentieth century (Solove, 2002). Public access to this information is often a prerequisite to citizens exercising power or seeking redress for potential rights violations stemming from secret (or not highly visible) activities of others (Forcese and Freeman, 2005, pp. 481-84). As such, an imbalance in information

access between a people and their government can tip the scales of power and limit the ability of the people to exercise democratic oversight and control those they have put in power to represent them (Forcese and Freeman, 2005, pp. 481-84). FOI laws often provide a great deal of access to government records and serve as a powerful and effective means for empowering oversight by journalists and ordinary citizens. In a very real sense, these laws provide a legal mechanism for citizen-initiated surveillance from underneath—sometimes called "sousveillance," inverse surveillance (Mann, Nolan, and Wellman, 2003), or reciprocal surveillance (Marx, 2005; Haggerty and Ericson, 2006, p. 10; Brin, 1998). The concept of inverse or reciprocal surveillance (which may take numerous forms) grants citizens greater power to check government abuse and force even greater transparency.

Watching the watchers, of course, may involve numerous methodologies beyond just requesting and analyzing public records. The miniaturization and decreasing cost of camera technologies has also empowered citizens to record matters of public interest, including the actions of police officers and other public officials. YouTube and Facebook (et al.) are replete with images and video of police officers interacting with civilians, and provide a platform for the "secondary visibility" (Goldsmith, 2010) of official police (mis)conduct. On the other hand, these same technological developments have also led to increased information acquisition about individual persons by states (vertical surveillance) as well as by other civilians (horizontal surveillance). In some ways, access to information has increased dramatically in recent decades; in others, political implementation of information policies has created what Jaeger (2007) calls "information politics," meaning "the manipulation of information access for political gain" (p. 851). However, the reality cuts both ways: governments and citizens both potentially have much greater access to information about the activities of the other than they have in the past—and this information has the potential to produce and influence power on both sides (*see* Forcese and Freeman, 2005, pp. 481-84).

Just months after some police agencies in Washington State began using BWCs in 2014, sensitive video footage of interviews with alleged prostitutes in hotel rooms and other officer-citizen interactions and arrests began to be posted to YouTube after the agencies were required to disclose every recording made by the cameras under broad state FOI law. Additionally, ALPR and facial recognition (and other biometric) technologies have also advanced to the point where vehicles and individuals can be identified, located, and tracked in public (and even not-so-public) spaces in real (or nearly-real) time, resulting in large databases of information about individuals' movements being held by various public and private entities. In Washington and a few other states, these databases have also been released to members of the public under state FOI laws, and the controversy surrounding the public disclosure of the information has resulted in some states exempting ALPR data from future release. If sensitive personal information is disclosed under legal FOI requirements, this information could easily contribute to violations of individual privacy. Under some current regulatory frameworks, *the visibility of individual citizens (innocent, presumed innocent, or guilty) is inextricably tied to the visibility of the state*.

This increased visibility, of both states and citizens, has been driven (at least in part) by advancements in technology and the methods of surveillance that such technological change has enabled. The consequences of these developments, and our society's legal, technological, and political responses, have important ramifications for individual freedom, and highlights tensions between individual interests in free speech, privacy, and security. The use of surveillance technologies, such as BWCs and ALPR, might be viewed as only abstractly linked to their stated purposes of crime control, "based on symbols, (that which is hidden must be revealed), theories (surveillance deters) or faith (technology works; it will work here as well)" (Leman-Langlois, 2008, p. 244). These assumptions play on our society's increasing reliance on and trust in technology to mediate power relationships and protect us from actual physical harms. Whether, in fact, these assumptions are correct in any set of cases is a question of great practical, philosophical, and empirical import.

By examining these (often) crisscrossed forms of surveillance by reference to recent accounts of government-citizen tension in the United States, and in Washington State in particular, this dissertation will emphasize the role that *information* (as object, process, or knowledge) (Buckland, 1991, p. 351; Marchionini, 2008), plays in generating power (and the potential for domination). The recent proliferation of surveillance in society and its attendant questions about information access and control have important ramifications for how we think about political freedom—and how much freedom we ought to let slip away for the sake of security. Importantly, security and freedom are not battling a zero-sum game; security can be protected by the exercise of non-arbitrary power (which, under a neorepublican conception of liberty, is freedom preserving) and the reduction of arbitrary power (domination) clarifies roles and promotes individual and collective political freedom but does not necessarily reduce the ability of the government to protect its people. Achieving this balance while maintaining robust individual rights of privacy and free speech (including access to information) is no small task.

1.3. Significance of the problem

Information policy encompasses a wide terrain, from enabling (or limiting) access to government information, allowing or prohibiting governments from accessing information about their citizens (Jaeger, 2007, p. 841), such as in the Fourth Amendment search and seizure context (*see* Slobogin, 2008), facilitating First Amendment guarantees of free speech (Balkin, 2013; 2004; Dawes, 2010, p. 377), and defining intellectual property policy (Jaeger, 2007, p. 842; Dawes, 2010, p. 377; *see also* Benkler, 1998). All of these instantiations of information policy have significant implications for democracy (Jaeger, 2007, p. 841; Balkin, 2013, pp. 102, 130; Jaeger and Burnett, 2005, pp. 466-69). Limiting access to government records not only limits the ability of the public at large to oversee government activity, but it also hinders journalists and the news media, as well as academic researchers and librarians (Jaeger and Burnett, 2005), from effectively carrying out their broader social functions. However, it can also protect the privacy and dignity of individuals as it limits broad access to the 'digital dossiers' of ordinary citizens.

Ideally, the nature of representative government would dispel the idea that governments (in all their parts) and citizens stand opposed to each other. Indeed, much government surveillance is ostensibly conducted for the good of the citizenry writ large (to protect against crime and terrorism, among other things), and governments are generally far from monolithic entities with singular purposes standing opposed to public access to information. But the ongoing collection of massive amounts of information by state bodies serves to reify the coercive power of government (Forcese and Freeman, 2005, pp. 481-84). Without similar expansion in the people's right to access information about government action (a form of "reciprocal surveillance" (Brin, 1998; Haggerty and Ericson, 2006, p. 10)), the people may lose their ability to conduct oversight and ensure government acts in a non-dominating fashion.

Without robust rights to access information about government action (a form of "reciprocal surveillance" (Brin, 1998; Haggarty & Ericson, 2006, p. 10)), the people may lose their ability to conduct oversight and ensure government acts in a non-dominating fashion. However, this same public access to information (which plays a significant part in ensuring transparency and holding government accountable to its citizens) may also potentially threaten the viability and effectiveness of such methods to achieve socially desirable outcomes and may also violate individual rights to privacy when personal information collected by the surveillance systems are disclosed or disseminated to third-parties (including the public, under FOI laws). These risks have been highlighted by the public disclosure and secondary publication (via YouTube, blogs, or online news outlets) of sensitive personal information contained in government records, including body-worn camera and dash-camera video footage, automated license plate recognition (ALPR) databases, gun-permit registries, and campaign contributions in support of controversial political endeavors, among others.

As a consequence, not only do we see tensions between transparency (access, accountability, and free speech) and secrecy (security), but we also see significant tensions growing between public access to government information, legitimate personal privacy interests, and societal interests in an effective and efficient criminal justice system. Importantly, as we increase transparency and the visibility of the state (e.g. by instituting or liberalizing access to information laws) while also maintaining or increasing surveillance and information seeking by government agencies (e.g. by allowing or requiring police officers to wear body cameras), we also increase the visibility of individual citizens who, on some accounts, incur significant privacy costs.

The world has shifted from a situation, which had existed for most of human existence, where citizens had virtually no power to demand access to government records to a contemporary recognition of access to information as an important human and political right (Blanton, 2011). The public sphere, which combines public access to the flow of information as well as public forums in which citizens may express themselves (Jaeger, 2007, p. 842), is vitally important to the ability of citizens to critique government action and "its monopoly on interpretation of political and social issues" (Jaeger, 2007, p. 842; *see* Dawes and Helbig, 2010, p. 50) and is essential to protect basic civil liberties (Strossen, 2013; Nerone, 1994, p. 6; Jaeger, 2007, p. 842; *see also*

Strossen, 2005, p. 78-79). However, the adoption of increasingly sophisticated surveillance methodologies in concert with the consequences of some outdated information access laws has placed the legitimacy of current legal frameworks into question, as similarly important human or civil rights, such as the right to privacy, become the unintended victims of unsuccessful information policies.

Yet, at the same time, it is clear we need an information policy that strikes a better balance while still retaining a robust system of information access. It is also clear that democracy is predicated on the presumption that the public is sufficiently informed (or has the ability to become informed) and able to intelligently participate in political life, regardless of whether a preferred political theory claims civic virtue is inherently or instrumentally valuable. And, "[w]ithout access to adequate and appropriate information related to governance, such informed participation and deliberation are impossible" (Jaeger, 2007, p. 843). A free press and the diffusion of public libraries and Internet access all play roles in supporting positive information policies, just as these interests are hindered by prohibitive national security laws (such as national security letters with accompanying gag orders or prohibitions on revealing aggregate statistics about such requests) and weakening protections for journalists and confidential sources. Additionally, promoting broad access to government information raises significant concerns about information reliability, comprehensibility, completeness, privacy of data subjects, and a host of other problems (Dawes, 2010, p. 378). Thus, as we seek to balance liberty with security—with public access and government secrecy for certain purposes—we need to critically and thoughtfully evaluate the broader ramifications of our information policies. The purpose of this dissertation is to do just that, at least with regard to the context presented by the cases under consideration in succeeding chapters.

1.4. Primary and secondary research questions

This dissertation is guided by the following primary research questions (questions 1-3 have both descriptive and normative aspects). Implicit in the phrasing of the questions are the assumptions that the moral value, and legal rights, of privacy, access to information, and criminal justice can conflict, in practice, and that line drawing in possible. These assumptions rely on the theoretical presupposition that these values are inherently valuable as distinct rights, all of which are also instrumental to something external—in this case, personal freedom. My arguments for these theoretical propositions are provided in much greater detail in section 2.2, *infra*.

RQ1: In the cases under consideration, how does (and how should) law differentiate between and prioritize the competing interests implicated by public access to government information (and the associated societal interests in state accountability and transparency, as well as individual rights under the First Amendment to gather information about government conduct), individual privacy (particularly where disclosure of government records or civilian video would result in the disclosure of personally identifiable information), and local or national security and law enforcement interests?

RQ2: Does the answer to the previous question depend on spatial or locational considerations, such as when the locus of the surveillance activity itself (or the information captured by such surveillance) is located in a public versus a private space?

RQ3: How does (and how should) the law address the distinct normative questions (posed above in RQ1 and RQ2) related to the 1) initial acquisition of personal information, 2) the subsequent use of the acquired information by the acquiring entity for its own purposes, and 3) any eventual disclosure of such information to third parties?

RQ4: How does utilizing a neorepublican theory of freedom inform the development of an information policy that answers the normative questions posed by this research? Is this approach adequate?

In the context of each of the three cases under consideration, the following secondary (descriptive) questions will be used to guide the analysis and to inform the answers to the primary research questions:

RQ5: In each of the three cases under consideration, what tensions exist between these various values (e.g. privacy, security, accountability, expression, and access to information)?

RQ6: How do the methods of surveillance under consideration in each of the phenomenon increase or diminish the visibility of police officers, state surveillance programs, and civilians?

RQ7: How does this increased visibility exacerbate (if at all) the tensions between these values?

RQ8: How does the law regulate the relevant methods of surveillance (including the collection, retention, and disclosure of personal information, as well as the public/private nature of the information)?

RQ9: What normative conclusions does the application of neorepublican theory generate about resolving tensions between freedom, free speech, and privacy in each case?

2. Methods

2.1. Introduction

Because this dissertation project is not explanatory research, it is not primarily driven by hypothesis testing. Rather, the exploratory purposes of the project consist of identifying and analyzing key issues, values, and variables through an analysis of legal rules (whether derived from statutes or cases), legal and philosophical theory, and social theory, applicable within the context provided by the research questions. In the descriptive portion of the research, I describe and define various social phenomena around officer-citizen surveillance interactions (or at least confirm or build on prior descriptive research in this area) as well as the applicable legal rules that apply to these phenomena. The research is also policy-oriented because of its focus on developing normative conclusions about what law should be, at least as can be derived from the prior analysis on what the law is and how this law has had impact in the real world.

Methodologically, the study is a *single-outcome study* employing a *within-case analysis* (Gerring, 2006; see also Seawright and Gerring, 2008). Gerring (2006) defines a single-outcome study as a case study design that is designed "to investigate a bounded unit in an attempt to elucidate a single outcome occurring within that unit" rather than the goal of discovering "something about a broader population of cases" (p. 707). A within-case analysis as part of the single-outcome study allows for the detailed explication of the case of special interest. The study is bounded by jurisdictional criteria (law) as well as by the phenomena under study. The single-outcome study might be more common within academic legal research than in the social sciences (perhaps as a consequence of the doctrinal nature of much legal scholarship). Despite limitations on the ability to translate findings from a single outcome study to a broader population (especially when the case under consideration is extreme or deviant), this method allows for a deeper understanding of particular circumstances—in this case, the balance between privacy law and access to information within Washington State (the descriptive "outcome") and allows normative claims of the sort: if the legal rules of a jurisdiction look like X, then Y is a possible outcome, which should be addressed—normatively—by implementing policy Z (e.g. for reasons based in applying social theory or political philosophy to the analysis of X and Y).

To this end, I employ doctrinal legal analysis, philosophical analysis and argumentation, and conceptual methods from Value Sensitive Design, to develop normative theory (i.e. policy-oriented normative conclusions about what the law should be and how the law should address the value tensions between privacy and access to information presented by the cases in Chapters 5-7). This theory development is informed by bringing together relevant theories and concepts from various fields that do not always talk to each other, including information science/studies, law, surveillance studies, political philosophy, and criminology/policing/criminal justice studies. I occasionally draw from empirical data and findings from prior and/or on-going research when these findings have relevance to the conceptual analysis, but the dissertation is designed to stand on its own as a conceptual investigation of these issues. In the following subsections, I provide

my rationale for selecting each of the phenomena under study (referred to below as the "cases"), followed by a summary of each case study.

2.2. Legal research

Doctrinal legal research is the study and analysis of legal texts (e.g. statutes and judicial decisions) and rules with the aim of developing and understanding legal doctrine (Chynoweth, 2009). It involves "a synthesis of rules, principles, norms, interpretive guidelines and values" (Hutchinson and Duncan, 2012, p. 84, *quoting* Mann, 2010, p. 197). However, knowing doctrine itself does not provide a complete picture of the law—that requires application of legal rules and doctrine "to the particular facts of the situation under consideration" (Chynoweth, 2009). Doctrinal legal research has long dominated the legal academy—of which it is the "core legal research method"—but "until relatively recently there has been no necessity to explain or classify it within any broader cross-disciplinary research framework" (Hutchinson and Duncan, 2012, p. 85). Relatedly, very little academic legal research contains any methodological description, and when it does—typically when the research is interdisciplinary, it involves empirical data collection, or is comparative—an article's methods section only describes the social scientific methodologies employed (e.g. sampling, case selection, etc.). As stated by Hutchinson and Duncan (2012), "the doctrinal method is often so implicit and so tacit that many working within the legal paradigm consider that it is unnecessary to verbalise the process" (p. 99). That is not to say the method should not be described in any detail, but merely to situate the method within its real-world context; well-utilized and practiced by lawyers and legal academics, but under theorized and under critiqued within and outside the discipline.

In this dissertation, I employ doctrinal legal research as defined above, as the process of synthesizing legal rules and legal texts to develop an understanding of what the law *is* (this work is largely the subject of Chapter 4) and *how it has been applied in practice* by judges in (generally appellate) court decisions. This necessarily involves identifying the local and federal constitutional, statutory, and case law applicable to a certain set of facts (or generalized scenario). After determining what law is relevant, often by referring iteratively between codified law and judicial interpretations of that law in particular cases, a synthesis of the current state of the law can be developed. The process of identifying relevant and useful case law also involves identifying whether (and how) later judgments have interpreted the legal conclusions presented in any given case to determine whether the case can be considered "good law"—that's is, law that has not been modified, overruled, or nullified by later legal developments. I have utilized Westlaw's® Classic—a standard legal research database—to help achieve these objectives, which contains links between cases, citations, and legal codes (as well as secondary commentary).

Understanding what law is applicable within each of the cases and identifying what the law is (e.g. how existing law balances informational privacy, speech, and access to information in a context also encompassing criminal procedure) is vitally important to making normative judgments relevant to each case. This methodology also allows me to uncover how the law differentiates (if it does) based on the public/private dichotomy—that is, has the law struck a different balance

between privacy and access to information based on spatial or property-based considerations related to the locus of the deployment of surveillance or of the personal information itself? These laws not only regulate surveillance and police-citizen encounters formally (even if not directly), but they also affect the meanings that officers (and the public) may ascribe to various surveillance-related phenomena and the concerns these individuals have in regards to the legitimacy of such surveillance. As Herbert (1998) has found, the law is not necessarily a determinant of police behavior, but is does structure such behavior in important ways (p. 352). I move from a doctrinal explication of the law to the application of legal theory, social theory, and political philosophy through philosophical argumentation to arrive at my ultimate normative conclusions. My utilization of *legal theory* as a conceptual method is particularly directed at examining and contrasting certain theories of privacy and access/free speech. I conclude with a section on limitations and directions for future work, and discuss how law in context (e.g. socio-legal) methodologies could inform future work in this area (including my on-going empirical research that extends beyond this dissertation project).

2.3. Philosophical method

In concert with the methodologies from Value Sensitive Design (below) and the legal research mentioned above, I use the philosophical method to identify the moral, political, or legal problem(s) raised by the parameters of each case. Then through normative philosophical analysis and argumentation I attempt to identify a reasoned and defensible solution(s) to the problems presented. This analysis involves a few analytic stages that build on each other. First, in order to espouse a defensible normative theory of privacy and information access, I establish my preferred basis for coming to moral judgments (i.e. my preferred normative ethical theory) and situate my foundational claims about the values of privacy, access to information (or expression more broadly), safety, and security within this theory. Much of this work is done in Chapter 3. In each of the cases that follow (Chapters 5-7), I move from using normative theory to establish and defend moral claims (ethics) and values to crafting arguments about normative conclusions to how law and policy ought to be instituted to address these problems and effect the solutions (through the use of philosophical argumentation and political philosophy). This endeavor encompasses normative conclusions about both moral rights and legal rights (and where these ought to differ).

Where moral rights can be seen as *universal* under some conceptualization (Regan, 1992, p. 44) (though there may be cultural differences that need to be addressed), legal rights are bounded by complicated and sometimes intersecting jurisdictions. However, when determining what legal rights *ought to be*, the importance of these jurisdictional limitations is significantly lessened. In fact, there are good reasons to want our normative judgments about what the law should be to be in line with our moral judgments. There may be situations, however, where we may have important reasons to separate the two; for example, we may want to say it is morally wrong for an individual to engage in hate speech, but it may not be appropriate to regulate this speech with legal instruments because to do so might restrict individual liberty or grant states too much power, as a matter of political philosophy, or because we want to allow people to make bad choices for a

variety of other reasons. Importantly, because we must distinguish between moral and legal rights, we must also distinguish between moral justice and legal justice, as legal justice is present even during the enforcement of a morally unjust law.

The trustworthiness of my normative conclusions, of course, depends on my development of defensible arguments. In Chapters 5-7, I present arguments situated in each individual case. In Chapter 8, I propose and defend a consolidated argument—what I refer to as an information policy. In doing so, I attempt to follow Westin's (2000) general guidelines to distinguish premises and conclusions, present ideas in a natural order, start from reliable premises, use concrete and concise language, avoid loaded language, use terms consistently, and stick to one meaning for each term. At times, I argue by example or analogy (Westin, 2000), utilizing the facts from prior legal cases, value scenarios developed in each chapter, or examples from recent developments. When appropriate, I also utilize authoritative sources to help bolster my claims, including legal authority. Empirical evidence, whether that presented by others or my own data collected in my past or on-going empirical projects, will also be used to support my normative claims.

2.4. Value Sensitive Design

Value Sensitive Design (VSD) has been defined as "a theoretically grounded approach to the design of technology that accounts for human values in a principled and comprehensive manner throughout the design process" (Yoo, et al., 2013, p. 420; Friedman, Kahn, and Borning, 2006; Friedman and Kahn, 2003). Van den Hoven (2007) has also referred to VSD as the process of "doing responsible information technology" (p. 67). The framework and its associated methodologies are intended to make human values an important part of the design of technologies (Friedman, 1996, p. 17; Van den Hoven, 2007, p. 67). VSD emerged in the field of Human-Computer Interaction (HCI) (Czeskis, et al., 2010; Friedman, Smith, et al., 2006) and aspects of VSD research and methods fit well within the domains of computer ethics and ethics of information technology (Moore and Unsworth, 2005; Van den Hoven, 2007). VSD emerged in the 1990s as researchers like Batya Friedman and Helen Nissenbaum collaborated on research investigating bias and autonomy as human values in the development of computer systems and software (Van den Hoven, 2007, pp. 67-68; Friedman, 1996; Friedman and Nissenbaum, 1997; 1996; 1995; Nissenbaum, 1998). VSD literature defines *values* as "what a person or group of people consider important in life" (Friedman, Kahn, and Borning, 2006, *citing* Simpson and Weiner, 1989).[2]

[2] Note that this definition of value differs importantly from the definition of *moral value* I employ in Chapter 3 based on Moore's (2010) theory of moral value and privacy that disregards subjective preference satisfaction. However, to the extent that a generalized outline of subjective preferences can impact our thinking about human flourishing as encompassing some aspects of our subjective personal life projects, it can be valuable to think about and measure these preferences, as long as we keep the two concepts separated and distinct throughout the analysis (see also my discussion of Cohen's (2013) theory of privacy in Chapter 3 for additional arguments for why this might be relevant to the overall project in this research).

Generally, VSD research includes a tripartite methodology, encompassing *conceptual*, *technical*, and *empirical investigations*. However, in this dissertation, I restrict my use of these methods to a few of those within the conceptual category, leaving technical and empirical analyses for later work.[3] In this current dissertation project, I employ conceptual methodologies from VSD to further elucidate the values and value tensions raised in each of the three cases under consideration, to clarify and define the parameters of each value, as well as to identify the relevant stakeholders (Miller and Friedman, et al., 2007) whose interests will need to be accounted for in the normative legal and philosophical analysis that will follow. A small amount of prior VSD literature has also grappled with the tensions between the disclosure of public records and privacy (Munson, et al., 2012; 2011; Johri and Nair, 2011), and I draw upon this literature in my examination of these issues.

Specifically, in this dissertation project, I utilize three conceptual methods from VSD: value scenarios, the value tensions framework, and stakeholder analyses. First, I employ *value scenarios* (Nathan, et al., 2007; Yoo, et al., 2013, p. 420; Czeskis, et al., 2010) to help me anticipate what is at stake with different policy and regulatory options, as well as to communicate comparisons of the potential outcomes of different policy and regulatory options suggested by my theoretical commitments. Value scenarios were introduced by Nathan, et al. (2007) as an extension of traditional scenario-based design and the concept of design noir (see Dunne and Raby, 2001) from within the HCI and design literatures (Nathan, et al., 2007, p. 2586). These scenarios are generally, "fictional vignettes that emphasize social and value implications of a 'hypothesized' technology" (Czeskis, 2010) and often "consist of stories that emphasize the social and value considerations of new technologies, especially long-term and potentially negative impacts" (Yoo, et al., 2013, p. 420). Value scenarios rely on the concept of systemic interaction, defined as "those developments which either happen at large social scales or those that have large-scale effects that go beyond the initial locus of the interaction" (Nathan, et al., 2007). Because the three primary cases in this dissertation concern surveillance technologies inserted into social interactions between citizens and state at some scale, and because the interactions between these technologies, law, and individual rights may have large-scale effects beyond the initial collection of information (e.g. privacy impacts of disclosing the data under public disclosure laws or the posting of the data to the internet), this method is relevant to the current study. Of course, the conceptual purpose of developing these scenarios is not to foretell the future with any degree of certainty, but rather to "help us think about how the actions we take today will shape the conditions of our future" (Nathan, et al., 2007). In some ways, my use of value scenarios will also allow them to function as philosophical cases upon which I can analyze my normative recommendations.

Secondly, I draw upon the value tensions perspective (Czeskis, et al., 2010) embedded in VSD literature as an analytic tool to think through the range of values that are relevant to my cases (aside from privacy, accountability, and transparency) and that may be at odds with each other.

[3] In particular, I am utilizing VSD methodologies in on-going empirical research investigating the role of human values in the design of body-worn cameras by companies designing these systems for use by law enforcement.

The value tensions perspective functions as a useful analytic tool as I consider the different values that are relevant to each case, which are obviously more wide-ranging than just privacy, transparency, and criminal justice.

Finally, I also employ stakeholder analyses to identify the various stakeholders that may be affected by the technologies I am examining as well as by my policy prescriptions. Although the direct repercussions of cases may be limited to only some of the possible stakeholders, it is important that I identify the boundaries of these groups (and the criteria that I use to include/exclude for purposes of my analysis). In VSD literature, *direct stakeholders* are defined as "the people directly interacting with technology," while *indirect stakeholder* are "others whose data or presence may be implicated by the technology" (Czeskis, et al., 2010).

This VSD analysis will be intertwined with my use of the philosophical method, and each will inform each other in the pursuit of identifying, defining, and conceptualizing values and value tensions.

2.5. Empirical data collection and analyses

As stated earlier, I draw upon some empirical research in this project, but do so solely as a tool to help frame and guide my conceptual analysis. On occasion I draw upon some of the findings from my own prior and on-going empirical projects, including collection and analysis of Seattle Police Department ALPR databases and fieldwork conducted with police officers wearing BWCs. This analysis is not necessary to the conceptual investigation pursued in this dissertation project but, given my commitments to law-in-action socio-legal research within an interpretivist position (see Chapter 3), I believe it strengthens, enriches, and contextualizes the conceptual work I am ultimately able to do. In each of the following case studies (Chapters 5-7), I describe more fully the empirical findings and my data collection methodologies relevant to the examples presented in each case. For example, in Chapters 5, 6, and 7, I present some of the initial findings from my on-going analysis of ALPR databases disclosed under public records laws by the Seattle Police Department as well as field research with two police departments in Washington State that are currently piloting BWC programs. This research is on-going and only a portion of the data collected to date is relevant to this dissertation.

2.6. Case selection

The phenomenon outlined above (citizen' rights to record police officers, on-officer video, and ALPR) were chosen purposively, based on some important similarities shared across cases as well as some differences. The phenomenon were chosen with the aims of 1) digging deeply into the experience within one jurisdiction (Washington State), and 2) by surfacing comparisons in law from other jurisdictions (persuasive jurisdictions within the United States—e.g. legislation from other states and case law from federal circuit courts outside the Ninth Circuit or other state courts that have addressed similar issues—as well as the European Court of Human Rights) to achieve an analysis that is, to some degree, representative of the broader phenomenon (so that the normative theoretical insights might be generalizable outside the cases to some extent) and because

they offer some useful variation on the variables of interest to my analysis (e.g. rights to access information about government conduct, visibility of police officers and civilians, access/privacy law). Civilian video of police officers, police officer use of wearable cameras, and license plate recognition all raise questions about legal rights to capture or collect personal information, to use the information for the entity's own purposes, as well as any eventual disclosure of such information to third parties. Additionally, privacy rights in each of these scenarios are dependent on (or linked to) spatial/locational considerations. Public access to the collected information is thus dependent on both legal limitations on acquisition, use, and disclosure, including privacy rights that may be based on spatial reasoning.

In terms of similarities, each of these cases highlight 1) the ability of surveillance to increase the (secondary) visibility of both civilians and police officers (i.e. they raise questions about privacy intrusions stemming from public access to and use of information), and 2) how spatial considerations play a role in designing legal rules and legal outcomes. Civilian video provides a form of secondary visibility to the persons captured in recordings, whether police officers, citizens interacting with police officers, or bystanders. This phenomenon is central to the development of the theory of new visibility (Thompson, 2005; Goldsmith, 2010) and is also highly relevant to the concepts of counter/reciprocal/inverse surveillance (Haggerty and Ericson, 2006; Marx, 2005; Brin, 1998), sousveillance (Mann, Nolan, and Wellman, 2003), and the participatory panopticon (Whitaker, 1999). Additionally, as the use of BWCs by police officers has also been partially a response to the rise of civilian video of police conduct and also functions partially as a reciprocal inversion of civilian video as a form of sousveillance (watching from beneath), an analysis of the civilian video phenomenon and the relevant legal frameworks is appropriate to set the stage for the other cases. The use of ALPR by law enforcement agencies increases the visibility of individuals (or at least individual vehicles that can be tied to a small number of identifiable persons) and makes the spatial movements of these persons visible to law enforcement and, when publicly disclosed, to the wider public. The collection and public disclosure of ALPR data also makes the movements of individual police officers more visible, as it can enable precise historical tracking of officer movements as well as spatial analysis of these movements over time. Likewise, the use of BWCs by police officers increases the visibility of the officers themselves, but also increases the secondary visibility of subjects of police attention and innocent bystanders. BWCs, by virtue of their status as wearable technology, also travel with officers through public spaces and into homes, hospitals, businesses, shelters, and a variety of other non-public spaces, implicating spatial considerations.

The differences across these three cases include 1) the methods/form of surveillance, 2) the identity of the entity conducting the primary surveillance activity (officer or citizen), 3) the nature of the information being collected (license plate numbers and photographs of vehicles or video evidence of police-citizen interactions), and 4) some of the laws applicable to each phenomenon (there is some overlap; for example, the Fourth Amendment applies to both BWCs and ALPR use, and Washington State privacy law applies to citizen recordings as well as on-officer BWC) and ALPR (though, as we will see, these laws have little to say in terms of regulating ALPR). Different legal

rights and obligations are in play when citizens are the actors making the primary recordings (primarily a free speech interest) versus a police officer (which is regulated, in large part, by the Fourth Amendment). However, the free speech interest in documenting police conduct through citizen recordings is similar to the free speech interest in accessing government records about police conduct when the police are conducting the primary surveillance—they both concern the right of citizens to access and document police conduct, either as a form of speech itself or as a predicate to informed deliberation and the exercise of speech or other protected rights. The cases also concern the collection and use of different types of personal information. A single scan of a license plate (even with all the associated metadata regarding time, location, or whether the plate was contained on a "hot list" of wanted vehicles), or even a larger set of license plate scans, may be seen as a qualitatively different type of privacy intrusion than a video of a person's interaction with a police officer inside his or her own home (or the posting of a video containing a third-party's personal information to the internet). This claim implicates the notion of the "mosaic theory" of the Fourth Amendment and the language in Justice Sotomayor's concurrence in United States v. Jones (2012) that questions the intrusiveness of aggregating and analyzing multiple data points on identifiable individuals.[4]

In terms of law and legal analysis, the set of chosen phenomenon is limited by legal jurisdiction—that is, there is a consistent focus on understanding and analyzing the law in Washington State as it applies to each of the cases, whether precedent is state or federal law—but persuasive authorities (e.g. federal appellate courts in other circuits) and approaches from jurisdictions (e.g. the European Court of Human Rights) will also inform the analysis and to uncover important differences between the selected cases and the broader population. This approach will allow for some limited cross-case comparison on the variables of interest and variation offered by the experience of each jurisdiction.

2.7. Connecting methods and research questions

The research questions presented here are well suited to the exploratory, descriptive, and policy-oriented methodology outlined above. In each of the chapters, I utilize philosophical problem identification and Value Sensitive Design methods to surface the key issues, values, tensions, and stakeholders (an exploratory outcome). I then examine the applicable law and the social and philosophical theories presented above to provide a description of the phenomenon under study as well as the law and legal rules that apply to these phenomenon. The descriptive and exploratory

[4] The mosaic theory is premised on the idea that courts can sometimes consider information gathered through broad government surveillance or the individual surveillance activities of government agents in the aggregate when deciding when a "search" for Fourth Amendment purposes has occurred, rather than being required to focus sequentially on each distinct piece of information or government act (Kerr, 2012). This is an important idea as it opens the door for challenging government acquisition of personal information (vis-à-vis Fourth Amendment searches) based on the idea that the aggregation of many pieces of personal information (over time and/or from different sources) can expose the individual to more significant privacy violations than when the collection of each of these bits of information is examined on its own. For a more in-depth discussion of the mosaic theory, see section 5.3.1, *infra*.

aspects of this project will answer the non-normative versions of Research Questions 1-3. The policy-oriented synthesis will then answer the normative versions of Research Questions 1-3, and the application of neorepublican conceptions of freedom as non-domination to each phenomenon will answer Research Question 4. The secondary research questions, numbered 5-9, are answered in the process of answering questions 1-4 in each case.

2.8. Theory development

An important outcome to this conceptual investigation is the development of an original theory that synthesizes and balances the values presented by the phenomenon under study into a larger information policy. The other methodologies mentioned above are designed to facilitate the development of theory that has the potential to inform legal change and the development of policy, and (possibly) the (re)design of technologies to better support the proposed solutions. I develop parts of this theory in Chapters 5, 6, and 7, and present a consolidated theory in Chapter 8.

3. Theoretical foundations

In the following sections, I outline the epistemological commitments, and theoretical and social theories that guide my dissertation research.

3.1. Epistemology and ontology

I view myself primarily as a socio-legal researcher with a research agenda focused primarily on issues of information policy (including the legal, ethical, and political aspects of such policy), and my philosophical positions fitting broadly within a post-positivistic account of empiricism. As a cross between an information scientist (broadly defined) and socio-legal researcher with an interest in understanding how legal structures and information technologies impact the everyday lives of people in society, I also approach much of my research from an interpretivist position. Additionally, while I can definitely see the polarization of extremes between positivism and various anti-positivistic accounts, I find myself drawn to the ideas expressed by Ron Weber (2004) that, in practice, many of the alleged differences, at least between positivism and interpretivism, are not as pronounced as some voices might make them appear. I find myself near this point of convergence. I am taking a realist and pragmatic position that allows for interplay between the positivistic approach to behaviorism and interpretivism in line with Tamanaha's proposal for a realistic socio-legal theory guided by philosophical pragmatism (Tamanaha, 1997).

Importantly, this dissertation project is a conceptual pre-curser to a larger empirical study. As such, the largely conceptual approach taken here represents an important step towards generating and positing theory. This dissertation also generates important conceptual groundwork that will support my future and on-going empirical research. Throughout this study, I draw upon some of my own exploratory empirical research—mostly data collected through fieldwork and public records requests—to inform my attempt to generate defensible theory. However, my intention is that any such use and reliance on this exploratory data is not required for this dissertation to be successful on its own. That is, my epistemological commitments allow for purely conceptual research (such as that proposed here) as an important aspect of my larger research agenda and for generating theory, but my preference is to, ultimately, combine this conceptual sort of work with appropriate empirical methodologies to test and refine the advanced theoretical contributions. Ultimately, I am drawn to a form of socio-legal research that "is ultimately optimistic, maintaining that law is a world of action and our responsibility is to participate in it" (Nourse and Shaffer, 2009, p. 137).

Despite this dissertation's focus on conceptualization, legal analysis, and theory-building, my overall research agenda generally fits well into the tradition of the law and society movement, active for the past few decades in the United States, and is informed by movements within legal and socio-legal philosophy that privilege an empirical account of law. Some of my work is informed by the Empirical Legal Studies (ELS) movement, which has been primarily driven by large-n quantitative studies focused directly on law itself, which I find valuable. However, I am specifically drawn to the philosophy found within a separate, though less well known, empirical

socio-legal studies movement, namely a New Legal Realism (NLR) that privileges an interdisciplinary and multi-method approach to understanding law in a broader social context. I also strongly agree with much of Tamanaha's proposals for a social theory of law based in pragmatism and realist thought (Tamanaha, 1997).

NLR is an emerging philosophical tradition in legal philosophy and has impacted some socio-legal research. It extends and modifies "old" legal realist thought, from a top-down focus on courts, judges, and legal institutions, to a bottom-up approach that seeks to understand the law first by focusing on the impact and everyday interactions of laypersons with the law (Nourse and Shaffer, 2009). Despite its bottom-up focus, NLR also values the integrated study of "law on the books," legal practice, legal institutions and the lawmaking process. NLR also espouses an interdisciplinary empirical approach to legal scholarship that combines both quantitative and qualitative methods to achieve a better understanding of the human experience and the dilemmas facing the rule of law and legal institutions. In this sense, it fits within post-positivistic empiricism and also contains aspects of certain types of pragmatism, or the blending of practical and theoretical accounts of law in society. It is, therefore, a good example of the type of interpretivism I present above in line with Tamanaha's (1997) thinking.

As stated above, I see myself primarily as a socio-legal researcher, but I also find myself, and my research, situated within a (very) broad conception of Information Science and definitely within the Information field more broadly. My connection to Information Science and the Information field exists by virtue of my interests in examining the way in which information, as a product of surveillance practices of states or citizens, constitutes power and affects civil liberties and citizen-state relations. My proposed research is also connected to the Information field by virtue of my emphasis on understanding how law enforcement agencies document information and respond to freedom of information requests. Throughout this dissertation project and my future research, I intend to utilize public records requests to acquire documents from government agencies and also to explore the way in which these agencies respond to my requests and similar requests of others and modify their documentation practices because of the surveillance aspects inherent in public records laws.

3.2. Legal and philosophical theory

In the following subsection, I outline and contrast the basic parameters of two conceptions of political freedom,[5] the liberal notion of negative liberty influenced by Isaiah Berlin (1969) and the neorepublican conception of domination espoused by Philip Pettit and Frank Lovett (Pettit, 1996; 1997; 2012; Lovett, 2013; Lovett and Pettit, 2009).[6] According to its proponents, neorepublican political theory owes its origins to the experiences of the early Roman republic, and has been influenced and adopted by early figures such as Machiavelli, Jefferson, and Madison, and, more

[5] I use freedom and liberty interchangeably throughout as synonyms.

[6] Republican and neorepublican political philosophy, of course, have no necessary connection to the Republican political party or its politics.

recently, by writers like Philip Pettit, Quentin Skinner, and Frank Lovett, among others (Lovett, 2013; Skinner, 1998a; 1998b; Fink, 1945; Robbins, 1959; Pocock, 1979; Sellars, 1994), although the precise historiography is still somewhat controversial (Lovett, 2013). Frank Lovett and Philip Pettit argue that their version of neorepublicanism has been adapted from what has been called "classical" republicanism to distinguish it from other, more communitarian, approaches (Lovett and Pettit, 2009). Lovett also states that since political liberty ought to be "understood as a sort of structural relationship that exists between persons or groups, rather than as a contingent outcome of that structure," freedom is properly seen "as a sort of structural independence—as the condition of not being subject to the arbitrary power of a master" (Lovett, 2013, s. 1.2).

Against this backdrop, I will then present an overview of some of the primary theories of privacy and free speech relevant to the cases discussed in Chapters 5-7, *infra*, and outline my own preferred normative conceptualization of these values and their connections to neorepublican freedom. Under this conceptualization, privacy, speech, and access to information are all valuable—at least in part—because of their ability to limit the actual interference and domination experienced by individuals. That is, they are each distinctly valuable as independent rights, and their instrumental potential to effectuate and preserve liberty is particularly important because freedom from domination is a vitally important component of—and necessary condition for—human flourishing. Some amount of privacy undoubtedly ought to be protected absent clear instrumental connections to freedom, and there are surely other aspects of human flourishing that are important/necessary as well, but it is precisely the connections between these values and the political philosophy of freedom that I intend to examine throughout this dissertation. Informational privacy rights restrict the ability of others (including the state) to collect and use personal information about a person (a form of power) and to disclose such personal information to others, thus reducing the possibility for state interference in private matters. Robust rights of free speech, belief, and association, with their associated limits on the state's ability to interfere with individual choice and action, similarly support this view of freedom. When considering the release of government surveillance information containing personally identifiable information about civilians, enhanced privacy protections would also serve to reduce the possible domination by one citizen over another based on this increased downstream and collateral form of horizontal visibility.

However, because I am exploring a narrower subset of the possible broader rights to privacy and speech/access, namely the connections that these values have to liberty in the context of the cases presented in Chapter 5-7, with an emphasis on limiting domination, the benefits of protecting these individual rights can be seen as tied directly to the structural institutions and processes that allow for self-governance by the people and, ultimately, render government action non-arbitrary (or, at least, less arbitrary). Privacy rights, First Amendment protections, and access to information laws are much less meaningful if the public has no ability to command noninterference in the first place (i.e. government could alter these rights on a whim without fear that the people could overrule the government action).

On a related note, a theory of privacy that rests purely on reducing privacy to merely an instrumental aspect of liberty might leave some needed room for a society to determine for itself, through democratic deliberation, how to best balance speech and privacy interests, especially in regard to prospective intrusions by private, as opposed to state, actors. This is true because, for example, a society could establish a number of balancing tests that would solve the problem of arbitrary interference. On the other hand, such a possibility may leave the door open too wide to a form of ethical relativism as the means to determine baseline rights; for example, by allowing each society to choose for itself—democratically—to prefer one of these rights at significant expense to the other (or to disregard them both entirely in favor of something else, e.g. security). Julie Cohen provides a convincing argument against this sort of reductionism and consequentialist "balancing" of rights, claiming that calls to balance privacy with other values "lacks visceral force" and often ends with privacy coming up low in our lists of priorities (Cohen, 2013, pp. 1904-1905). The list of "privacy's counterweights is long and growing," and concerns for public safety, national security, and government transparency may be seen as more modern and cutting edge (Cohen, 2013, pp. 1904-1905).

Adam D. Moore (2010) also provides ample reasons to resist a pure reductionist approach that would not necessarily protect privacy as a distinct right with intrinsic value. He also presents a persuasive argument in favor of privacy based on its necessary connections to human flourishing. On this account, the real moral value of privacy should not be determined by desire satisfaction or personal (or even group) preferences (Moore, 2010, pp. 34-39). Rather, privacy has objective moral value—that is, its value exists "independent of the affective states of sentient beings" (Moore, 2010, p. 39)—because it is necessary to human flourishing and wellbeing (a eudaemonist account of value). Moore's middle-of-the-line approach, combining the essentialist and plan of life theories of human flourishing, appears to provide a convincing framework that resonates with my view that privacy is necessary for freedom (defined as the absence of domination) which is subsequently a necessary condition for human flourishing. Indeed, the basic notion of the plan of life position, if limited somewhat to ensure against sliding into subjectivity, presumes that an individual's ability to engage in autonomous decision-making in the creation and execution of a "unified, integrated… plan of life" without restraints on his/her "opportunity and ability to realize… basic goals according to their ordering in [that person's] life plan" (Taylor, 1983, p. 130; Moore, 2010, p. 42). In the presence of some possibility of domination, regardless of whether actual interference occurs, a person would not be fully able to satisfy these conditions.

In subsequent chapters of the dissertation, I will develop and apply my preferred approach to each case under consideration, drawing largely from the neorepublican position, as a means of working towards an overarching theory of information control and access (aka "information policy") in the final Chapter.

3.2.1. Freedom

In Isaiah Berlin's seminal essay on the topic of political liberty (1969; see also Swift, 2006), he outlines the trajectory of two different conceptions of liberty, what he calls "negative" and

"positive" liberties. These conceptions diverge because, on one hand, negative liberty "is simply the area within which a [person] can act unobstructed by others" (Berlin, 1969, p. 169), while positive liberty involves self-mastery, truly autonomous action, and the ability to act on second-order desires (Berlin, 1969, p. 178). Phrased differently, the extent to which a person is free, in the negative sense, rests on whether, or how thoroughly, that person is prevented, by another, from doing something the person wishes to do (Berlin, 1969, p. 169). A certain level of interference by another with one person's freedom to do something, in Berlin's view, can equate to coercion or slavery, and thus ought to be avoided (Berlin, 1969, p. 169). Berlin (1969) also noted that a certain amount of negative interference may be justified, stating that, "We cannot remain absolutely free, and must give up some of our liberty to preserve the rest" (p. 173).

Other writers have distinguished between various form of positive and negative liberty contained within Berlin's dichotomy, sometimes referred to as "effective freedom" and "formal freedom," as a way to clarify Berlin's distinctions and to make the point that the absence of restraint (defined in terms of legal restraints) does not always guarantee the actual ability of an individual to do something he or she is legally entitled to do (for example, a person may not be able to invest in some activity that would facilitate self-mastery or action in accordance with higher-order desires due to economic hardship or physical disability) (Swift, 2006, p. 55). On one hand, negative freedom is concerned with the absence of state restraint (or interference)—on some accounts this would also be bounded by the legitimate rights of others—while positive freedom may be concerned about equalizing the effective freedoms of everyone in a society (e.g. adequate food and access to transportation might be assured by a state mandating a certain level of basic income). Despite some claims that Berlin's distinction between positive and negative liberty (also sometimes referred to as "freedom from" and freedom to") doesn't hold up (Swift, 2006, pp. 52-54), Berlin does provide a very insightful tracing of the use of positive ideas about liberty that informed the development of various totalitarian regimes in recent history (see Berlin, 1969; Swift, 2006, p. 51).

In contrast to Berlin's account of negative liberty, Pettit's position removes the requirement of actual interference, but still maintains an arguably negative approach by focusing on eliminating the possibility of arbitrary interference from others without requiring any action (or self-realization) on the part of an individual to claim freedom (for example, through acting on their second-order desires or achieving self-mastery) (Lovett, 2013, s. 3.2). This claim itself, that neorepublicanism is related to the negative conception of freedom is, of course, not uncontroversial. The neorepublican conception does immunize certain forms of actual interference—non-arbitrary interference, to be precise—from its critique, considering some forms of actual interference entirely unproblematic.[7] Thus, the basic neorepublican position is not as negative as Berlin's account would require, and it represents a divide from more liberal thinking. However, rather than predicating freedom on ideas of self-mastery, autonomy, or a person's ability

[7] Defining "arbitrariness" in this context is not a trivial problem.

to act in accordance with their higher-order desires—one account of positive liberty—neorepublican theory is more concerned with ensuring the ability of the people to self-govern, by reducing domination (Lovett, 2013). Importantly, this approach to republican political thought is distinctly not republicanism of the more communitarian or Aristotelian varieties that might be more properly compared to forms of positive liberty. In contrast to communitarian or Aristotelian republicanism, neorepublicanism's definition of liberty does not consider the process of collective will formation or political participation as inherent aspects of political freedom (Lovett and Pettit, 2009, p. 12). Rather, political participation or civic virtue is an instrumental means of achieving and maintaining a high level of political freedom (Lovett and Pettit, 2009, p. 23), and should be promoted because of its instrumental utility.

Applied to the government-citizen relationship, if an act or policy arbitrarily dominates the will and autonomy of citizens, thus violating their ability to self-govern (as a collective body of citizens), then these acts or policies are unjustified. This power to remove the potential for domination is Pettit's notion of "antipower" (Pettit, 1996, pp. 576-77). This proposition is part of a larger neorepublican research agenda based on three primary tenants: individual freedom (conceptualized as freedom as nondomination), limited government power over its citizens based on a mixture of constitutionalism and the rule of law (with an emphasis on the importance of the free state promoting the freedom of its citizens without dominating them), and a vigilant commitment by citizens to preserve the freedom preserving structure and substance of their government through active democratic participation (Lovett and Pettit, 2009, p.11).

This argument is closely related to Roberts (2014) (somewhat more communitarian) position that,

> The members of a republican democracy can only realize the ideal of self-government, and be sure that they will enjoy conditions of non-domination, through active participation in the decision-making processes that generate—determine the nature and extent of—the norms that will regulate their conduct. Participation may take various forms, of course—from contributions to discussion on the development of political policies generally, to ex ante contestation of concrete proposals and submission of counter proposals as part of a formal consultation process, and the empanelling of ad hoc citizens' assemblies to generate legislative proposals on issues of fundamental importance. But with membership of a self-governing polity comes the expectation that citizens will, when necessary, set aside private interests and pursue the public good of ensuring that the laws to which individuals are subjected track their common interests (p. 8).

Importantly, Berlin himself noted that his version of negative liberty was not "logically… connected with democracy or self-government," although he admitted that democratic self-government may better guarantee liberty than other forms of rule (Berlin, 1969, p. 177). Berlin noted that, "The answer to the question 'Who governs me?' is logically distinct from the question 'How far does the government interfere with me?'" (Berlin, 1969, p. 177) and, admittedly, some forms of positive freedom might also privilege the value of political engagement and self-government (Swift, 2006, p. 64). Self-government, in the context of neorepublican theory, however, is limited to democratic governance within a society and is distinct, in this regard, from

theories that encompass the self-government of one's own person, in isolation from society, and that are tied to individual self-mastery and an individual's capacity to act autonomously on second-order desires.

Pettit is concerned that the noninterference view limits our potential for appropriate emancipation from domination; in effect, the noninterference position allows too many restrictions on individual liberty and may lead to an apathetic defense of some important freedoms. For example, recent legal challenges to state mass surveillance programs have failed because individuals could not show evidence of actual interference with their privacy rights (see Clapper v. Amnesty International USA, 2013); however, when we consider the *possibility* for such secretive mass surveillance programs to impact state-citizen power relationships and violate individual privacy, the neorepublican approach allows a clear platform from which to challenge claims that citizens should not have standing to sue the government in these cases (Newell, 2014d). Additionally, the noninterference view problematizes the application of law, as even generally freedom-preserving restrictions built into the rule of law constitute interference with absolute liberty (for example, the penalization of premeditated murder). On some accounts, because of its negative focus, neorepublicanism is not necessarily as distinct from liberal commitments as some of its proponents insist. On the other hand, however this argument is spun, the neorepublican continues to recognize the sharp distinction between a slave with a benevolent master and a person not susceptible to the potential domination of a slaveholder (Lovett, 2013, s. 2.1). The neorepublican position, like the liberal one, must also condition its scope based on an underlying recognition of baseline fundamental civil, political, and human rights that should not be negotiable in the political process or overrun by majority governance (see Pettit, 1996, p. 590).

Because power and domination—to some degree—are built into the structure of social and political institutions (e.g. police departments and criminal justice systems), improper or inadequate democratic safeguards against abuse could potentially allow institutions to dominate and subjugate the people systemically. Domination, then, could become institutionalized and integrated into our social and political institutions in a way that creates systemic domination, as well as evidenced in the relationships between agents of government and individuals or groups of citizens.

In analyzing neorepublican freedom in an applied context, as this dissertation attempts to do, three primary questions become crucially important. First, what does it mean for one agent to hold power over and subjugate (or dominate) another? Second, what might emancipation from this power appropriately look like? And finally, what does it mean to conceptualize freedom as nothing more than emancipation from such power – what Pettit calls "antipower"? The following subsections address these questions in turn.

3.2.1.1. Power and domination

Paradigmatically, power and domination are exemplified by slavery. Thus, Pettit argues, "One agent dominates another if and only if he or she has a certain power over the other: in particular the power to interfere in the affairs of the other and to inflict a certain damage" (Pettit, 1996, p. 578). Importantly, the dominating agent must have the actual capacity (rather than merely

"virtual" or unrealized capacity) to exercise arbitrary power over the dominated person(s), and that power must also be capable of inflicting a certain type of harm. For present purposes, the definition of harm, which can be controversial, encompasses situations where a dominating agent acts with benevolent intent. But what must this exercise of power look like, and what type of harm (or damage) is required?

Pettit answers these questions by stating that domination requires the capacity to interfere, with impunity and in an arbitrary fashion, with certain choices that the dominated agent otherwise has the capacity to make (here, "certain" means that the scope of the interference need not impinge on all of the dominated agent's choices, but may be limited to certain choices of varying centrality or importance). Interference requires "an intentional attempt to worsen an agent's situation of choice" (Pettit, 1996, p. 578). Likewise, on Pettit's view, unintentional or accidental interference is not freely exercised subjugation. However, interference does encompass a wide amount of possible actions, including restraint, obstruction, coercion, punishment (or threat of punishment), and manipulation (which includes, in Pettit's view, "agenda fixing, the deceptive… shaping of people's beliefs or desires, [and] rigging… the consequences of people's actions") (Pettit, 1996, p. 579). This characterization could easily be seen as legitimizing interference merely based on benign intent, but note that Pettit is not only concerned with interference as such, but the possibility that such interference *could* occur, given existing power relations. Thus, we must act, not to restrict malicious interference, but to restructure power so that agents do not wield the power to engage in such interference at will. In this case, the possibility of domination is lessened or removed as antipower is increased.

Thus, interference, as Pettit defines it, worsens the dominated agent's position—and causes damage—because it changes the options available to the person or alters the payoffs of the person's choices by allowing the subjugator to manipulate the options and payoffs in play. In this sense, the power-wielding agent has the necessary capacity to interfere. If an agent may act without risk of penalty for interfering—whether from the victim themselves or society at large—the agent would have "absolutely arbitrary power" (Pettit, 1996, p. 580). The only check on the exercise of such power is in the agent itself—in that agent's free and capricious will. Thus, it follows that a person (X) is dominated by another (Y) when X has no recourse (legal or otherwise) to contest actions by Y that interfere with X's situation of choice (and where Y has the actual capacity to engage in such actions)[8]. Thus, going back to the earlier example, because widespread state surveillance of the communications of its citizens has the potential to interfere with individual citizens' situations of choice (for example, by chilling free expression), this relationship exhibits domination. When governments collect information about personally identifiable individuals (especially citizens), and then disclose this information broadly (such as under public records laws) for reasons that do not necessarily increase freedom or promote antipower, this release of information can also diminish a person's ability to make autonomous choices. These cases need to

[8] Exceptions will exist, of course, such as when the only otherwise dominating aspect of Y's act is required to keep X from violating the rights of another person.

be examined carefully, so that we can develop a theoretical basis for balancing the competing interests in speech, disclosure, and individual privacy.

3.2.1.2. Antipower and emancipation

Discussing the domination of the powerless may lead us to question what we can or ought to do to diminish or remove the subjugation. Reversing roles would not solve the problem, but would merely relocate it (Pettit, 1996, p. 588). Fairly allocating power to both sides, on the other hand, does not just merely equalize the subjugation; if both sides—say the people and their government—may interfere with the other's affairs, then neither may act with impunity since the other may exact something in return (Pettit, 1996, p. 588). Thus, "neither dominates the other" (Pettit, 1996, p. 588). This is an exemplification of antipower. According to Pettit, "Antipower is what comes into being as the power of some over others—the power of some over others in the sense associated with domination—is actively reduced and eliminated" (Pettit, 1996, p. 588). Antipower, then, subjugates power and, as a form of power itself, allows persons to control the nature of their own destiny (Pettit, 1996, p. 589); in this sense it functions much like rights do more generally. This makes sense when antipower essentially encompasses the conditions necessary and sufficient for freedom to exist. When these conditions obtain, the "person enjoys the noninterference resiliently" because they are not dependent on the arbitrary use of power, precisely because they have the power to "command noninterference" (Pettit, 1996, p. 589). As such, they enjoy some measure of freedom.

Much of this work can be accomplished by instituting legal frameworks that insist on equal rights, due process, and fairly applied laws, but I think the neorepublican philosophy can help provide reasons and direction in support of these ends. In the cases of body-cameras, the right to record, and ALPR, popular access to information about government action and government surveillance programs can act as a form of antipower to reduce domination. However, the release of some personal information as part of these transparency processes may also deter active disclosure requests (at least by those with something to lose by disclosure) or shift dominating power to external (i.e. non-government) entities, such as employers, advertisers, and other private interests, who may then analyze and act on available information to alter the potential payoffs and opportunities afforded certain individuals.

To promote antipower, and reduce domination, we can protect the powerless against the powerful by regulating the use of the powerful agent's resources or by granting the powerless new resources. This could involve creating or empowering protective institutions and the "nonvoluntaristic" rule of law (characterized by constitutional governance and associated protections for minorities). The rule of law itself could be used as a form of power, and thus provide legal incentives to avoid interfering with the lives of others (for example, through an effective criminal justice system) and "generality, transparency, nonretroactivity, and coherence," based on constitutional guarantees can help limit this possibility (Pettit, 1996, p. 590). Regulating the resources of the powerful might also include checks on and separations of power, regular representative elections, democratic participation, limited tenure of government officials, providing access to independent courts or

other bodies with powers to review government action, and open access to information (Pettit, 1996, p. 591).

Of course, fully eliminating domination may not be always be easy, or even completely possible, and antipower may exist in varying degrees, based on how much power a person (or group of people) can effectively wield to command noninterference or limit domination. Commanding noninterference may require collective action, and this theory admittedly relies on the presence of institutions as means to administer government and facilitate the peoples' claims. This does not mean, however, that we ought to be complacent, or even limit our concern to reducing actual interference. On the contrary, if an act or policy of an institution or agent of government arbitrarily dominates the will and autonomy of citizens, thus violating their ability to effectively self-govern, then these acts or policies and are unjustified.

As stated above, governments must allow their citizens enough access to information necessary for individual self-government. To be fully non-arbitrary and non-dominating, government must also respect and provide effective institutional and legal mechanisms for their citizenry to effectuate self-government and command noninterference. Establishing liberal access rights to information about government conduct and mechanisms that ensure that citizens can effectively command noninterference are justified on the grounds that they reduce the possibility of arbitrary, and actual, interference with the right of the people to govern themselves. Such measures, when properly balanced against legitimate privacy interests, would also limit the institutionalization of systemic domination within political and social institutions.

3.2.2. Privacy

Privacy is a particularly useful instrumental means of supporting the goal of maintaining individual liberty from government intrusion, interference, and/or domination (or from private actors, for that matter). Privacy is a "core value that limits the forces of oppression" (Moore, 2013). Talk of liberty, without including privacy as a specific element of concern, shortchanges the very nature of such liberty itself. Thus, I believe this conception of privacy is consistent with the claim that "privacy… is a necessary condition for human well-being or flourishing" (Moore, 2013; 2010); that privacy has objective moral value, though its contours might be relative to culture, religion, time, etc. (Moore, 2010). Conceptualizing privacy as a necessary and freedom preserving right protects individuals from intrusions well beyond the basic privacy interests in territoriality and a need for space away from overcrowding (see Westin, 1967, p. 8; Moore, 2013). Privacy rights should also be protected against expression to a greater extent than American law currently suggests. Westin (1967) stated that, "the achievement of privacy for individuals, families, and groups in modern society has become a matter of freedom rather than the product of necessity" (pp. 21-22). Like Cohen (2013), I also argue that "freedom from surveillance, whether public or private, is foundational to the practice of informed and reflective citizenship" and that "privacy… is an indispensable structural feature of liberal democratic political systems" (p. 1905; see also Roberts, 2014).

3.2.2.1. Defining privacy

Privacy has been defined in a multitude of ways, both normatively and descriptively (see Moore, 2010, and Solove, et al., 2006, pp. 40-51, for examples and additional citations). Solove goes so far to claim that defining privacy is a fruitless task because, like liberty, privacy means so many things to different people (see Solove, 2006; see also Post, 2001, p. 2087; Allen, 2011, p. 3; Thompson, 1975, p. 295). As stated succinctly by Cohen, "privacy has an image problem" (Cohen, 2013, p. 1904). The umbrella term "privacy" contains both the concept of what privacy is and how it should be valued, as well as a (generally) narrower right to privacy which outlines the extent to which privacy is legally protected (Solove and Schwartz, 2009, p. 39; Gross, 1967, p. 36). Westin stated that "privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve" (Westin, 1967, p. 7). Privacy has also been conceptualized in reductionist (privacy as an element of another more fundamental right) and non-reductionist (privacy as a distinct right in itself) terms (Moore, 2010, pp. 14-16).

Westin famously defined 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. 7). This definition is similar in many respects to the one I endorse, and Westin's work contributes valuably to my conception of privacy. On its face, Westin's definition does not necessarily extend to subsequent use of information previously disclosed or communicated, but limiting the extent of communication could also arguably encompass more than just initial disclosure. It is phrased in terms of a moral (or legal) claim (a normative position), but its inclusion of groups and institutions places it beyond the ambit of merely an individual right. Defining privacy in terms of control also supports self-development and autonomy (Moore, 2010, p. 17) (albeit a certain sort of autonomy (see Cohen, pp. 1905-1909)).

In response to the existing ambiguity surrounding how to define privacy, Allen (2011) has described five different meanings of privacy (physical, informational, decisional, proprietary, and associational), and Solove (2006) has developed a taxonomy of informational privacy violations (broken into four major categories: collection, processing, dissemination, and invasion). These classifications are undoubtedly helpful in understanding the broad scope of what is meant by "privacy," or how privacy has, in fact, been protected in the past. However, I believe a normative theory of privacy, or liberty for that matter, can be very useful for thinking about what privacy rights ought to encompass (or at least what a system of democratic governance should provide for an engaged citizenry to determine for themselves what choices re privacy they wish to live under). This undertaking constructs, as I see it, a primarily individualistic conception of privacy and its value—rather than something approaching Etzioni's liberal communitarianism theory—though it

does place some importance on collective (rather than merely individual) self-governance[9] as an instrumental means to preserving privacy as a restraint on domination.

In this project, I define informational privacy as the right to control access to and uses of personal information (Moore, 2010, p. 16). This normative definition includes the right to control both initial and subsequent uses of personal information (e.g. a person may consent to the use of the personal information for certain purposes by specified entities, but may object to further sharing and subsequent use for additional purposes outside the scope of the original consent). This definition, despite its clear connections to liberal individualist and libertarian thinking,[10] also resonates with aspects of both liberal communitarian and republican thought. Specifically, the importance on placing or allowing restrictions on subsequent (or secondary) access to or uses of personal information has been clear in work by Etzioni (2014)[11] and is also implicit in arguments for adopting the mosaic theory (see e.g. Slobogin, 2012; Dickman, 2011; United States v. Maynard, 2010; Etzioni, 2014, p. 643).

A narrow view of what privacy as "control" means might be critiqued on the basis that individuals might not have the power or ability to actually exert control. Additionally, in private/corporate contexts such as when individuals share personal information with a corporate interest (e.g. Google, Microsoft, Amazon, or Facebook), individuals might have "consented" to broad language about data usage and downstream external use of their information by merely clicking a button—a situation that some feel foretells the failure of the control hypothesis. Julie Cohen is particularly suspicious of at least a narrow reading of control-based definitions of privacy (Cohen, 2013, p. 1906). According to Cohen (2013), privacy cannot "be reduced to a fixed condition or attribute (such as seclusion or control) whose boundaries can be crisply delineated by the application of deductive logic," but is rather dynamic and "shorthand for breathing room to engage in the processes of boundary management that enable and constitute self-development" (p. 1906). Privacy decisions by the European Court of Human Rights (ECtHR) finding protectable rights to privacy in private activities occurring in public spaces (e.g. Von Hanover v. Germany, 2004) enable this sort of boundary management function and, in conjunction with a theory of free speech limited to democratic self-governance (see my discussion of this in the following subsection, 2.1.2.3.), are consistent with the neorepublican theory of freedom outlined above.

Calo's (2012) concept of "visceral notice" is also helpful as means of explaining how notice and consent might be bolstered by integrating innovative ways of informing consumers about a product's access to and use of an individual's personal information into the "very experience of a product" (p. 1027). Calo (2012) approaches the topic from the position that, "experience as a form

---

[9] This admittedly bears some relation to Etzioni's (2014) comments about the need to balance privacy with other common goods or the broader public interest (see p. 651).

[10] See for example, the broader context and arguments presented by Moore (2013; 2010; 2007).

[11] Etzioni (2014) states that, "the greatest current threats to privacy come not at the point that personal information is collected, but rather from the secondary uses of such information" (p. 641).

of privacy disclosure is worthy of further study before we give in to calls to abandon notice as a regulatory strategy in privacy and elsewhere" (p. 1027). In this vein, "[t]echnology and clever design create the possibility of tailoring anecdotes to individual consumers, thereby showing them what is specifically relevant to them, instead of describing generally what might be" (Calo, 2012, p. 1042).[12] This strategy also helps confront arguments that control-based theories of privacy are unsatisfactory because, in practice, civilians may lack the actual capacity to control access to and uses of their information.

However, my concerns in this dissertation are more limited, and I don't think it necessary to completely resolve all of the possible objections at this juncture. I think a control-based definition can adequately cover these scenarios as long as we begin with the baseline assumption that privacy rights (both *access* and *use* considerations) are presumptively set restrictively. Phrased differently, individuals must clearly *opt-in* to both access and uses of their personal information—and they must do so with documented and informed consent. Absent clear and informed consent, the state should be empowered (and required to) to protect citizens against violations of their privacy that would result in domination by the state, corporate interests, or other private individuals.

3.2.2.1. The value of privacy

At some level, I claim that privacy ought to involve some culturally relative socio-political choices vis-à-vis the legitimate exercise of power of the state (or other persons) over the individual. However, a certain and substantial core ought to be protectable absent reducibility to any other value, including liberty. In practice, it is clear that the right to privacy (in some current instantiations) is instrumentally connected with restraining government power (e.g. consider the Fourth Amendment prohibition on unwarranted searches and seizures). Helen Nissenbaum (1998) has similarly noted that, "privacy is an important means by which individuals may sustain power, liberty, and autonomy against potentially overwhelming forces of government" (p. 569). This approach also extends to protecting individuals from domination by other private parties, and is not restricted to government domination. However, as Moore (2010) suggests, a reductionist account of privacy "might mean jettisoning the idea" of a distinct right to privacy altogether in favor of focusing on the more fundamental concept—e.g. liberty. Frederick Davis (1959) has also argued that a reductionist account may also make advocating for privacy rights irrelevant as long as more fundamental rights are adequately protected (Davis, 1959, p. 20; Moore, 2010, p. 15). Moore (2010) is somewhat critical of the reductionist premise, suggesting that "it is unclear whether or not privacy is reducible to more 'basic' rights" (though he does not object outright), but he does note the "close connections" between privacy and liberty (p. 15).

Indeed, as Alan Westin (1967) explains, humanity may share some basic universal need for privacy (although it may surface differently in various cultural contexts), and this might also extend to other animal species as well (see also Moore, 2013; Newell, Metoyer, and Moore, 2015). This

[12] This argument has also been featured in others discussion about incorporating privacy into the design of technologies (see Hartzog and Stutzman, 2013, pp. 413-414).

may well exist as an independent human value that ought to be protected by law (e.g. as a fundamental human right). However, this need for some basic level of privacy protections may be more limited than some modern conceptions of privacy (and it is likely to be at least partially related to physical privacy concerns (see Westin, 1967; Moore, 2013)). In modern society, "our contemporary norms of privacy are 'modern' and 'advanced' values largely absent from primitive societies of the past and present" (Westin, 1967, p. 11). These "advanced" values are more likely embedded in the "socio-political realm" (Westin, 1967, p. 21) and, I would argue, privacy's instrumental connections to political liberty is important for human flourishing but not necessarily indicative that all of this privacy is reducible to liberty. This characterization allows us to agree on a possible core, universal, right to privacy (which humans may share across different cultures, and even with other animals), while recognizing that some privacy interests are also culturally and individually distinct choices about values. Robust privacy rights should be promoted by democratic civic participation, self-governance by the people, and the promotion of liberty (aka nondomination) buttressed by constitutional guarantees of equality, due process, and limits on pure majoritarian decision-making to preserve minority rights. In this way, these political protections are also likely to cover the more basic privacy rights. This result, in my view, also helps account for varying valuations of privacy across time and cultures.

Roberts (2014) has only recently provided the first explicitly republican modern theory of privacy, though other writers like Cohen (2013) and Etzioni (2014) have also provided alternatives to privacy theories based in liberal individualism. According to Roberts (2014),

> the value of privacy for republicans lies in its capacity to shield individuals from the threat of domination. A consequence of loss of one's privacy is that others may acquire dominating power—the capacity to interfere in one's decisions on an arbitrary basis (p. 2).

If we connect this basic republican conceptualization to Moore's (2010) claim that the value of privacy is based on its ability to enable human flourishing, we can develop a position that sees privacy (as control over access and use) as directly connected to human flourishing precisely because it reduces domination and increases antipower.[13] This dual focus on simultaneously promoting human flourishing and reducing domination is subsequently benefited by privacy theories that would decrease unwanted visibility—whether conceptualized as the desire for separation from others (Moore, 2010; Westin, 1967), obscurity (Hartzog and Stutzman, 2013a; 2013b; Selinger and Hartzog, 2014; 2013), semantic discontinuity (Cohen, 2012; 2013), or the mosaic theory (Slobogin, 2012; Dickman, 2011; United States v. Maynard, 2010; see also Kerr, 2012). The personal autonomy necessary to carry out our own personal life projects and to engage in democratic deliberation and self-governance is hindered by domination and, without robust

[13] Roberts (2014) also recognizes, citing Moore (2010) and Westin (1967), that "there is no reason to think that republicans would reject" the claim that "it is part of human nature to seek a degree of separation from others in some circumstances, and that such separation is essential to human flourishing" (Roberts, 2014, p. 9).

antipower, individuals are "likely to be incapable of exercising the kind of political autonomy that is required" (Roberts, 2014, p. 3) for human flourishing and republican self-government.

Cohen's (2012; 2013) concept of *semantic discontinuity* resonates with much of the broader republican theory of privacy and access to information I argue for in this project. Cohen developed the concept of semantic discontinuity as an important component of her broader theory of personal freedom and human flourishing (see Cohen, 2012, p. 6; see also Balkin, 2012, p. 81). In terms of her larger theory of human flourishing, Cohen explicitly connects herself to the capabilities theory of Martha Nussbaum (2000, pp. 70-96) and Amartya Sen (2004, pp. 330-338) and extends that theory to the "networked information society" (Cohen, 2012, p. 6). Ultimately, Cohen elaborates three key ideas necessary for human flourishing:

> information law and policy should foster institutional and technical structures that promote *access to knowledge*, that create *operational transparency*, and that preserve room for the *play of everyday practice* (Cohen, 2012, p. 6 (emphasis added); see also Balkin, 2012, p. 81).

Semantic discontinuity itself refers to "gaps and inconsistencies within systems of meaning, and to a resulting interstitial complexity that leaves room for the play of everyday practice" (Cohen, 2012, p. 224). Balkin (2012) takes this to mean that,

> Although Cohen initially states this idea in terms of meanings, it soon becomes clear that she is talking about gaps in enforcement and in systems of surveillance and control. That is because systems of meaning in a networked environment are also systems of control and surveillance…. Therefore, 'semantic discontinuity' means 'interstitial flexibility within the system of legal rights, institutional arrangements, and associated technical controls.' Semantic discontinuity means discontinuity in forms of social and technical power. It 'is the opposite of seamlessness: it is a function of interstitial complexity within the institutional and technical frameworks that define information rights and obligations and establish protocols for information collection, storage, processing, and exchange' (p. 81, *quoting* Cohen, 2012, pp. 234, 239).

Thus, in practical and institutional terms, "Semantic discontinuity involves gaps and imperfections in systems of control and surveillance" (Rich, 2014, p. 928)—also referred to as "disorganization" (Miller, 2014, p. 134)—because these gaps and imperfections make space for the play of everyday practice to occur. This also requires legal and institutional mechanisms that would avert the "perfect preventive state" (Rich, 2014, p. 928), implicating tensions with efficiency and accuracy in criminal justice and law enforcement.[14]

[14] These aspects of Cohen's theory come into fairly direct conflict with Etzioni's (2014) communitarian position that would prioritize public safety as an important common good. Indeed, Cohen herself directly tackles the liberal communitarian position when she states that, "Privacy's goal, simply put, is to ensure that the development of subjectivity and the development of communal values do not proceed in lockstep" (Cohen, 2012, p. 150; Cohen, 2013, p. 1911).

As an additional requirement, Cohen (2012) also advocates that, "the politics of 'access to knowledge' should include a commitment to privacy, and why a commitment to human flourishing demands a more critical stance toward the market-driven evolution of network architectures" (p. 6). Her claims in relation to access to knowledge are, in many ways, interconnected with my own arguments in favor of access to government information developed herein (see also Newell, 2014b; 2014c; 2014d). In Cohen's view:

> without the raw materials necessary for social and cultural participation, one cannot participate meaningfully in the development of culture and community, and without access to the appropriate networks and tools, one cannot partake of the resources that the networked information society has to offer (Cohen, 2012, p. 224).

Finally, Cohen's idea of *operational transparency* refers to the requirement that individuals "know how they are situated in code and technologies, what is being done to them, how code and technology limit their actions and choices and why" (Balkin, 2012, p. 81, *citing* Cohen, 2012, pp. 224, 234-235). This requirement is "designed to put users themselves in a better position to engage in processes of boundary management" (Cohen, 2012, p. 224)—arguably with significant ramifications for the individual ability to become informed and exercise effective control over access to and uses of their personal information.[15]

On the other hand, the concept of privacy as *obscurity* (Hartzog and Stutzman, 2013a; 2013b; Selinger and Hartzog, 2014; 2013) also resonates with many of these same concerns, as it focuses on identifying the "fundamental ways information can be obtained or kept out of reach, correctly interpreted or misunderstood" (Selinger and Hartzog, 2014, p. 1). Obscurity as an analytic concept has also arisen as a response "to increasing frustration with the theoretical and practical limits of traditional privacy theory" (Selinger and Hartzog, 2014, p. 1), and work by Hartzog, Stutzman, and Selinger (Hartzog and Stutzman, 2013a; 2013b; Selinger and Hartzog, 2014; 2013) has provided discussion of useful practical, methodological, and technological solutions to combat increasing visibility by making personal data more obscure. Some of this work also aims to increase obscurity (privacy) by incorporating it into the design process itself (Hartzog and Stutzman, 2013), much like the vision of Value Sensitive Design. In one piece, Hartzog and Stutzman (2013) outline a doctrinal model for obscurity (in the context of internet communications):

> Information is obscure online if it exists in a context missing one or more key factors that are essential to discovery or comprehension. We have identified four of these factors: (1) search visibility, (2) unprotected access, (3) identification, and (4) clarity. The presence of these factors diminishes obscurity, and their absence enhances it. Thus, in determining whether information is obscure online, courts should consider whether any of these factors were present. Information that is entirely unobscure is completely obvious, and vice versa. Courts should engage in

[15] Calo's (2012) concept of "visceral notice" is also relevant and useful here.

> a case-by-case analysis of the factors to determine the degree of online obscurity (p. 48).

This model "could serve as a metric for the boundary of allowable disclosure by information recipients" and might take the shape of "some form of mandated obscurity" (Hartzog and Stutzman, 2013, p. 48).

Harkening back to Moore's (2010) qualified acceptance of Taylor's (1989) 'plan of life' conception of what it means for a life to be flourishing, we can see the importance of privacy at allowing us to be "project pursuers" (Moore, 2010, p. 42). Some of Julie Cohen's ideas also resonate with this line of reasoning. Cohen claims that privacy:

> shelters dynamic, emergent subjectivity from the efforts of commercial and government actors to render individuals and communities fixed, transparent, and predictable. It protects the situated practices of boundary management through which the capacity for self-determination develops (Cohen, 2013, p. 1905).

These conclusions also appear consistent with the mosaic theory of the Fourth Amendment (discussed in Chapter 4, *infra*) in that it would shelter warrantless state access to aggregated information about individuals that can be used to "render individuals and communities fixed, transparent, and predictable," as Cohen (2013, p. 1905) describes, even when each smaller piece of information might be such that it would not be protectable absent aggregation.[16] Cohen also argues that, "privacy incursions can be episodic or systematic, but systematic deprivations of privacy also facilitate episodic privacy incursions" (Cohen, 2013, p. 1905). Seen this way, invasions of privacy involving access to or use of aggregated pieces of personal information (a systematic incursion) also has the potential to constitute a new, episodic, intrusion. The analysis of whether privacy has been violated in that case should not be dependent on examining the collection of each individual piece of independently sourced personal information in the sequential fashion traditionally employed in Fourth Amendment cases as outlined by Kerr (2012), but by whether the access to or use of the aggregated information has qualitatively changed the nature of the new episodic intrusion. The "use" limitation explicit in the above definition of privacy would be violated in these cases.

On the other hand, Cohen's preference for the subjectivity in understanding "selfhood" and social shaping probably (see Cohen, 2013, p. 1909) would fit better within the 'plan of life' (Taylor, 1989) theory of human flourishing than within Moore's more balanced approach that maintains a place for essentialism as limit to subjectivity (Moore, 2010, p. 42). This, in my view, makes Cohen's theory—much like Nissenbaum's (2004) contextual integrity—more useful in understanding human experiences, norms, and expectations than in helping to establish a more general baseline to enable legal protections (which is more limited it its ability to cater to individual

[16] Though, obviously, it can be difficult to determine how much aggregation is too much.

subjectivity[17]). Privacy law should be reactive to subjective experience to the extent that it can generalize such experience in a way that can apply fairly to a broad citizenry with drastically divergent life experiences. Cognitive and behavioral sciences are undoubtedly important to ensuring privacy laws act in ways that are supporting human flourishing, but the law cannot cater to the subjectivity of myriad selfhoods. What we need is an arrangement that allows individuals to autonomously enact their own projects (to play as part of their own everyday practice, in Cohen's (2012; 2013) terms), based on their own subjectivity but limited by the rights of others, without the risk of domination. A theory of antipower that accounts for both privacy and access to information, as outlined above, ought to be a sufficient condition to achieve this outcome.

3.2.2.2. The boundaries of privacy (and privacy harms)

A legal privacy right based in control, but with a default presumption of that individual have not waived or consented to access or uses of their personal information (as described in the next paragraph), combined with a republican conception of the freedom such privacy ought to afford, enables—in my view at least—a way around some of Cohen's criticisms. For example, Cohen argues that liberal theories of privacy based on reductionist "core principles," cannot explain why disclosing personal information to a few friends does not equate to sharing with others (e.g. employers, corporations, government). When we consider to whom the individual consented to share information with (a few friends) the risk for dominating influence is qualitatively different than if the state acquired that information. By not presuming that consent has been extended beyond the initial grant of access (i.e. further use has not been consented to), we could, for example, argue against the appropriateness of the third party doctrine in Fourth Amendment law because the exception violates our initial set of presumptions about consent and waiver. Additionally, it is exactly the premise of the republican theory of privacy that greater visibility (access) or use of this personal information directly implicates domination. This republican position, in opposition to most liberal theories, also explains why this domination (and violation of privacy) is possible when 1) no actual interference has occurred and 2) the individual doesn't even know that the information has been accessed or used (see Roberts, 2014, pp. 13-14), such as in cases of covert or secret surveillance by states or corporations—and including the *possibility* of unconsented-to downstream sharing and use of personal information by third-parties. As such,

> the loss of privacy we suffer when others watch or acquire information about us is harmful to the extent that it provides others with power to interfere in our decisions that we do not control—the power to remove, replace or misrepresent options that would be available to us had we not suffered a loss of privacy. This harm arises whether or not we are aware that others are watching or acquiring information about us (Roberts, 2014, p. 16).

[17] This is not to say that morality ought to track legal regulation in this context, as it may well be morally suspect to violate known subjectively held values of others. However, law and morality, in this case as well as many others, need to be treated separately as distinct considerations.

Likewise, Daniel Solove (2201) has argued that, the primary problem that state or commercial databases of personal information create, "emerges from subjecting personal information to the bureaucratic process with little intelligent control or limitation, resulting in a lack of meaningful participation in decisions about our information" (p. 1422), which also "foster[s] a state of powerlessness and vulnerability" (p. 1423). The existence of these expansive databases of information about individuals increases civilian visibility, defeats obscurity, and violates the concept of semantic discontinuity. Specifically, it exhibits the characteristics of *domination* and calls for an increase in *antipower*.

Additionally, perhaps we should not restrict our analysis to describing the appropriate boundaries of governmental collection and use of personal information, but also to examining the idea that the mere possibility (or individual/public perception) of surveillance may implicate chilling effects on lawful individual action. As such, the argument goes, surveillance itself need not actually occur for liberty and privacy to be impacted. In a Potemkin village full of (dummy) ALPR and red light cameras, body- and dashboard-cameras, CCTV, and drones, we might expect citizens to experience a chilling effect on the exercise of their rights to engage in certain lawful activities, such as politically motivated speech or planned non-violent protest. Along these lines, Ryan Calo (2011) has outlined what he calls the *subjective* and *objective* categories of privacy harm (p. 1133). In connecting his argument to the control theory of privacy, Calo (2011) ties *objective* harms to the "adverse consequence[s]… that flow[] from the loss of control over information or sensory access" and *subjective* harms to the "perception of loss of control that results in fear or discomfort" (p. 1143). Calo's (2011) definition of subjective privacy harms extends to "the perception of unwanted observation, broadly defined" (p. 1144). According to Calo (2011), "Watching a person directly—their body, brain waves, or behavior—is observation. So, too, is reading a report of their preferences, associations, and whereabouts" (p. 1144). However, in contrast to harm accruing by the fact that another entity has obtained the power to interfere arbitrarily (the republican position), Calo (2011) argues that subjective privacy harm does not require *actual observation* (p. 1142).

This scenario necessarily evokes the case of the Potemkin village. At first glance, this situation does seem to generate some pause and suggest that this reality could chill expressive freedoms—and generate subjective perceptions of potentially unwanted observation. However, it appears that the harms associated with such perception would need to be built on a foundation of secrecy. As soon as the citizenry at large became aware that all the cameras were fakes and that nothing was actually being recorded, the impact would lessen, eventually becoming negligible under a continuing state of state transparency.[18] If we institutionalize a certain level of transparency based on these same republican principles, as I attempt to advocate in my larger argument in this dissertation, it is not clear that a Potemkin village would be possible—or at least fewer chilling

[18] A case where the mixed deployment of real and dummy cameras, together, caused this chill in the expression of civil liberties would, however, present more difficult problems. Additionally, I am not saying that the Potemkin scenario could never constitute some form of domination; rather, with the level of transparency I am arguing for, the dominating effects would be limited.

effects would occur if it were obvious to everyone in the community at the outset that the cameras were all fakes. In any case, I am not prepared to extend my conceptualization of relevant harms to individualized subjective (and possibly unreasonable or irrational) perceptions of surveillance when no other entity has actually acquired the power to interfere arbitrarily or when the subjective perceptions—regardless of actual information collection—are irrational and not developed through some process of logical reasoning (i.e. the existence of dummy cameras would legitimize subjective privacy harms to some extent because it would raise reasonable questions about whether any information was actually being collected). Rather, the "loss of privacy" is "harmful to the extent that those who watch or collect the [personal] information" about another person actually acquire the power to interfere arbitrarily, whether or not the person is aware of any access (Roberts, 2014, p. 16) and whether or not information is actually collected. Under this conceptualization, privacy would not actually be violated in cases of non-observation (except when objective factors provide a basis or questioning whether observation was in fact occurring), but it would support findings of violation when actual observation had occurred in secret. Aligning privacy rights with rules about robust access to information rights under an umbrella of republican political philosophy allows us to avoid problems associated with the chill of rights in a Potemkin village filled with fake surveillance apparatus.

On the other hand, Calo's (2011) definition of the *objective* category of privacy harms is quite helpful—but ultimately not as inclusive as a republican conception. Objective harms are defined as "the forced or unanticipated use of information about a person against that person" (p. 1143).

> Objective privacy harms can occur when personal information is used to justify an adverse action against a person, as when the government leverages data mining of sensitive personal information to block a citizen from air travel, or when one neighbor forms a negative judgment about another based on gossip. Objective harms can also occur when such information is used to commit a crime, such as identity theft or murder. To constitute harm, the use must be *unanticipated* or, if known to the victim, *coerced*. Again, however, no human being actually needs to see the personal information itself for it to be used against the victim (Calo, 2011, p. 1143).

Importantly, under this objective category, the possibility that no human being sees the information does not suffer the same objection as presented in the case of subjective perception without any actual observation. This definition would seem to include only cases where interference had actually occurred—whether known or unbeknownst to the individual herself—because it explicitly requires some use of the information to the detriment to the individual, thus satisfying both the liberal test for actual interference and the republican claim that even secret surveillance can be problematic.

3.3. Free speech and access to information

The First Amendment states, in part: "Congress shall make no law . . . abridging the freedom of speech" (U.S. Const., amend. I). Just as privacy is subject to numerous definitions and overarching theoretical accounts, the theoretical basis for a right to free speech and expression (and broader

First Amendment rights, such as the rights of assembly, association, and belief) has also been much debated. Greenawalt (1995) provides a good account of the major bases for protecting free speech, categorized as consequentialist or non-consequentialist reasons. Of these, a few consequentialist justifications are particularly relevant to my approach to understanding the proper role of the First Amendment's free speech guarantee. There are more possible justifications than those presented below, as I have chosen to limit my discussion to those I feel are most clearly implicated by my overall theoretical commitments, namely that free speech should be seen as protecting speech that promotes truth discovery, checks on abuse of power, and democratic deliberation.

First, the basic consequentialist justification for free speech is the importance of "truth discovery" (Greenawalt, 1995, p. 281; see also Mill, 1859; Whitney v. California, 1927 (Brandeis concurrence)). This justification, in my view, holds importance to both liberal and republican conceptions of free speech. The idea that an open marketplace of ideas, where individuals have the ability to present ideas without risk of censure, may stimulate debate, critical thought, and the eventual collective discovery of truth is obviously important, regardless of whether or not we ought to limit the protected sphere to only those ideas related to collective self-governance (and whether or not "truth" always rises to the top). Mill (1859), in particular, was concerned with the potential for governments to suppress communication and to make us dependent on them, undermining self-government, because even attempts to suppress "false" information may well also capture true or partly true information and would hamper the development of the open marketplace of ideas. To a great extent, this viewpoint has been captured by the liberal tradition, and Volokh's (2000) passionate defense of free speech in the face of potential privacy restrictions (which he largely see as unwarranted and dangerous), pushes this justification close to its limits. To others, such as Solove (2003; Solove, et al., 2006, p. 147), Meiklejohn (1961; 1960; 1948), Post (1997; 1995; 1993), Baker (1978; 1989), Sunstein (1992; 1993), and Reddish (2013; Reddish and Mollen, 2009), speech of merely private concern, that does not implicate or further efforts to effectuate democratic self-governance, may be appropriately limited. This view (or actually, views, as these authors do not always agree) also relies heavily on the truth discovery justification for free speech, but it places limits on the types of speech that ought to fall within Constitutional protections. For example, Meiklejohn (1948; 1960; 1961) differentiates between "communication" and "speech" (which, as a subset of communication, impacts self-government). Others have differentiated between high- and low-value speech. Meiklejohn's conceptualization allows us to protect speech (communication that impacts self-governance) but doesn't negate the ability to regulate or limit communication—for example, based on privacy grounds.

Closely connected to (and potentially contained within) the truth discovery rationale is a second line of reasoning: that free speech provides a check on abuses of (especially government) authority (Greenawalt, 1995, p. 282-83; Blasi, 1977; Moore, 2013). This checking power extends beyond checking abuse, however; it also rests on the assumption that the First Amendment should support the exposure of wrongdoing—which implicates the right to gather and access information as a predicate for actual speech. This theory also has ties to the democratic governance theories described below.

Third, the idea that free speech contributes to the development and maintenance of democratic rule (as mentioned above) has also been very influential. Some of these theories can appropriately be termed republican in nature. The primary democratic theories of the First Amendment have been promulgated by Alexander Meiklejohn (1961; 1960; 1948), Robert C. Post (1997; 1995; 1993), C. Edwin Baker (1978; 1989), and Cass R. Sunstein (1992; 1993). Martin Reddish (2013; Reddish and Mollen, 2009) has recently provided another democratic theory to the mix, sharply criticizing the prior accounts as being too focused on collectivist cooperation, rather than protecting individual self-interest. Reddish (2013) advocates an individualistic account of the purposes of the First Amendment that specifically promotes the individual right to speech and organize in a person's own self-interest as a way to incentivize political participation. Meiklejohn and Post, on the other hand, promote more collectivist and cooperative democratic participation, with differing emphases on voting and individuals recognizing themselves as self-governing, respectively, as the ends to be achieved.

Sunstein (1992) focuses on the connections between Madison's conception of American sovereignty (in the People) and the right of free speech. This right to "freely examin[e] public characters and measures, and of free communication among the people thereon" is "the only effectual guardian of every other right" (Sunstein, 1992, p. 257). In Sunstein's (1992) view, current First Amendment jurisprudence "protect[s] speech that should not be protected" because its theoretical basis is "off the mark" and even threatens democratic efforts of the people to self-govern (p. 257). Meiklejohn (1961) argued that, "the First Amendment does not protect a "freedom to speak," rather, "it protects the freedom of those activities of thought and communication by which we 'govern'" (p. 255). Thus, the First Amendment right to free speech concerns "a public power [and] governmental responsibility" rather than "a private right" (Meiklejohn, 1961, p. 255). Meiklejohn (1961) was primarily concerned with the power, and obligation, of the people to vote, but also found that "people do need novels and dramas and paintings and poems, 'because they will be called upon to vote'" (p. 263). In a similar vein, Justice Brandeis, in Whitney v. California (1927), stated powerfully:

> Those who won our independence believed that the final end of the State was to make men free to develop their faculties, and that, in its government, the deliberative forces should prevail over the arbitrary. They valued liberty both as an end, and as a means… that, without free speech and assembly, discussion would be futile; that, with them, discussion affords ordinarily adequate protection against the dissemination of noxious doctrine; that the greatest menace to freedom is an inert people; that public discussion is a political duty, and that this should be a fundamental principle of the American government" (Whitney v. California, 1927, p. 375).

Jack Balkin (2009) argues that the First Amendment's free speech principle is about more than just democracy (qua voting), and he would extend it to encompass what he calls "democratic culture," meaning, "a culture in which ordinary people can participate, both collectively and individually, in the creation and elaboration of cultural meanings that constitute them as individuals" (p. 438). I read this claim as related to (and potentially consistent with) Meiklejohn's

(1961, p. 263) extension of free speech rights to the creation of novels, dramas, paintings, and poems—which Meiklejohn believes are necessary to educated and informed voting and political participation. According to Balkin (2009), democratic culture is "about individual liberty as well as collective self-governance" (p. 3). However, if we extend free speech rights to democratic culture, which I think we should to some extent, rather than just democratic political participation, we also run the risk of having speech interests butt up against privacy more frequently—and we may have to create a more complicated balancing mechanism.

Thus, in my view, the First Amendment (and the aspects of freedom of information laws that are related to free speech concerns), is inextricably tied up in notions of self-government, truth discovery (at least when restricted to matters related to governing or, if not, those that do not invade another person's privacy), checking potential government abuse or domination, and, to some extent, allowing individuals to participate in the creation of culture and meaning within society. That said, we should recognize robust rights to gather information, the ability to withdraw and contemplate or discuss openly and debate ideas in public, to think and believe as each sees fit, and to assemble for these purposes, insofar as such activity does not violate another person's rights (including the right to privacy). However, speech that does not promote, facilitate, or relate to self-government may need to give way to privacy rights.

3.4. Privacy in public

A clear problem for an absolute right to control the initial release and the subsequent use of personal information is implicated when the information is voluntarily exposed to public view (or is subject to public access, even if not openly exposed). Whether something in the public realm can (or should) be protected as private information and protected by legal rules has been the subject of much academic and judicial debate.[19] Philosophical theories of privacy have primarily focused, with valid reasons, on privacy interests in sensitive and intimate information that have not been disclosed voluntarily to the public (see Solove, et al., 2006, p. 39). That is, privacy, to some, only protects information kept carefully within the "private" realm (Nissenbaum, 1998, p. 568). The distinction between the public and private realm has also been explicitly invoked in the work of John Stuart Mill (1859). For Mill (1859), individual conduct moves from the private to the public realm when "self-regarding" acts "violate a distinct and assignable obligation to any other person or persons" (p. 68-69). Similarly, "there is a sphere of action in which society, as distinguished from the individual, has, if any, only an indirect interest" (Mill, 1859).[20]

In Von Hannover v. Germany (2004), the ECtHR held that the publication by a German tabloid of a series of photographs of a public figure engaged in personal activities in public places (such as the sidewalk and a restaurant's open-air patio) violated her right to privacy under the European

[19] In fact, privacy in public was a significant theme in Warren and Brandeis's seminal 1890 article, *The Right to Privacy* (Warren and Brandeis, 1890).

[20] Mill's concept of "self-regarding" action has, however, been subjected to a great deal of debate, multiple interpretations, and criticism (see Ten, 1968).

Convention on Human Rights and Fundamental Freedoms. The court came to this conclusion because,

> "[A]lthough the public has a right to be informed, which is an essential right in a democratic society that, in certain special circumstances, can even extend to aspects of the private life of public figures, particularly where politicians are concerned, this is not the case here. The situation here does not come within the sphere of any political or public debate because the published photos and accompanying commentaries relate exclusively to details of the applicant's private life" (para. 64).

Thus, because the speech at issue did not relate to matters of public interest (defined narrowly, and excluding mere curiosity (see Moore, 2013)) or further aims of democratic deliberation, the right of privacy (as the right to control the use of personal information) could prevail over the right to free expression. I believe this strikes an appropriate balance in most cases. The holding would not prohibit the taking of the photographs in a public space, but only applies to the subsequent use of that information post-capture, which can be regulated when it concerns the release of merely private information about another, un-consenting, person. However, as stated above, when the speech concerns matters of genuine public interest (related to informed and democratic self-governance), speech may prevail, even when it involves exposing personal or private details of another person. Although, when obscuring personal information is possible without limiting the usefulness of the speech for democratic deliberation, there is no reason why the right to speak should include the right to include such personal information.

That said, it seems intuitive (to me) that a person implicitly waives their right to limit *access* to information they volunteer to general public view—including their presence in public itself. With the relative permanence of information in today's interconnected and digitally mediated world, it also seems arguable that such a person has waived their right to subsequently withdraw access to previously public information (granted it was published voluntarily) and then object to reference to the information itself, unless the information is subsequently acquired through illegal or improper means (i.e. access is granted in perpetuity if, and only if, the information is sourced from residual copies of the previously public information lawfully obtained). However, it does not necessarily follow that a person has waived her right to object to all further *uses* of that information.[21] Also, this allowance for an *implied* waiver of privacy rights should be limited to episodic intrusions (as defined by Cohen (2013) and discussed above). The implied waiver should not extend to systematic intrusions, or to long-term archiving and aggregation of many such pieces of information. Mill's writing may also suggest some interesting points here, when he finds some

[21] And it may also be that the initial waiver I argue is implied by a person's presence in a public space should be limited to those temporally situated within the same space, and that any subsequent recording or archiving of that information *without any additional justification* should be considered a subsequent *use* of that information and a violation of privacy. This distinction is important considering the definition I employ (drawing on Moore's (2007; 2010) definition) relies on the assumption that privacy may be violated by access to personal information as well as by subsequent use of that information. Waiving rights to object to access should not mean a person has waived the right to object to uses of their information or that such use cannot constitute a violation of that person's privacy.

difference between actions that infringe another's "constituted rights" (which can be punished by the application of law), actions that are merely hurtful but not violative of rights (punishable by opinion, but not law) and those that involve no harmful effect on society (outside the reach of society) (Mill, 1859, pp. 63-64).

To illustrate, let us consider the following example: when a person, "X", steps outside of her home and walks down a busy public street, we might conclude that X has waived her right to claim some privacy interest (related to access) in the fact that she is walking down the street (or even in her precise location) in plain view of other pedestrians, police officers, and anyone else in the near vicinity. It seems ridiculous to suggest we should "turn off our eyes," despite the fact that a person's mere presence in public appears to be within Mill's private, self-regarding sphere (that, if it affects others, does so only indirectly). But should the fact that the 'eyes' in the scene happen to be those of sophisticated robots or other electronic devices (drones, CCTV cameras, smartphones, Google Glass, or an officer-mounted camera) alter this conclusion? Or, rather than turn off our eyes (or recording devices), should we require the use of privacy-preserving technologies, such as an anti-monitoring suit (Moore, 2005, p. 199) or a device that obscures the view of nearby lenses? I would argue we should not require this sort of affirmative obligation, and that a focus on the potentially dominating effects of information collection (especially systematic intrusions that aggregate pieces of information over time or from different sources) can help us recognize the need to increase antipower and build obscurity into the regulation of state surveillance.

Continuing the previous hypothetical, it seems intuitive to argue that bystanders cannot, and should not, be restricted from later telling someone else (including a police officer) about, or recording, what they observed in a public space.[22] This is true even if the speech at issue doesn't necessarily implicate self-governance. Even if conceptually drafting a social contract is undesirable, as Mill suggests, the ability to report on actions witnessed in public (or the right to take photographs in public spaces filled with people) may be necessary "return" (Mill, 1859, p. 63) for the benefits of protection that society (and law enforcement) offers. Of course, this characterization assumes that we enter public spaces in a truly voluntary fashion. This might be debatable (as we often are required to pass through public spaces to supply ourselves with food or engage in work), and such a distinction would only strengthen a claim to a right to privacy in public. However, despite this important caveat, the idea that when a person discloses information to a third party, they waive any right to object to further disclosure by the third party, even to government agents, makes some sense insofar as it requires us to conclude that such a privacy interest has been waived in these circumstances and in relation to those who also temporally occupy and share the same space. They are the primary, if not intended, "recipients" of that information. However, this situation becomes increasingly complex as we introduce various technological means of surveillance into the scene,

[22] However, this situation is complicated by the fact that digital recorders like CCTV cameras, smartphones, body cameras, or ALPR cameras capture information that can be become part of a permanent, persistent, and searchable memory.

particularly if the surveillance technologies are capable of recording data that can be easily searched and mined for relevant information years into the future, and as we consider that electronic surveillance information can be easily shared with third parties.

Thus, we can characterize a person's mere presence in public as reasonably implying a waiver of the right to object to another accessing that information (e.g. taking a photograph),[23] but there is no reason this waiver should extend to further uses of such information, especially those that could be used to infringe the liberty or other rights of the person (e.g. entry into a long-term police database or disclosure under freedom of information laws) absent strong connections between that personal information itself and matters relevant to self-governance and the public interest. Relatedly, even if personal information privacy rights ought to protect individual activity in public spaces to some degree, the importance of citizen oversight, personal liberty, and First Amendment rights to gather and access information about government conduct weigh in favor of a conclusion that public officials engaged in their official duties (especially in public spaces) have effectively waived certain additional privacy interests (interests that ordinary citizens ought to maintain) by virtue of their positions as public servants. This conclusion is particularly important when applied to law enforcement and other government agents who have the power to coerce, detain, arrest, and otherwise interfere significantly with personal liberty interests. Thus, the privacy protections for ordinary citizens do not extend fully to uniformed public officials engaged in their official business and citizens should be able to, for example, take and disseminate footage of official police action without the risk of state reprisal. In the context of law enforcement, much of what officers do in public is a matter of social interest because it constitutes (potentially coercive) state action, and free speech claims to document, record, and discuss state actions are also supported by the aims of democratic First Amendment theory.

3.5. Social Theory

3.5.1. Surveillance and surveillance theory

The word surveillance has its origins in the French verb "surveiller," which literally means to "watch over" (Lyon, 2007, p. 13). Lyon defines surveillance as "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction" (though he also notes exceptions to this general definition) (Lyon, 2007, p. 14). Haggerty and Ericson (2006) also claim that surveillance "involves the collection and analysis of information about populations in order to govern their activities" (p. 3). In the context of academic research, surveillance is also an "analytical category" and, as such, a "simplifying device" (Haggerty, 2006, p. 39). Surveillance research (commonly called "surveillance studies"), on the other hand, is research that "detail[s] the ways in which everyday life in surveillance societies occurs" and which "continuously reopen[s] the 'black-box' into which surveillance is vanishing" (Wood and Webster, 2009, p. 260). Surveillance itself, as a phenomenon, is inextricably linked

[23] If not, we would prohibit individuals from taking photographs or video in public spaces without first acquiring consent from anyone who's image or voice might be captured.

with questions of liberty, security, and the relationships between people and their governments (Wood and Webster, 2009, p. 260). There have been numerous theories offered to explain surveillance—its place in modern society, its effects on society, and its implications for liberty and privacy—ranging from the panopticon to the concepts of synopticon and social sorting and beyond. In the paragraphs that follow, I outline and discuss some of these theories, as relevant to the topic of this dissertation.

Rather than concentrating on abstract ideas, good surveillance theory ought to keep "the practices and processes of everyday life" in constant focus (Lyon, 2007, p. 47). It must also do this while explaining "what is important without becoming overly abstract or paranoid or technologically deterministic" (Lyon, 2007, p. 47). Lyon also tells us that surveillance theory should rely on history (presumably to include prior empirical knowledge) and should be open to empirical and moral critique (Lyon, 2007, p. 47). Broad theories of surveillance, not situated in particular circumstances, settings, or political climates, or that are not developed in reference to particular technologies, may not be tremendously useful (see Lyon, 2007, p. 46-47). Thus, Lyon states that, "the quest for an abstract grand theory of surveillance is a wild-goose chase" (Lyon, 2007, p. 46; *see also* Haggerty, 2006, p. 39). In order to better understand the experience of living with a certain manifestation of surveillance in society, from a researcher's perspective, it may also be helpful to consider three dimensions proposed by Wood and Webster (2009): 1) contrasting perceptions of surveillance, 2) depth of surveillance, and 3) exposure to surveillance (pp. 265-68) (each of these will be taken up in turn, below). In my view, the bottom-up approach of NLR and its focus on examining everyday interactions complements Lyon's prescription to focus on the practical implications of surveillance in everyday life, as well as Wood and Webster's dimensions. Thus, using methodologies inspired by NLR can provide a good way to conduct research on the implications of, and interactions between, law and surveillance in society. This enterprise is also normative, as I agree with Wood and Webster (2009) that "better understanding, and enhanced societal awareness, of surveillance can lead to better informed public policy and practice" (p.260). Lastly, in any attempt to understand the place of surveillance in society, we must not lose sight of the possible unintended consequences posed by the adoption of new technologies or their use for new purposes, the stakeholder politics shaping and defining such adoption and use, and the politics that shape resistance (Haggerty and Ericson, 2006, pp. 6-21).

In terms of normativity and surveillance theory, surveillance need not be seen as inherently good or bad (Haggerty, 2006, p. 41). There are significant value conflicts that should restrain our normative conclusions about surveillance prior to some deeper analysis of the "aims, dynamics and rationalizations of particular surveillance projects" (Haggerty, 2006, p. 41). Gary Marx has clearly elaborated on many of these conflicts:

> …we value both the individual and the community. We want both liberty and order. We seek privacy and often anonymity, but we also know that secrecy can hide dastardly deeds and that visibility can bring accountability. But too much visibility may inhibit experimentation, creativity and risk taking…. we want to be seen and to see, yet also to be left alone. We value freedom of expression and a free press

> but do not wish to see individuals defamed or harassed. We desire honesty in communication and also civility and diplomacy. We value the right to know, but also the right to control personal information…. Whatever action is taken there are likely costs, gains and trade-offs. At best we can hope to find a compass rather than a map and a moving equilibrium rather than a fixed point for decision making (Marx, 2005).

The *panopticon*, Bentham's utopian prison design developed as a metaphorical landmark of power and social control by Michel Foucault (1979), is arguably a good example of a broad surveillance theory that has been "over-extended" at the direct expense of other important aspects of surveillance (*see* Haggerty, 2006, p. 23; Lyon, 2007, pp. 47, 57). The idea of the panopticon, as extended by Foucault and others, has been called the "leading scholarly model or metaphor for analyzing surveillance" (Haggerty, 2006, p. 23). In the panoptic design, an agent in power has the ability to watch others without their knowledge and, because of shades or other privacy mechanisms, can do so without the risk that the others will watch back. According to Lyon, this results in a "one-sided account" with too much focus on "the subtly coercive experience of living with the uncertainty of being seen" (Lyon, 2007, p. 57). Haggerty expressed his view about the relevance of focusing on Foucault's panoptic ideas quite strikingly when he stated that:

> …changes in surveillance processes and practices are progressively undermining the relevance of the panoptic model for understanding contemporary surveillance. Foucault continues to reign supreme in surveillance studies and it is perhaps time to cut off the head of the king. The panoptic model masks as much as it reveals, foregrounding processes which are of decreasing relevance, while ignoring or slighting dynamics that fall outside of its framework (Haggerty, 2006, p. 27).

Panoptic theory has undergirded many CCTV installation projects, in the UK and elsewhere. However, critiques of these programs showing that CCTV camera placement itself may not actually deter crime (or if it does, it only displaces it) (Webster, 2009; Baile, 2008; Welsh and Farrington, 2004) suggest that something more must accompany the surveillance (or the expectation of surveillance) itself before certain positive outcomes can become more likely. A number of studies analyzing the impact of surveillance cameras have indicated that video cameras have little or no statistical effect on incidents of crime (Webster, 2009; Baile, 2008; Welsh and Farrington, 2004), and that the purposes and uses of video surveillance systems have been shifting over time (Webster, 2009). The theory of "surveillance creep" is premised on the idea that "the policy focus of video surveillance has shifted as the technology has diffused, from crime prevention, to community safety and now also to national security" Webster, 2009; Lyon, 1994; Lyon, 2007, p. 52). According to Webster, the "net result" of the accumulation of surveillance systems has only been increased levels and "intensities of surveillance" (Webster, 2009). Surveillance creep may also be contributing to what has been called the "normalization" of surveillance in modern societies (see Webster, 2009; Wood and Webster, 2009, pp. 262-65). Haggerty (2006) also argues that references to a plethora of different *opticons* in scholarly literature, points to the conclusion that the panopticon—although it has become reified as a cross-

disciplinary stand-in model for surveillance—needs to be limited and modified to properly cover the contemporary dynamics of surveillance (p. 26).

Foucauldian panopticism also omits the role of the media (either the mass media or social media) (Lyon, 2007, p. 59). Thomas Mathieson's concepts of the "synopticon" and the "spectacle" attempt to bring this missing element back into the equation (Mathieson, 1997). Mathieson focused primarily on the role of the mass media in shifting society from one where the few watched the many—the panoptic model—to one where "*the many… see and contemplate the few*, so that the tendency for the few to see and supervise the many is contextualized by a highly significant counterpart" (Mathieson, 1997, p. 219). However, this synoptic view can easily be extended beyond just the role of the mass media. Reg Whitaker described a "participatory panopticon" where decentered surveillance from many sources—including commercial establishments—also brings benefits to consumers, thus motivating consensual participation (Whitaker, 1999, p. 141), what Lyon (2006) also calls the "panopticommodity" (p. 8). Others scholars present theories of "inverse surveillance" or "sousveillance" (Mann and Ferenbok, 2013; Mann, Nolan and Wellman, 2003) or "counter-surveillance" (Monahan, 2006). While inverse surveillance generally refers to reversing the panoptic gaze by empowering individuals to watch those in power through the use of technology or other means, counter-surveillance—as defined by Monahan—refers to "intentional, tactical uses, or disruptions of surveillance technologies to challenge institutional power asymmetries" (Monahan, 2006, p. 516) more akin to resistance. Haggerty (2006) has suggested that the ability of the citizenry (or those not typically empowered in the panopticon) to watch the powerful, represents a major development for surveillance theory, and that the realization by those in power of their own visibility will lead them to "develop a self-interest in the politics of surveillance" (p. 30).

Likewise, in the context of the present research, the panoptic possibility of the watcher being able to watch others without been visible to them, may not be inclusive enough to fully explain the cases of police body-cameras or civilian video, as these phenomena include both elements of surveillance (in a panoptic sense) as well as aspects of sousveillance (or watching back). In some respects, each of these forms of surveillance rely not only on documenting and recording the conduct of the other (or the self) but also in modifying behavior (a form of social control) through the mere presence of the recording device itself. This finding is not necessarily inconsistent with panoptic theories of surveillance, but a focus merely on surveillance as directed from state-to-citizen may not be broad enough to capture and explain the broader dynamics inherent in participatory or reciprocal surveillance that generally occur in open places, rather than the enclosed spaces considered by Foucault (Lyon, 2007, p. 59). Likewise, Haggerty and Ericson's (2000; 2006) concept of the "surveillant assemblage" directs our focus to the "disconnected and semi-coordinated character of surveillance" in modern times (Haggerty and Ericson, 2006, p. 4-5). Surveillance is disconnected because it is not all organized and instituted by one single entity (e.g. the state). However, when institutional actors (e.g. states and corporations) coordinate and share information between them, they can harness a great deal of power (see Haggerty and Ericson,

2006, p. 4-5). This concept bears some relation to the "mosaic theory" of the Fourth Amendment, discussed *infra* at Chapter 4.

Interestingly, Foucault's (1979) argument that visibility would encourage "soul training" as a disciplinary function to nudge inmates towards self-reflection and behavioral change, has some resonance with claims made by proponents of body-camera adoption—especially after the killings of Michael Brown in Ferguson, Missouri and Eric Garner on Staten island, New York. These proponents claim that body-camera usage by police officers will affect the behavior of the officers as well as the citizens with whom they interact (see Ariel, Farrar, and Sutherland, 2014). This interesting claim demonstrates how popular perceptions about some forms of surveillance can vary dramatically from others (Wood and Webster's (2009) first dimension): for example, we accept and encourage body-camera adoption, but we abhor mass surveillance of our emails or phone calls. As such, some of Foucault's ideas about producing "docile bodies" and critiquing "vision" as a playing a role in state domination are indeed still relevant (see Foucault, 1979; Lyon, 2007, p. 59). However, a strict panoptic analysis would ignore the fact that the social control imagined by wearable surveillance cameras cuts both ways—it applies to both those in power (the officers) and those who are not (the civilians). The social control and "soul training" that may be present in the prison may not be the sole (or primary) functions of new forms of surveillance, such as body-cameras, civilian video, and license plate scanning. Civilian video and body-cameras are also oriented strongly towards the evidentiary value of recordings, and license plate readers may be employed—for example, by parking enforcement agencies—in order to boost revenue and enforce the payment of parking fines. Despite the need to look beyond the panopticon, however, it may be best "to accept the panoptic presence, even if only as the ghost lurking within the post-panoptic world" (Lyon, 2006, p. 4) as suggested by Boyne (2000) and Lyon (2006). Surveillance theory cannot ignore panoptic theory, but it must move beyond it (Lyon, 2006, p. 12).

Other theorists have distinguished between reciprocal and non-reciprocal surveillance (Marx, 2005; Haggerty and Ericson, 2006, p. 10; Brin, 1998). According to Gary Marx:

> An important distinction that often involves power differentials is whether the surveillance is non-reciprocal or reciprocal. The former is one-way with personal data going from the watched to the watcher (e.g., employers, merchants, police, wardens, teachers, parents). With reciprocal surveillance it is bi-directional (e.g., many conflicts, contests and recreational games) (Marx, 2005).

Marx also distinguishes between symmetrical and asymmetrical surveillance, and explicitly recognizes the role of freedom of information requests as form of surveillance from underneath; as a means for the many to watch the few:

> Surveillance that is reciprocal may be *asymmetrical* or *symmetrical* with respect to means and goals. Thus in a democratic society citizens and government engage in reciprocal but distinct forms of mutual surveillance. For example citizens can watch government through Freedom of Information Requests, open hearings and meetings, and conflict of interest and other disclosures required as a condition for running for office. But citizens cannot legally wiretap, carry out Fourth Amendment

> searches or see others' tax returns. In bounded settings such as a protest demonstration, there may be greater equivalence with respect to particular means e.g., police and demonstrators videotaping each other (Marx, 2005).

Visibility is a central component of surveillance (Lyon, 2007, p. 47). In the context of this current research, visibility as a concept in surveillance studies relates well to Thompson's (2004) concept of "new visibility" and Goldsmith's (2010) application of that concept to policing. Similarly, the concepts of counter/reciprocal/inverse (sous)surveillance, introduced above, also play a role in helping us understand how to better conceptualize visibility in a post-panoptic environment (despite all simply being forms of surveillance themselves). The connections between visibility and surveillance have historical roots in the idea that the watchers are watching because they do not trust the watched (Lyon, 2007, p. 48). For those who don't trust—whether an employer, police officer, or citizen—visibility can turn bodies into something "to be observed and tested" (Lyon, 2007, p. 48). Policing and criminal justice has also long played a prominent role in how surveillance is conceptualized. When we hear the expression that a person is "under surveillance," we generally link that surveillance to a supposed law enforcement purpose (Lyon, 2007, p. 49). Police have utilized various mechanisms for making public spaces (and the inhabitants thereof) more visible; from Victorian streets (Cohen, 1985; Lyon, 2007, p. 49) to high-tech devices for undercover police work (Marx, 1988) to stingrays (cell site simulators), license plate scanners, facial recognition, large-scale CCTV networks, and body-worn cameras. This surveillance of public spaces also likely affects some categories of citizens disproportionately, with the potential for increasing stigmatization and more frequent criminalization of these more visible members of society (Lyon, 2007, p. 49; Perri 6, 2003).

Links between totalitarian surveillance—of the sort envisioned by George Orwell in his conceptualization of Big Brother in *Nineteen Eighty-Four* (1949)—and modern liberal democracies has been a common theme in surveillance theory (Lyon, 2007, p. 52-53). It is precisely in the bureaucratic state, where record keeping and monitoring have "become routine and technologically-augmented that restrictions on liberty… may be anticipated" (Lyon, 2007, pp. 53, 68). However, in contemporary society, it is not just within state governments that surveillance and possibility of restrictions on liberty may be found (Lyon, 2007, p. 54). Corporate interests and commercial surveillance play a substantial role in documenting individual persons, allowing the creation of what Daniel Solove has called the "digital dossier" (Solove, 2004). These commercially held data doubles of real-world people (at whatever granularity) are also often intermingled with government surveillance data. In the terms of Wood and Webster's (2009) dimensions, this surveillance is also deep, unobtrusive and sophisticated" (p. 267).

Despite limited effects on crime rates, some evidence suggests that video surveillance systems may reduce antisocial and undesirable behavior in certain cases, although more research is likely necessary to draw firm conclusions (Webster, 2009; Gill and Spriggs, 2005). However, some researchers have begun to report that surveillance may be used to discriminate against certain groups by limiting their access to public spaces through targeted monitoring and coordinated officer interventions (Sætnan, et al., 2004). This phenomenon of discrimination through

surveillance technologies has been referred to as the "purification" or "commercialization" of public spaces (Lomell, 2004), or "surveillance as social sorting" (Lyon, 2003). This desire to "purify" public spaces and—in the commercial space—to not "put customers off" means, in practice, "excluding 'undesirables'" (Lomell, 2004). Similar observational research has documented that security operators more often than not "single out and target" individuals based on appearance alone, rather than behavior (Lomell, 2004; Norris and Armstrong, 1999; McCahill, 2002). The actual or potential discriminatory effects of surveillance technologies have been documented or discussed in a variety of settings (Lyon, 2003), including public streets, transportation centers and shopping malls (Lomell, 2004; Sætnan, et al., 2004), the workplace (Zureik, 2003; Ball, 2003; Coultrup and Fountain, 2012; Johnston and Cheng, 2002; Moore, 2000), through use of electronic identity cards (Stalder and Lyon, 2003), intelligent transportation systems (Bennett, et al., 2003), genetic testing (Nelkin and Andrews, 2003), and the "racializing" of medical research (Poudrier, 2003). In an observational study of various video surveillance control rooms in Scandinavia, researchers have reported various patterns of discriminatory enforcement by private security firms, instituted through coordinated monitoring and officer intervention (Lomell, 2004; Sætnan, et al., 2004).

The accumulation of large amounts of information from multiple sites of surveillance results in surveillance agents mining for documentary traces and examining the data doubles of both the weak and the powerful members of society (Haggerty, 2006, p. 29). However, those in society without the means to exploit these surveillance potentialities—generally those who are both poorer and more frequently the target of state observation—are often left without the recourse available to the more well-off members of society (Haggerty, 2006, p. 29). Additionally, our perceptions about surveillance may also be linked to our exposure to surveillance, as indicated by Wood and Webster's (2009) third dimension (p. 267-68), potentially leading to lack of concern by those who are not confronted with intense or obtrusive surveillance on a regular basis. However, despite continuing inequities, in recent times we have also seen the proliferation of social visibility in which "more people from more walks of life are now monitored" (Haggerty and Ericson, 2006, p. 5). Freedom of information laws and processes, as well as rights to record public officials, represent powerful and important tools for the citizenry to wield in the name of inverting visibility, further increasing social visibility at all levels, and calling government actors to account. This sort of inverse surveillance is much more democratic than Mathieson's (1997) mass-media-based synopticon, and potentially much more powerful.

3.5.2. Policing, new visibility, and public oversight

In contrast to the more common term, 'surveillance,' which originates from the French word 'surveiller'—meaning to watch over something and which is typically associated with governments or corporations watching individuals—'sousveillance' generally refers to the act of an individual watching from below as a form of inverse surveillance. The term was coined by Steve Mann, an academic and inventor, who derived the term from the French "sous" (under) and "veillance" (to watch). This usage is similar to other terms also seen in literature, including inverse

surveillance, counter surveillance, and reciprocal surveillance. Sousveillance may refer to the ability of an individual person or group of persons to observe or record the actions of authorities, or it may also refer to the ability of individuals to watch each other. There have been a number of notable instances of sousveillance over the years, including the civilian video of the beatings of Rodney King and Reginald Denny in 1991 and 1992, the shooting of San Francisco BART passenger Oscar Grant in 2009, the death of Ian Tomlinson during the London riots of 2009, and the choking death of Eric Garner at the hands of NYPD officers in 2014.

Traditionally, police—"the most visible of all criminal justice institutions" (Chermak and Weiss, 2005, p.502; Goldsmith, 2010, p. 914)—were generally visible only through direct interactions with citizens (and within the view of nearby onlookers). Goldsmith (2010) refers to this as "primary visibility" (p. 914). This visibility also included uniforms and marked vehicles as markers of official authority and legitimacy. However, the development of mass media led to a "secondary visibility" (Goldsmith, 2010, p. 914) that allowed individuals not spatially connected to the scene of original interaction to access photographic and narrative materials documenting and describing these distant encounters and subsequently pass judgment. The Rodney King video filmed by George Holliday in 1991 provides a clear (and now famous) example, causing outrage and reaction across the United States as well as internationally. The shooting of Oscar Grant in San Francisco (Antony and Thomas, 2010), the killing of Ian Tomlinson in London (Greer and McLaughlin, 2010), and the choking death of Eric Garner (Murray, et al., 2014; Gambino, 2014) (all captured by citizens wielding cameras embedded in cellphones and later made available on Youtube.com and other websites), and numerous other examples, demonstrate the increasing power of these recordings to spread widely and influence public perception and media coverage of police related events (see Greer and McLaughlin, 2010).

Civilian video and the presence of large numbers of recording devices in many public spaces (especially in densely populated, urban areas) has increased the nature and amount of secondary visibility as more and more police-citizen encounters are being recorded and broadcast over the Internet to increasingly wider audiences around the world. This increase in secondary visibility has been termed policing's "new visibility" (Goldsmith, 2010, *citing* Thompson, 2005). These recordings available on YouTube, et al. also include numerous videos recorded by police department cameras installed in patrol vehicles (dash-cams) or worn on officers' uniforms (body-cameras) and obtained by citizens under public disclosure requests and uploaded to the Internet. Thus, as wearable cameras become more widely adopted, officers and departments will need to confront existing public disclosure laws and the prediction that such adoption will result in greater numbers of videos being uploaded to the Internet (this prediction is a simple one: as more footage is captured, more will get released through existing channels and subsequently uploaded to the Internet, as long as disclosure laws are not altered).

Police departments have "a clear interest in how their personnel and activities become visible to others and in what is revealed as a result to outsiders" (Goldsmith, 2010, p. 915, citing Mawby, 2002, and Adut, 2008). This claim has played out in practice. For example, in recent years the

Seattle Police Department (SPD) was engaged in a series of lawsuits where they objected to the release of dash-camera footage to local news organizations, attorneys, and private citizens (see Newell, 2014a; 2014c). On their face, these refusals were based on interpretations of state privacy laws, out of concern for invading the privacy of innocent bystanders captured on tape. The SPD also initially claimed the ability to seal footage for three years (unless relevant to current litigation), and then to destroy footage at that point (the expiration for the statute of limitations), effectively exempting footage from public disclosure except in certain narrow circumstances. Secrecy, despite certain legitimate justifications (e.g. not compromising an on-going investigation), has been a "familiar protective practice[]" used by police to avoid "public embarrassment and formal accountability" (Goldsmith, 2010, p. 915, citing Westley, 1956, and Punch, 1985; 2009), and any allowances for secrecy ought to be accompanied with clear sunset provisions to force disclosure when the justification has been exhausted. Thus, it would be naïve to believe officers (and departments) would 1) record all encounters judiciously, 2) preserve all recordings properly, and 3) properly release all footage related to public requests under state disclosure laws (especially when the footage is damning), unless strict laws, regulations, or other transparency measures were in place—including, potentially, forms of independent citizen oversight.[24] These practices are also evidence of agency-level resistance to surveillance (in the form of public records requests).

Goldsmith (2010) has also argued that any value for the police in increased visibility was contingent "upon maintaining 'normal appearances' and delivering 'proper performances'" (p. 915, citing Goffman, 1971; 1990). The possibility that misconduct, then, might become more visible as a result of increased recording poses a serious problem for law enforcement image management. As mentioned above, the recording of non-arrest, "peace keeping," activities may also subject officers to oversight from a variety of sources that may diminish their ability to "act alternatively" in situations where they might otherwise have chosen not to make an arrest; for example, to merely give a warning in a situation where an offense was not patently illegal (see Bittner, 1990, p. 36). In the case of officer-mounted cameras, however, the police fulfill a gatekeeper role that is not available when confronted with the lenses of civilian video. This gatekeeping, as evidenced in the SPD example, potentially threatens the public's ability to conduct effective citizen oversight, especially when combined with certain efforts and laws that would restrict the ability of citizens to conduct 'reciprocal surveillance' by filming officers in public spaces or during other police-citizen interactions. On the other hand, if additional research bears out the results of the Rialto Study (Ariel and Farrar, 2013; Ariel, Farrar, and Sutherland, 2014) that the use of these systems significantly lowers the rates of officer use of force and citizen complaint, then some of these concerns may be alleviated to some degree in practice.

[24] For recommendations about the most effective form of citizen oversight, see Walker, 2000, pp. 179-180; see also Walker, 2005; Herbert, 2006a, p. 69)

3.5.2.1. Subservience, separation, and generativity

The proper role of officer-mounted wearable cameras is also informed by an understanding of some of the power dynamics implicated by police-citizen encounters. Herbert (2006a; 2006b) provides a useful articulation of three dynamics that structure police efforts to legitimize themselves to the citizenry they serve. This three-pronged analysis provides an important theoretical basis for critiquing and exploring the risks and benefits of implementing these systems in actual police practice, as well as police officers' reactions to being surveilled themselves (whether by citizens or through the use of these wearable systems or dash-cam systems). First, democratic government institutions must be subservient to the public to some degree (Herbert, 2006b, p. 482). As such, police must be responsive to citizen oversight (Walker, 2000, p. 7). Wearable cameras and civilian video both plainly hold the promise of exposing wrongful action (one purpose of oversight). However, as stated above, police have a clear interest in controlling the extent of their visibility in this regard (Goldsmith, 2010). Because of this, there is a direct tension between police subservience to the citizenry and the second dynamic, separation. This dynamic may also help explain why officers often react negatively to citizens recording their public activities.

Herbert (2006b) argues that the police's desire for separation is implicated both by the legal order (their ability to engage in coercive action is in some conflict with a purely subservient role, albeit regulated by formal law) and their desire for professional status (the "skilled practitioner" discussed by Bittner (1990, p. 33)). That is, as professionals, they have special knowledge and training, can make appropriate decisions that could not be made by ordinary civilians, are distinct from the citizenry, and should be sheltered from citizen meddling (Herbert, 2006b, p. 487-88). Separation is also sought as officers feel the need to "possess unquestioned authority, particularly in situations where danger may be present," often as a consequence of their desires to remain safe in dangerous circumstances and to receive deference because of their professional skills and training, and because they are putting themselves in harm's way for a higher purpose (Herbert, 2006b, p. 488). The recording of these potentially dangerous encounters also threatens to expose the use of force, even when arguably appropriate or necessary under the circumstances, to heightened levels of scrutiny. This may be one cause for the significant drop-off in the use of force by the Rialto police officers (Ariel and Farrar, 2013; Ariel, Farrar, and Sutherland, 2014)—and it is possible it signals an unwillingness by the officers to engage physically on camera, even when to do so might be appropriate, and not only when force is unwarranted.

These questions of police epistemology and morality inform Herbert's (2006a; 2006b) third mode: generativity. Police practices and policies have the potential to shape social life, and the use of officer-mounted cameras poses an obvious challenge to the status quo of officer-citizen interactions and, likely, the perception citizens form of officers in general. In any case, there is a certain disconnect between public sentiment and officers' self-recognition as "deeply virtuous… risk-taking protectors of society" (Herbert, 2006b, p. 491) that is likely to play out in interactions post-adoption of these surveillance systems. In particular, if officers are enabled to use these

wearable camera systems, any attempts to prohibit the public from likewise recording their encounters with police become even less legitimate (if a case for their illegitimacy can even be made in the first place). If the use of these systems contributes to special exemptions for law enforcement to record conversations under varying state wiretapping and/or eavesdropping laws, the non-reciprocal nature of these legal exemptions may constitute a form of impermissible domination and further illegitimate such policies in the sight of the public.

Relatedly, research on resistance to surveillance has also become an area of interest within the surveillance studies community (Marx, 2003; Grenville, 2010; Haggerty and Ericson, 2006; Monahan, 2006; Shay, Conti and Hartzog, 2013; Wilson and Serisier, 2010). Gary Marx has developed, through a variety of empirical studies, a taxonomy of eleven forms of resistance or non-compliance: "discovery moves, avoidance moves, piggybacking moves, switching moves, distorting moves, blocking moves, masking (identification) moves, breaking moves, refusal moves, cooperative moves, and counter-surveillance moves" (Marx, 2003). Others, such as Grenville (2010), have extended some of Marx's work; finding that awareness of and experience with surveillance are strongly correlated with forms of resistance to preserve privacy (although these results also vary significantly by country) (p. 75). Given numerous news reports of officers failing to activate in-car cameras during potentially problematic interactions, it can be expected that officers may also find ways to resist the gaze of body-mounted cameras as well. Lyon (2006) has also noted a conundrum, where active resistance increases along with the stringency and rigor of a surveillance regime, while "the more soft and subtle the panoptic strategies, the more it produces the desired docile bodies" (p. 4; *see also* p. 18).

4. Setting the stage: privacy, space, and public access to information

4.1. Introduction

Personal privacy rights, whether physical or informational in nature, are often intertwined with questions of space, and outcomes in legal cases are often based on judicial reasoning that relies on a clear dichotomy between the public and private. Information about activities occurring within the walls of a person's home or in another non-public place often receive greater legal protections than those that occur in public spaces. These accounts of privacy also rely to a significant extent on notions of property—that is, a person's home or property interests provide a strong shield to prying eyes. On some accounts, what has been exposed to public view is, by definition, not private and, as a consequence, privacy law should not limit the disclosure of publicly available information (except, perhaps, in situations where the public disclosure itself is the result of unlawful or unauthorized acts) even when that information is about a personally identifiable individual. This view has taken considerable hold in American privacy jurisprudence. However, even in Europe, with its legislative focus on *data protection* rather than "privacy" *per se*, privacy ideas and spatial considerations have also played a significant role in shaping regulatory regimes. At least according to the jurisprudence of the European Court of Human Rights (ECtHR), an individual's right to a private life may trump society's interest in publication or distribution when the information at issue relates to private matters that do not contribute much to matters of public interest and debate, even when the information itself was collected in public spaces. In these cases, public access to information is limited by personal privacy rights.

On the other hand, under a battery of freedom of information (FOI) laws, governments around the world are required to disclose information contained in records held by public agencies. FOI laws are vitally important in many aspects of democratic governance; they allow for transparency, heightened accountability within publicly funded agencies and government, and provide the citizenry with information that can be used for a wide variety of social goods, including supporting free speech principles. However, as these governments collect increasing amounts of information about their citizens and others living within (or even without) their borders, some of this personal information may be subject to public disclosure. Absent exceptions to disclosure built into local or national FOI laws, this information ceases to be private, no matter how sensitive, merely because a government agency holds it within its possession—and regardless of whether the information was obtained voluntarily and knowingly, surreptitiously, or by compulsion. We then have, as Daniel Solove has also argued, a situation where governments "compel individuals to reveal a vast amount of personal information about themselves" and then "routinely [pour] this information into the public domain—by posting it on the Internet where it could be accessed from all over the world, by giving it away to any individual or company that asked for it, or even by providing entire databases of personal information upon request" (Solove, 2002, p. 1138). If this is the case (and it is in many places), we have a situation where governments can compel a lack of personal information privacy, not just *vis-à-vis* the government itself (which arguably has strong claim to need some personal information from its citizens; e.g. name and address in return for a driver's

license, or fingerprints and other personal information from individuals convicted of felonies). However, there is no reason why these claims should then extend to unlimited—and *legally mandated*—disclosure of this information to any member of the requesting public, which can lead to significant privacy intrusions.

In the following sections, I outline the basic legal frameworks that govern the right to individual privacy *vis-à-vis* the government under federal law in the United States (primarily under the Fourth Amendment to the Constitution), in Washington State (primarily under the state constitution, the Privacy Act, and common law privacy torts), and in Europe (at least insofar as it is represented by the jurisprudence of the European Court of Human Rights, which is only one of many relevant legal institutions in Europe). This analysis is limited to the primary laws that govern the police-citizen interactions and data collection/disclosure relevant to the three cases presented in Chapters 5-7, and does not constitute an exhaustive review of all privacy laws that might be relevant in certain specific circumstances. The subsequent chapters deal more deeply with how these legal frameworks apply to the specific issues raised in each case. The European cases from the ECtHR are presented primarily as a means to provide contrast to the approach taken in the American context, and are not necessarily indicative of all the varying approaches taken by other national or supranational courts or law-making bodies in Europe (i.e., it does not comprise a full comparative analysis). However, as all member states to the European Union are signatory to the European Convention on Human Rights (and the EU itself is obligated to accede to the convention under the Treaty of Lisbon) and are thus subject to the jurisdiction of the ECtHR, these cases should provide an adequate introduction to how European jurisdictions have tackled similar issues. Following this overview of relevant privacy laws, I present an overview of the basic rationale behind the adoption of FOI law in Washington State and discuss the approach taken in the Washington Public Records Act (RCW § 42.56.001, *et seq.*). I conclude this chapter with an initial discussion (to be addressed in more depth in the subsequent chapters) of the potential conflict between personal privacy and the disclosure of personal information under state public records laws.

4.2. Constitutional protections in the U.S.: the Fourth Amendment, privacy, and space

The Fourth Amendment regulates the ability of government agents (within the United States) to conduct searches or seizures of citizens' persons, houses, papers or effects. Importantly, the Fourth Amendment's privacy protections only cover some forms of governmental intrusion into an individual's private life: searches and seizures that are deemed *unreasonable* and for which the government has not obtained an adequate judicial warrant. In such cases, any evidence gained from the unwarranted search is subject to exclusion from the evidence presented in any subsequent criminal trial. The text of the amendment reads:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized (U.S. Const. amend. IV).

The Fourth Amendment protects an individual's privacy interest in his (or her) person, home, and belongings from governmental intrusion when either the individual has a subjective expectation of privacy that society is prepared to recognize as reasonable (Smith v. Maryland, 1979, p. 740; Katz v. United States, 1967, p. 361 (Harlan J. concurring)) or when the government's intrusion would constitute a trespass onto private property (United States v. Jones, 2012). The Supreme Court has held that searches, for Fourth Amendment purposes, may be physical or electronic in nature (see e.g. United States v. Jones, 2012; Katz v. United States, 1967). A number of scholars have argued that the Supreme Court's Fourth Amendment privacy jurisprudence is misguided or, at least, "has not fared well with the changing times" and the advancement of technology (see e.g. Solove, 2004, p. 190, quoting Sundby, 1994, p. 1771). In any case, it does provide more limited privacy protections—in many circumstances—than does Washington State's Constitution (discussed *infra* at s. 4.3.1).

The Fifth Amendment, by comparison, prohibits the government from forcing an individual to incriminate himself (U.S. Const. amend. V). At one point in time, these constitutional amendments together barred government from "any forcible and compulsory extortion of a man's own testimony or of his private papers to be used as evidence to convict him of crime or to forfeit his goods," because such compulsion is an "invasion of his indefeasible right of personal security, personal liberty and private property" (Boyd v. United States, 1886, p. 630; Solove, 2004, p. 63). However, the court subsequently backed away from that position in later opinions (Solove, 2004, pp. 63-64; Warden, Md. Penitentiary v. Hayden, 1967, pp. 309-10; Shapiro v. United States, 1948, pp. 16-17). A number of recent federal court cases in the United States have reaffirmed the right of government to monitor publicly owned spaces, as long the surveillance does not capture areas where a reasonable expectation of privacy (measured both subjectively and objectively) exists. In these cases, however, federal courts found that video surveillance violated Fourth Amendment guarantees against unreasonable searches in middle school and police station locker rooms (Brannum v. Overton County School Board, 2008; Bernhard v. City of Ontario, 2008), as well as a shared physical education teachers office adjacent to a school locker room (Doe v. Dearborn Public Schools, 2008), because the respective plaintiffs maintained reasonable expectations of privacy in those spaces. However, the stronger legal basis for governmental surveillance in more public areas, compared to the obviously more private nature of locker rooms and personal office space, is based on the premise that individuals do not maintain any objective expectation of privacy in their conduct in these public spaces, and that these surveillance systems represent a valid use of state power to protect public safety (Nieto, 1997). As a result, video (and other) surveillance in these areas is generally permissible (Nieto, 1997; Carson, 2010; Sher, 1996).

Some opponents to this dominant view, however, claim that citizens should maintain a right to anonymity in public spaces that would prohibit government from engaging in pervasive video surveillance and tracking without proper justification (Slobogin, 2002, pp. 213-300; Rosen, 2011). However, it appears these arguments have largely far fallen on deaf judicial ears. In addition to these Constitutional concerns, state privacy laws also generally permit public employers to monitor employees after appropriate disclosure (Robertson and DiLello, 2008).

Despite the fairly clear legal basis for visual (and other) surveillance of public spaces in the United States, legal scholars have also noted the potential chilling effects that such realities may have on speech in public spaces (Nieto, 1997; Sher, 1996; Slobogin, 2002). Some commentators have argued that, because video surveillance raises the problem of the "unobservable observer", where the watched do not—or cannot—know who is watching or for what purpose, national or local policy ought to require more overt surveillance practices, public disclosure, and independent oversight of control rooms (see e.g. Goold, 2002, pp. 21-27).

4.2.1. Property, trespass, and reasonable expectations of privacy

Historically, Fourth Amendment protections have been tied closely to property and spatial considerations. Property considerations have been implicated most clearly in cases dealing with searches of private residences, and protection to information contained in these private spaces has vastly outweighed any interests individuals might have in information in more public venues. As such, non-secrecy (or presence in public space) has long constituted a waiver of Fourth Amendment rights to object to searches of that information (see United States v. Jones, 2012, p. 957, Sotomayor J. concurring). Traditional trespass/property-based court decisions, recently reinvigorated by the Supreme Court's decisions in United States v. Jones (2012) and Florida v. Jardines (2013) (both authored by Justice Scalia), have determined whether a search has occurred on the basis of whether a government agent has committed a physical trespass. For instance, in one important early decision, Olmstead v. United States (1928), the Supreme Court held that warrantless government wiretapping of a person's telephone line did not violate the Fourth Amendment unless it involved physical trespass onto the defendant's property. According to the court, the mere amplification of words transmitted over public telephone lines, without some physical trespass onto a physical area, was not enough to implicate the Fourth Amendment's warrant requirement (Olmstead v. United States, 1928). As a result, the court immunized government agents in that case from liability for tapping into the defendant's phone calls, because they tapped the lines at a place outside the defendant's physical residence and office. Justice Brandeis wrote a passionate dissent in the case, arguing, much in line with arguments made in his seminal article of 1890 (Warren and Brandeis, 1890), that, by not finding police wiretapping an unreasonable search in that case, the Court's Fourth Amendment jurisprudence failed to properly reflect changing societal conditions (Olmstead v. United States, 1928, pp. 472-73 (Brandeis J dissenting)). Brandeis wrote, "[c]lauses guaranteeing to the individual protection against specific abuses of power, must have a similar capacity of adaptation to a changing world" (Olmstead v. United States, 1928, pp. 472).

Later, in 1961, the Supreme Court constrained *Olmstead*'s trespass doctrine in Silverman v. United States (1961), holding that the government only acts unreasonably when it commits an "unauthorized physical encroachment within a constitutionally protected area" (p. 510). Importantly, the *Silverman* decision moved away from reliance on local trespass law, instead basing its analysis "upon the reality of an actual intrusion" into such an area (Silverman v. United States, 1961, p. 512), leaving the idea of a "constitutionally protected area" largely undefined.

Against that revised analytic frame, the court found that the police, in that case, had inserted a microphone into the floorboards of a vacant house used by the defendants as a gambling establishment, and that the "spike" microphone had actually contacted the house's heating ducts as a means of capturing and amplifying sounds from inside the house, effectively encroaching into the house itself (Silverman v. United States, 1961, pp. 506-07). The court held that, in contrast to the facts of *Olmstead*:

> The officers overheard the petitioners' conversations only by usurping part of the petitioners' house or office—a heating system which was an integral part of the premises occupied by the petitioners, a usurpation that was effected without their knowledge and without their consent. In these circumstances we need not pause to consider whether or not there was a technical trespass under the local property law relating to party walls. Inherent Fourth Amendment rights are not inevitably measurable in terms of ancient niceties of tort or real property law (Silverman v. United States, 1961, p. 511).

A few years later, in Katz v. United States (1967), the Supreme Court moved away from this trespass-based analysis, effectively adopting the view put forward by Justice Brandeis in *Olmstead*. In *Katz*, a man named Charles Katz was originally convicted of using a public pay phone to make illegal gambling bets and wagers. Part of the government's case relied on evidence obtained through the use of a listening device that the police had attached to the outside of the public pay phone frequently used by Katz to place his bets. The Court of Appeals upheld Katz's conviction because the court found that the use of the listening device did not invade the physical space occupied by the defendant (e.g. the inside of the phone booth), in line with *Olmstead*, *Silverman*, and other previous decisions. However, the Supreme Court moved away from any adherence to its earlier jurisprudence. Speaking for the majority, Justice Stewart held that:

> Once… it is recognized that the Fourth Amendment protects people—and not simply "areas"—against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure. We conclude that the underpinnings of *Olmstead* and [other similar cases] have been so eroded by our subsequent decisions that the "trespass" doctrine there enunciated can no longer be regarded as controlling. The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth, and thus constituted a "search and seizure" within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance (Katz v. United States, 1967, p. 353).

Through an influential concurrence by Justice Harlan, the court also articulated a new two-step approach to determine the reasonableness of government action under the Fourth Amendment (Katz v. United States, 1967, p. 361). The test announced by Justice Harlan requires that, for a warrantless search to be unreasonable (and thus violate the Fourth Amendment), the person subject to the search must "have exhibited an actual (subjective) expectation of privacy," and that such an expectation must also "be one that society is prepared to recognize as 'reasonable'" (Katz v. United

States, 1967, p. 361). A person using a phone, stated the *Katz* court, "is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world" (Katz v. United States, 1967, p. 352), and therefore retains a privacy right in the conversation (Warshak v. United States, 2007, p. 470, *citing* Katz v. United States, 1967, p. 352). Importantly, Harlan stated that by closing the door of the phone booth, Katz had demonstrated an expectation of privacy; an expectation the majority of the Justices found to be objectively reasonable.

In the intervening years, a few scholars attempted to identify empirically, primarily through survey methodologies, whether the Supreme Court's pronouncements about what society is prepared to recognize as reasonable match popular sentiments, but the Court has not generally relied on empirical data when deciding cases or employing the *Katz* test (see Blumenthal, Adya, and Meera, 2009; Slobogin and Schumacher, 1993a; 1993b). Although Justice Harlan's test was not part of the majority opinion in *Katz* (and thus not binding as precedent in later cases), it was subsequently adopted by the Supreme Court as the primary mechanism to determine whether any particular government-initiated search or seizure was unreasonable.[25] These decisions have generally held that when information is released to the public (or even to some third party) it cannot then be the subject of any legitimate expectation of privacy under the Katz formulation. From 1967 until the *Jones* decision in 2012, the reasonable expectation of privacy test largely succeeded the prior focus on whether the government has violated a property right, such as by committing trespass, in conducting a search. However, despite this decades-long focus on the *Katz* test, Justice Scalia's majority opinions in United States v. Jones (2012) and Florida v. Jardines (2013) have recently marked a resurgence of the earlier trespass doctrine.

In United States v. Jones (2012), the Supreme Court held that because of the Fourth Amendment's historic ties to property, *Katz* had not actually overruled physical trespass as a means of implicating the Fourth Amendment's prohibition on unreasonable search or seizure; rather, *Katz* had merely expanded the scope of Fourth Amendment protections to some situations that did not involve trespass (United States v. Jones, 2012, pp. 950-51). Thus, both Justice Harlan's test and the historic trespass test could be invoked in future Fourth Amendment cases as means to invalidate government conduct and exclude evidence from criminal prosecutions. In *Jones*, the court held that unwarranted placement of a GPS tracking device by the government on a vehicle frequently used by the defendant, a suspected drug trafficker, violated the Fourth Amendment because the officers committed a trespass by physically attaching the device to the vehicle. In Florida v. Jardines (2013), the court held that a police officer impermissibly entered a constitutionally protected area (the "curtilage" of the defendant's home) when he brought a trained police dog up the front walk and allowed it to sniff the area around the front door of the defendant's house (p. 1415-16). The *Jardines* court, just like in *Jones*, explicitly rejected the need to reach a *Katz* analysis, stating that: "One virtue of the Fourth Amendment's property-rights baseline is that it keeps easy cases easy" (Florida v. Jardines, 2013, p. 1417). Of particular importance to the analysis

[25] Beginning with some discussion in Terry v. Ohio (1968), later being formally adopted by the court in Smith v. Maryland (1979).

in this dissertation, the facts of both *Jones* and *Jardines* are intertwined with spatial considerations—whether an individual's movements on public streets or the rights to exclude certain activity within the curtilage surrounding a person's home.

4.2.2. The third party doctrine

The third party doctrine is a judicially created legal rule that limits a person's reasonable expectation of privacy in information that person voluntarily exposes to third parties. The doctrine has been described as "the Fourth Amendment rule scholars love to hate" (Kerr, 2009, p. 563). For years, it has been subjected to voluminous amounts of criticism, both by legal scholars and state courts (Kerr, 2009, p. 563-64). The Supreme Court has upheld the rule, holding that citizens "assume the risk" that what they disclose to a third party will be transferred on to the government, but has not explicitly defended it (Kerr, 2009, p. 564). This assumption of risk also applies when a person voluntarily ventures into or traverses a public space. Now, after *Jones*, criticism of the practical consequences of the doctrine has reached the Supreme Court itself (see *e.g.* United States v. Jones, 2012, p. 957 (Sotomayor J. concurring)).

In its early years, the third-party doctrine was applied in cases involving undercover agents and confidential informants (Kerr, 2009, p. 567). These cases held that defendants could not claim Fourth Amendment violations based off of conversations with government agents—sometimes wearing wires—because the "the Fourth Amendment does not protect 'a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it'" (Kerr, 2009, p. 568, *quoting* Hoffa v. United States, 1966, p. 302). In later cases, the Court applied the doctrine to business records. In United States v. Miller (1976), the Supreme Court held that a bank depositor does not have any reasonable expectation of privacy in financial information (in the form of deposit slips, checks, and bank records) because such information was conveyed voluntarily to the bank and "exposed to their employees in the ordinary course of business" (United States v. Miller, 1976, p. 435). As such, the court found that:

> [t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. . . . [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed (United States v. Miller, 1976, p. 443 (citations omitted)).

In her concurrence in *Jones*, Justice Sotomayor stated that the time had come for Fourth Amendment jurisprudence to discard the premise that legitimate expectations of privacy could only be found in situations of near or complete secrecy (United States v. Jones, 2012, p. 957). Sotomayor argued that people should be able to maintain reasonable expectations of privacy in some information voluntarily disclosed to third parties. The opposite and historical view of the court, Sotomayor stated, was "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks" (United

States v. Jones, 2012, p. 957). Sotomayor considered that logs of phone calls, text messages, and websites visited, as well as email correspondence, purchase histories from online retailers, and geolocation information were all forms of information that were technically disclosed to third parties through mundane tasks, but where such disclosure should not constitute waiver of all privacy interests (United States v. Jones, 2012, p. 957). "[W]hatever the societal expectations," Sotomayor stated, these forms of information:

> Can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection (United States v. Jones, 2012, p. 957).

Some lower federal courts have begun to question a strict application of the third-party doctrine as well. In 2010, the Sixth Circuit addressed the question of whether the government violated the Fourth Amendment when agents compelled an ISP to turn over the contents of the defendant's emails without first obtaining a warrant (United States v. Warshak, 2010, p. 288). In that case, the Sixth Circuit held that, even though the subscriber agreement allowed the ISP to access the contents of its clients' emails in certain circumstances, "the mere *ability* of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy" (United States v. Warshak, 2010, p. 288). The court found that this conclusion was consistent with the *Katz* holding, because the telephone service company in the prior case also had a legal right to listen to phone calls in certain cases. The *Warshak* court also differentiated the facts in that case from those in *Miller*, because the third-party ISP was merely an intermediary rather than the intended recipient (as the bank was in *Miller*). Under the rationale in this case, the government could not demand the information from the intermediary corporation or service provider, but the conclusion would not necessarily extend to information released by the recipients of the communication, such as the email recipient or Facebook friend. Whether this was the right result, or merely a step in the right direction, remains the subject of some controversy. However, as evidenced by the recent indication by the five concurring justices in *Jones* (Sotomayor was the most explicit, but Alito's opinion can also be read this way) that they may be willing to rethink Fourth Amendment theory (Slobogin, 2012, p. 1-2), the time may be ripe for further challenges to precedent. Indeed, the fact that the *Jones* decision followed from the introduction of the mosaic theory in the lower court's decision signals that the justices may be willing to entertain this issue in coming years.

4.3. Privacy and access in Washington

Because this dissertation focuses on analyzing the specific and fairly unique interaction between privacy and FOI law in Washington State, the following subsections constitute an overview of the relevant legal provisions in Washington State law. Under Washington law, four primary types of privacy protections are relevant:

1) Privacy protections under the state constitution (Wash. Const. art. I, § 7);

2) The Washington Privacy Act (Rev. Code Wash. 9.73);
3) Privacy-based exemptions contained within the Washington Public Records Act (Rev. Code Wash. 42.56); and
4) Common-law privacy protections (torts).

The following subsections provide an overview of each of these areas of the law. Exemptions in the PRA (number 3, above) are discussed in section 4.4, below.

4.3.1. Privacy under the Washington state Constitution

The Washington State Constitution, originally enacted in 1889, contains a prominent provision for the protection of personal privacy.[26] Section 7 of Article 1 states that, "No person shall be disturbed in his private affairs, or his home invaded, without authority of law" (Wash. Const. art I, § 7). The wording and intent of this provision is largely similar to that of the Fourth Amendment; however, Washington State courts have repeatedly held that the State Constitution provides citizens with significantly greater protections than does its federal counterpart (State v. White, 2007, p. 135; State v. MacDicken, 2014, p. 940); State v. Meneese, 2012, p. 946; State v. Monaghan, 2012, pp. 787; State v. Eisfeldt, 2008, p. 637; Columbia Basin Apartment Ass'n v. City of Pasco, 2001, pp. 803-04; City of Seattle v. McCready, 1994, p. 267; Seattle v. Mesiani, 1988, p. 456; State v. Gunwall, 1986, p. 65); State v. Stroud, 1986, p. 148).

On one hand, the Fourth Amendment restricts law enforcement's ability to conduct *unreasonable* searches—requiring police to obtain a warrant before conducting a search in those cases—but it does not require warrants for otherwise reasonable searches (e.g. where a search would not violate a legitimate expectation of privacy). Section 7 of the Washington State Constitution, on the other hand, "is unconcerned with the reasonableness of the search, but instead requires a warrant before any search, reasonable or not" (State v. Eisfeldt, 2008, p. 634-35; see also State v. Monaghan, 2012, pp. 787-88). Thus, a police officer in Washington State is required to acquire a warrant prior to conducting *any* search, subject only to a few limited exceptions (State v. Monaghan, 2012, pp. 787), regardless of whether the subject maintains a subjective or objective expectation of privacy in such information or locality. Section 7 likely imposes a limit on public disclosure under the state Public Records Act (see Nissen v. Pierce County, 2014, pp. 581-82; Freedom Found. v. Gregoire, 2013, p. 695)—when it would apply—but no cases have examined this question in detail.

Claims under Section 7 are subject to a two-part analysis. First, courts must determine "whether the State has intruded into a person's private affairs;" if so, courts proceed to the second part of the analysis, in which they ask "whether the authority of law required by [Section 7] justifies the intrusion, which is satisfied only by a valid warrant, limited to a few jealously guarded exceptions." (State v. Hinton, 2012, p. 34 (reversed on other grounds); see also McCarthy v. Barrett, 2011, p.

[26] These protections have a great deal of relevance to limits on government searches and the collection of personal information about citizens, but they have little bearing on issues related to public disclosure.

1145; State v. Monaghan, 2012; State v. Lakotiy, 2009; State v. Athan, 2007; State v. Miles, 2007; State v. Surge, 2007).

Importantly, and despite the qualitative differences and some broader protections of the Washington law *vis-à-vis* the Fourth Amendment, Section 7 is still tied to notions of public/private (see e.g., State v. Carter, 2004, p. 125 (focus on homes and private affairs)) that arguably have a significant impact on how privacy in public is concerned, possibly resulting in similar conclusions to these questions as would the Fourth Amendment. However, instead of generally assuming subjective privacy expectations have been waived by a person's presence in public or the lack of total secrecy of some personal information, Washington courts must consider a separate array of considerations. Under Washington law, "Private affairs" is defined (rather opaquely) as "those privacy interests which citizens of this state have held, and should be entitled to hold, safe from government trespass absent a warrant" (State v. Collins, 2009, p. 439, *quoting* State v. Myrick, 1984, p. 511; State v. Hatchie, 2006; State v. Cheatam, 2003). More specifically, under Section 7, "courts consider whether the information obtained reveals 'intimate or discrete' details of a person's life, what expectation of privacy a person has in the information sought, whether there are historical protections afforded to the perceived interest, and the purpose for which the information is acquired and by whom it is kept" (State v. Collins, 2009, p. 439, *quoting* State v. Jorden, 2007, p. 127). Part of this analysis allows courts to examine the historical treatment of the constitutional text by courts as well as "the current implications of recognizing or not recognizing an interest" (York v. Wahkiakim School Dist. No. 200, 2008, p. 306).

4.3.2. The Washington Privacy Act

The Washington State Privacy Act, RCW 9.73 *et seq.*, contains a broad range of privacy protections, primarily for personal communications, but it does not create a broad privacy protection regime; it protects the privacy of telegrams (RCW § 9.73.010), sealed letters (RCW § 9.73.020), and private communications (e.g. RCW §§ 9.73.030, 9.73.040), and also regulates the use of pen registers and trap and trace devices (RCW § 9.73.260). A number of these provisions are implicated by citizen recordings and police officer use of body-cameras, discussed in this dissertation at Chapter 6 and Chapter 7, respectively. This section gives a brief overview of the law, leaving more thorough examination of specific provisions of the law to the chapters in the dissertation where they are directly relevant.

Importantly, the Privacy Act prohibits both wiretapping and eavesdropping (RCW § 9.73.030(1)(a)-(b)) absent some legal authority (e.g. a warrant or court order) (see RCW § 9.73.040). Under the wiretapping provision, RCW 9.73.030(1)(a), it is unlawful for "any individual, partnership, corporation, association, or the state of Washington, its agencies, and political subdivisions" to record or intercept any:

> Private communication transmitted by telephone, telegraph, radio, or other device between two or more individuals between points within or without the state by any device electronic or otherwise designed to record and/or transmit said communication regardless how such device is powered or actuated, without first

> obtaining the consent of all the participants in the communication (RCW § 9.73.030(1)(a)).

The statute's consent requirement requires all parties to a conversation to consent before recording becomes lawful—a so called, "all-party consent" law. Any recording of a transmitted private communication without such consent is classified as a gross misdemeanor (RCW § 9.73.080(1)). Similarly, the subsequent provision in the act, the eavesdropping provision, requires the same level of consent and carries the same penalties. That section prohibits the interception or recording of any:

> Private conversation, by any device electronic or otherwise designed to record or transmit such conversation regardless how the device is powered or actuated without first obtaining the consent of all the persons engaged in the conversation (RCW § 9.73.030(1)(b)).

The statute does contain some exceptions to the all-party consent rule; specifically, only one party's consent is required to lawfully record communications or conversations when they are "of an emergency nature, such as the reporting of a fire, medical emergency, crime, or disaster," or when they:

> "…convey threats of extortion, blackmail, bodily harm, or other unlawful requests or demands… occur anonymously or repeatedly or at an extremely inconvenient hour, or… [when they] relate to communications by a hostage holder or barricaded person" (RCW § 9.73.030(2)).

Consent is considered obtained when "reasonably effective" notice has been given by the person doing the recording (RCW § 9.73.030(3)). Such verbal notice must also be captured in the recording, or it is not valid for consent purposes (RCW § 9.73.030(3)). Traditional journalists, when "acting in the course of bona fide news gathering" are exempt from the regular consent requirement as long as their recording device is "is readily apparent or obvious to the speakers" (RCW § 9.73.030(4)). A number of more specific regulations and exemptions for law enforcement will be discussed in Chapters 6 and 7, infra, where relevant to the particular situations analyzed in those chapters.

4.3.3. Common law privacy in Washington

Washington State courts have recognized, to varying degrees, all four of Prosser's privacy torts (Prosser, 1960, p. 389): intrusion into seclusion (Doe v. Gonzaga University, 2001; McLenan-Kenny v. Washington Dept. of Labor and Industries, 2014), dissemination of private facts (Adams v. King County, 2008; White v. Township of Winthrop, 2005; Mayer v. Huesner, 2005; Doe v. Gonzaga University, 2001; Reid v. Pierce County, 1998), false light (Corey v. Pierce County, 2010; Eastwood v. Cascade Broadcasting Co., 1986; Brink v. Griffith, 1964), and appropriation, which has been codified in Washington law at RCW 63.60, *et seq*. Because only the former two of these four torts are potentially implicated to some degree by the police surveillance and the public disclosure of personal information under consideration in this dissertation, a brief presentation of those two torts—as recognized by Washington courts—follows.

Intrusion into seclusion. This tort requires a plaintiff to prove each of the following elements by a preponderance of the evidence:

> "1. An intentional intrusion, physically or otherwise, upon the solitude or seclusion of plaintiff, or his private affairs; 2. With respect to the matter or affair which plaintiff claims was invaded, that plaintiff had a legitimate and reasonable expectation of privacy; 3. The intrusion would be highly offensive to a reasonable person; and 4. That the defendant's conduct was a proximate cause of damage to plaintiff" (Doe v. Gonzaga University, 2001, pp. 705-06).

Government agents may be sued under this cause of action, although the agents must have intruded intentionally into the plaintiff's seclusion, such that a mistake of fact about whether they had obtained consent to search a premises would immunize an officer from such a claim (Youker v. Douglas County, 2014, pp. 797-98). However, despite the common law cause of action, plaintiffs cannot bring intrusion claims under the Washington State Constitution in order to claim civil damages (Reid v. Pierce County, 1998, pp. 213-14).

Public disclosure of private facts. Washington courts have adopted this tort as set forth in Restatement (2d) of Torts (1977) § 652D (White v. Township of Winthrop, 2005; Fisher v. State ex rel. Dept. of Health, 2005; Reid v. Pierce County, 1998), which reads:

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public (Restatement (2d) of Torts, 1977, § 652D).

Unlike intrusion, this tort requires an element of publication. Publication to only a small number of persons may not be actionable, as disclosure must either be to the public at large or in a way that "the matter is substantially certain to become public knowledge" (Fisher v. State ex rel. Dept. of Health, 2005, p. 879; *see also* Restatement (2d) of Torts, 1977, § 652D, comment a). However, in some cases, this publication may be required by law under the state Public Records Act (RCW § 42.56.001 *et seq.*; *see e.g.*, Bellevue John Does 1-11 v. Bellevue School Dist. #405, 2008, p. 206). One such case, where a requestor sought the names of public school teachers alleged to have committed sexual misconduct towards students, the Supreme Court of Washington held that the teachers' identities should only be disclosed "if the misconduct is substantiated or the teacher's conduct results in some form of discipline" (Bellevue John Does 1-11 v. Bellevue School Dist. #405, 2008, p. 206). Otherwise, the court held that the names of teachers should be redacted from any disclosed records (Bellevue John Does 1-11 v. Bellevue School Dist. #405, 2008, p. 226-27).

4.4. Public records access in Washington state

Washington State has a very broad public records law. It was adopted in 1972 by popular vote (Initiative Measure No. 276, 1972; Nast v. Michels, 1986, p. 310) as part of a larger anti-secrecy and government transparency measure (Richard, 2010, p. 495). The Washington Supreme Court has called the PRA a "strongly worded mandate for broad disclosure of public records" (Hearst

Corp. v. Hoppe, 1978, p. 127). The PRA is subject to a number of exceptions, most not relevant to the cases under consideration in this research, and its purpose is stated clearly in RCW 42.56.030:

> The people of this state do not yield their sovereignty to the agencies that serve them. The people, in delegating authority, do not give their public servants the right to decide what is good for the people to know and what is not good for them to know. The people insist on remaining informed so that they may maintain control over the instruments that they have created (RCW § 42.56.030).

All public agencies are required to make public records available as stated in RCW § 42.56.070(1):

> Each agency, in accordance with published rules, shall make available for public inspection and copying all public records, unless the record falls within the specific exemptions of [subsection 9] of this section, this chapter, or other statute which exempts or prohibits disclosure of specific information or records. To the extent required to prevent an unreasonable invasion of personal privacy interests protected by this chapter, an agency shall delete identifying details in a manner consistent with this chapter when it makes available or publishes any public record; however, in each case, the justification for the deletion shall be explained fully in writing (RCW § 42.56.070(1)).

Under the act, a "public record" is defined broadly as "any writing containing information relating to the conduct of government or the performance of any governmental or proprietary function prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics" with certain exceptions for legislative records held by the state Senate and House of Representatives (RCW § 42.56.010(3)).

According to one general study of government transparency across a variety of categories (of which public records access is only one), Washington State ranked third overall when compared with the other 50 states (Kilgore, 2012). Further analysis of the published dataset from the Public Integrity Investigation survey also confirms that Washington also ranks third (tied) when only considering the Public Access to Information category from that broader survey (see Figure 1).

STATE	FOI SCORE	RANK	STATE	FOI SCORE	RANK
Connecticut	166.67	1	Illinois	145.83	6
Nebraska	162.50	2	Pennsylvania	145.83	6
Washington	**150.00**	**3**	New Jersey	141.67	8
North Dakota	150.00	3	Idaho	141.67	9
Rhode Island	150.00	3	Arizona	133.33	10

Figure 1. Ranking (top ten) of the most transparent states, based solely on scores given to states in the State Integrity Investigation under that study's first category: Public Access to Information. This table represents my own analysis of the data, made possible by the dataset being publicly available online.[27]

[27] Dataset available at Public Integrity Investigation, Corruption Risk Index Raw Data, http://www.stateintegrity.org/corruption_risk_index_raw_data (direct link to Excel file: https://statecorruption.nationbuilder.com/assets/pages/2533/ScorecardExport_State_Integrity_Investigation_Scores050912.xls).

As additional, though purely anecdotal, evidence of the broad reach of Washington's Public Records Act (RCW § 42.56.001 *et seq.*), while conducting fieldwork with police agencies in Washington over the past few months, I have heard a number of police officials make the claim that their perception is that Washington law—as it relates to police disclosure of records—is the most transparent in the country.[28]

Washington courts have interpreted the PRA under the presumption that "full access to information concerning the conduct of every level of government is a fundamental and necessary precondition to the sound governance of a free society" (Nissen v. Pierce County, 2014, pp. 581-82, *citing* Neighborhood Alliance of Spokane County v. Spokane County, 2011, pp. 714–15). In line with its broadly encompassing purpose, access-promoting portions of the law are to be "liberally construed" while exemptions to the law should be "narrowly construed" to protect and promote the public interest (RCW § 42.56.030). Additionally, the PRA is designed to trump other laws (such as the state Privacy Act) when they conflict with its open-access prerogatives (RCW § 42.56.030), although other laws that specifically exempt certain records are held to supplement the PRA rather than as being in conflict (Building Industry Ass'n of Washington v. State Dept. of Labor and Industries, 2004, p. 663). Agencies themselves bear the burden of proving that an exemption is appropriate or that denying a request is within the law, and courts will presume that disclosure is otherwise required absent such a showing (In re Request of Rosier, 1986, p. 609).

In one recent, and particularly relevant, case, the Supreme Court of Washington held that a particular exemption under the Privacy Act relating to non-disclosure of police audio and video recordings made by in-car recording systems (so called "dash-cam" or "dashboard cameras") prior to the end of litigation was to be narrowly construed to include only cases "where the videos relate to actual, pending litigation" (Fisher Broadcasting-Seattle TV LLC v. City of Seattle, 2014, p. 526; see RCW § 42.56.). As such, potential litigation (e.g. where a person *could* bring a suit but had not actually filed a complaint at the time of the public disclosure response by the agency) was not a bar to disclosure. For more on this issue, see Chapter 7, infra.

On the other hand, Washington courts have held that the PRA does not trump constitutional protections (Nissen v. Pierce County, 2014, pp. 581-82; Freedom Found. v. Gregoire, 2013, p. 695). This essentially means that the constitutional rights of Washington citizens under Art. I, Section 7 (including government employees), to be free from unwarranted "searches and intrusions into their private affairs" outweighs public disclosure interests (Nissen v. Pierce County, 2014, pp. 581-82, *citing* Freedom Found. v. Gregoire, 2013, p. 695).

The PRA also recognizes the right to privacy as a possible exemption from disclosure, though the exemption is narrower than it might appear at first blush. Under the act, privacy violations as defined as instances where "disclosure of information about [a] person: (1) would be highly

[28] This of course, is a statement that requires detailed empirical study—and I hope my future research will begin to answer this and other related questions.

offensive to a reasonable person, and (2) is not of legitimate concern to the public" (RCW § 42.56.050).[29] However, the PRA limits the application of this right to privacy to the express provisions of the act (see RCW § 42.56.050) that provide limited grounds for redaction or denial.

There are, as a general rule, only three such express privacy-related provisions within the PRA:

1. RCW 42.56.230(3), which exempts "[p]ersonal information in files maintained for employees, appointees, or elected officials of any public agency to the extent that disclosure would violate their right to privacy";
2. RCW 42.56.230(4), which exempts "[i]nformation required of any taxpayer in connection with the assessment or collection of any tax if the disclosure of the information to other persons would: (a) Be prohibited to such persons under state or local law; or (b) violate the taxpayer's right to privacy or result in unfair competitive disadvantage to the taxpayer"; and
3. RCW 42.56.240(1), which exempts "[s]pecific intelligence information and specific investigative records compiled by investigative, law enforcement, and penology agencies, … the nondisclosure of which is essential to effective law enforcement or for the protection of any person's right to privacy."

Thus, if an express exemption does not exist within the PRA itself, privacy cannot be used as a reason to refuse disclosure. In cases where an express privacy exemption applies, the information must still meet the requirements of RCW section 42.56.050, stated above. In other cases, specific exemptions apply to bar the release of other sensitive information, such as information revealing the identity of minors who have been victims of sexual assault (RCW § 42.56.240(5); Koenig v. City of Des Moines, 2006, pp. 181-183)). According to the statute,

> Identifying information means the child victim's name, address, location, photograph, and in cases in which the child victim is a relative or stepchild of the alleged perpetrator, identification of the relationship between the child and the alleged perpetrator (RCW § 42.56.240(5)).

Other information contained in police reports or other records (presumably to include BWC footage) are not exempt and must be disclosed (see Koenig v. City of Des Moines, 2006, p. 187). According to the Supreme Court of Washington, even sexually explicit material contained in such reports must be disclosed, regardless of whether such disclosure would be "highly offensive to a

---

[29] This two-part test originates from the Restatement (Second) of Torts § 652. According to Perry (2015):

> "a court will look to the Restatement in analyzing whether disclosure of particular information will violate an individual's right of privacy. The Restatement specifically provides that "no right to privacy exists for facts that are matters of public record, such as a person's date of birth, the fact of his marriage, his military record, and the fact that he is admitted to the practice of medicine or is licensed to drive a taxicab. By contrast, disclosure of a person's sexual relations, family quarrels, unpleasant or humiliating illnesses, intimate personal letters, and most details of a person's life at home could give rise to a right of privacy." (Restatement (Second) of Torts at § 652D, comment b). Thus, disclosing a person's date of birth will not violate his or her right of privacy."

reasonable person" under section 42.56.050, because the "the legislature considered the ability to gauge the performance of law enforcement as more than a 'slight benefit' to the public, describing it as 'necessary'" (Koenig v. City of Des Moines, 2006, p. 186).[30]

This limitation on a more general privacy exemption to the PRA was a conscious choice by the Washington legislature. Section 42.56.050 (formerly RCW 42.17) was adopted by the legislature in 1987. The text of the bill inserting that provision into the PRA stated that:

> The legislature intends to restore the law relating to the release of public records largely to that which existed prior to the Washington Supreme Court decision in *In Re Rosier*, 105 Wn.2d 606 (1986). The intent of this legislation is to make clear that: (1) Absent statutory provisions to the contrary, agencies possessing records should in responding to requests for disclosure not make any distinctions in releasing or not releasing records based upon the identity of the person or agency which requested the records, and (2) agencies having public records should rely only upon statutory exemptions or prohibitions for refusal to provide public records (1987 Session Laws of the State of Washington, 1987, pp. 1546-47).

In the case of In re Request of Rosier (1986), the Supreme Court of Washington had found that the PRA included a general privacy exemption (p. 609). Subsequent to the legislative change, courts have limited the privacy-based exemptions to those explicitly enumerated in the act (see City of Lakewood v. Koenig, 2014 ("The PRA contains no general exemptions from disclosure to protect individual privacy or vital government functions."), *citing* Progressive Animal Welfare Soc. v. University of Washington, 1994.). These exceptions have been "narrowly tailored to specific situations in which privacy rights or vital governmental interests require protection" (City of Lakewood v. Koenig, 2014, para. 8, *quoting* Resident Action Council v. Seattle Housing Authority, 2013, p. 383). Should one of these privacy exemptions apply to a record, agencies may not simply deny a request. Rather, they must redact the exempt information and disclose the remainder of the responsive record. As interpreted by the Seattle City Attorney's Office:

> Identifying information generally includes name, residential and business address, telephone number cell phone number, date of birth, other unique identifying information, such as a unique job title (e.g., the only person with the title) or particular relationship to a person whose identity is exempt (e.g., a parent). The photo and other identifying information on a copy of a driver's license would reflect identifying information, and the letters, but not the numbers, in a driver's license number may also contain identifying information (Perry, 2015).

As such, police agencies in Washington State have recently been required to disclose entire databases of Automated License Plate Reader (ALPR) scans (including un-redacted license plate numbers of every vehicle scanned by the system along with precise geolocation and timestamp

[30] This is true even in cases where a requestor seeks records related to a sexual assault by naming the victim in the request. In such a case, the identifying information of a child victim must be disclosed (even though the requestor knew it) and the remaining information about the crime must be disclosed (Koenig v. City of Des Moines, 2006, pp. 186-187).

information, as well as information about plate numbers counted as a "hit" against government watch lists) (Newell, 2014b; Chapter 5, *infra*) as well as dash-camera and body-camera footage (see Chapter 7, *infra*). Some of the information contained in these disclosed files is potentially sensitive personal information about individuals not being charged with crimes—or, if they are being charged, have not been found guilty. In the case of ALPR databases, the aggregate data contained in these disclosures could potentially be analyzed to infer additional information about, or predict, otherwise innocent individuals' movements. On top of privacy concerns related to the disclosure of the personal information of civilians, these records also disclose very detailed and precise information about the movements and actions of individual police officers—including when they are not on duty and when they have not been accused of any wrongdoing.

4.5. Privacy in public: Cases from the European Court of Human Rights

In Europe, the ECtHR has been an important international (regional) venue for the resolution of issues related to rights of privacy and expression. The court has often been forced to balance the competing interests at stake in cases coming from all over Europe, often producing controversial outcomes, such as that in Von Hannover v. Germany (2004). In 2012, the court suggested some limitations to (but ensured its decision was nonetheless consistent with) its earlier decision, in the follow-up case of Von Hannover v. Germany (II) (2012). In the first Von Hannover case, the ECtHR protected a public figure's right to privacy in public spaces against the right of the German press to publish photographs of the claimant in various public places. In the second, it elaborated on the balancing test courts should undertake to decide these controversial cases. In this section, I will use the Von Hannover decision as my jumping off point, and will explore decisions both prior to and following that decision that have also addressed the tension between these competing human (and civil) rights.

Article 8 of the Convention states:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society… or for the protection of the rights and freedoms of others (European Convention on Human Rights, art. 8).

On the other hand, Article 10 states:

> 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers….
>
> 2. The exercise of these freedoms… may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society… [including] for the protection of the reputation or the rights of others, [or] for preventing the disclosure of information received in confidence…" (European Convention on Human Rights, art. 10).

The rights of freedom of expression and freedom of the press often conflict with the individual rights of individuals to the privacy of their personal information. Whether an individual may take a photograph of another person in a public space (e.g. on a public street or in a public park) and then publish or distribute that photograph without violating the other person's right to privacy is an important political question. It is also a question that has confronted, and divided, domestic and supranational courts, such as the ECtHR, in recent years. In particular, courts and lawmakers in the UK have begun to question whether the ECtHR has gone too far in protecting personal privacy in some of its decisions under Article 8 of the Convention at the expense of the other party's freedom of expression. Privacy rights in publicly available information may seem paradoxical to some (Nissenbaum, 1998a; 1998b), but recent decisions of the ECtHR have granted these rights over claims of freedom of expression under Article 10 in a variety of contexts.

Often these situations involve the right of the press to publish photographs taken of individual persons in public spaces, but we need not limit ourselves to consider the rights of the press, as citizens also may claim a right to publish or distribute personal information of others available in public spaces (whether online or offline). In recent months, the British Royal Family has objected to the publication of a number of images of family members, including photographs of Catherine, Duchess of Cambridge, sunbathing topless while on vacation (Foster and Smith-Spark, 2012). The family has also initiated criminal charges against the photographer, who used a high-powered lens while standing on the edge of a public road to take the photographs. Reportedly, President Barack Obama has also recently pressured news photographers to remove photographs of his daughters from agency circulation (Renfrew, 2013). These high-profile cases generate a certain expected amount of buzz in online news reporting and on gossip websites, but presumably ordinary citizens also similarly value their privacy, even while in publicly visible places, although the risk of publication might not be as high.

In Von Hannover (2004), the applicant, Princess Caroline Von Hannover of Monaco, claimed that decisions of the German courts refusing to prohibit the publication of certain photographs of her in the tabloid press violated her rights to private life under Article 8 of the Convention (Von Hannover v. Germany, 2004, paras. 2, 10). Rather than being a one-off attempt at prohibiting publication, this series of judicial decisions represents only a small part of the Princess's overall litigation strategy to limit publication of photographs all over Europe, as she had brought lawsuits in a variety of European countries since the 1990s (Von Hannover v. Germany, 2004, para. 9). The case at hand involved the publication of over 40 photographs in three different German tabloid papers from 1993 until 1997, including images of the Princess sitting in a restaurant courtyard with a male companion, riding a horse, with her children, shopping, tripping over an obstacle at a Monte Carlo beach club, and riding a bicycle (Von Hannover v. Germany, 2004).

Initially, the domestic German courts found that Von Hannover was "a contemporary figure '*par excellence*'" and thus had to tolerate the publication of photographs taken in public places (Von Hannover v. Germany, 2004, para. 21). "Even if the constant hounding by photographers made her daily life difficult," the Hamburg Court of Appeal stated, "it arose from a legitimate desire to

inform the general public" (Von Hannover v. Germany, 2004, para. 21). On appeal, the Federal Court of Justice allowed part of the Princess's appeal, stating that (as summarized by the ECtHR):

> …even figures of contemporary society "*par excellence*" were entitled to respect for their private life and that this was not limited to their home but also covered the publication of photos. Outside their home, however, they could not rely on the protection of their privacy unless they had retired to a secluded place—away from the public eye … where it was objectively clear to everyone that they wanted to be alone and where, confident of being away from prying eyes, they behaved in a given situation in a manner in which they would not behave in a public place (Von Hannover v. Germany, 2004, para. 23).

Based on this standard, the court held that publication of the photographs showing the Princess sitting with a male companion in a secluded part of a restaurant courtyard violated her right to privacy. In regards to the other photographs, the court found that the public had legitimate interests in knowing how she behaved in public. On a subsequent appeal to the German Federal Constitutional Court (FCC), Von Hannover won another small victory. The FCC held that the publication of three photographs of the Princess with her children also violated her personality (privacy) rights under German law. Subsequently, the Princess initiated two more rounds of litigation based on additional photographs published in 1997, but the German courts denied her claims based on the publication of those images. And, in relation to the photographs taken at the open-air Monte Carlo Beach Club, which was a private establishment, the courts found that her claims of privacy failed because the area where she was photographed was not a "secluded" place (Von Hannover v. Germany, 2004).

Princess Von Hannover argued at the ECtHR that the German reliance on a "secluded place" was too narrow to protect her Article 8 right to privacy, especially because she claimed that paparazzi "constantly hounded" her and "followed her every daily movement" (Von Hannover v. Germany, 2004, para. 44). This situation, she claimed, deprived her of any privacy and limited her ability to move around freely. Rather than contributing to legitimate public debate, she argued the photographs merely provided tabloid press with an opportunity to satisfy it readers' "voyeuristic tendencies" and rake in big profits from her exploitation (Von Hannover v. Germany, 2004, para. 44). The ECtHR considered these claims in relation to the remaining photographs, including those depicting her on horseback, riding a bicycle, shopping on her own and with companions, with her bodyguard at a market, on a skiing holiday in Austria, leaving her Parisian residence, playing tennis, and tripping over the obstacle at the Monte Carlo Beach Club. The court found that these photographs fell within the scope of the Princess's private life under Article 8, because they included aspects of her identity and interfered with her ability to develop relationships with others (Von Hannover v. Germany, 2004, para. 50).

According to the court, a person's private life "includes a person's physical and psychological integrity" and therefore, even in public, some interactions with others "may fall within the scope of "private life" (Von Hannover v. Germany, 2004, para. 50). The court also made clear that Article 8 obligated states to not merely refrain from interfering with their citizens' private lives,

but it also entails positive obligations, including the "adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves" (Von Hannover v. Germany, 2004, para. 57). Additionally, even though freedom of expression is "one of the essential foundations of a democratic society" (Von Hannover v. Germany, 2004, para. 58), photographs implicate a person's privacy rights and reputational interests in particularly important ways. Photographs, the court stated, do not just disseminate ideas, but they also reveal private and intimate information about an individual (Von Hannover v. Germany, 2004, para. 59). The court also noted that the "climate of continual harassment" implicated by paparazzi photography and the tabloid press has the capability to create strong subjective feelings of intrusion into private matters (Von Hannover v. Germany, 2004, para. 59). In conclusion, the court found a violation of Article 8, because:

> …the decisive factor in balancing the protection of private life against freedom of expression should lie in the contribution that the published photos and articles make to a debate of general interest. It is clear in the instant case that they made no such contribution, since the applicant exercises no official function and the photos and articles related exclusively to details of her private life (Von Hannover v. Germany, 2004, para. 76).

The court further held that:

> "…the public does not have a legitimate interest in knowing where the applicant is and how she behaves generally in her private life even if she appears in places that cannot always be described as secluded and despite the fact that she is well known to the public…. Even if such a public interest exists, as does a commercial interest of the magazines in publishing these photos and these articles, in the instant case those interests must, in the Court's view, yield to the applicant's right to the effective protection of her private life" (Von Hannover v. Germany, 2004, para. 77).

In a concurring opinion, Judge Barreto argued that the proper balancing test is not whether the publication contributes to a debate of public interest (the majority view) or whether the photographs are taken in a secluded place (as the German courts had held), but should be based on a case-by-case inquiry into whether the individual has a "'legitimate expectation' of being safe from the media" (Von Hannover v. Germany, 2004, J. Barreto concurrence). Interestingly, this is similar to the "reasonable expectation of privacy" test employed in subsequent decisions by UK courts.

The Von Hannover (2004) decision has been hailed as a landmark in ECtHR privacy and expression jurisprudence, but the court has also handed down a number of additional decisions about the right to publish or distribute photographs of private individuals. An in-depth analysis of these other decisions is not within the scope of this present analysis, but a short summary of these cases is important. In Peck v. United Kingdom (2003), the court held that an individual's Article 8 rights were violated when CCTV images that depicted him in a public street moments after he had attempted to commit suicide by slashing his wrists with a knife were published in print and on

television, because certain incidents that occur in public can still fall within the person's private life, especially when publication could expose the action to far greater observation than reasonably expected by the individual.

Sciacca v. Italy (2006) provides a particularly interesting insight, as it relates to the disclosure of a photograph taken by the police, the subject of subsequent chapters in this dissertation. In that case, the court reaffirmed the Von Hannover (2004) decision and held that the publication by the police of the photograph of a private individual suspected of criminal activity violated the person's Article 8 rights. The court found that being the subject of criminal proceedings was not enough justification to publish an individual's photograph. The photograph at issue was taken by the Italian Revenue Police (*Guardia di Finanza*) after they had questioned and arrested the applicant (Mrs. Sciacca) about possible connections to a variety of financial crimes (Sciacca v. Italy, 2006, paras. 11-16, 25) and released to the press by the police at a press conference about the investigation. Mrs. Sciacca complained to the court that the disclosure of the photograph, prior to any finding of guilt in her trial was not justified (Sciacca v. Italy, 2006, para. 24). The court cited language in Von Hannover (2004) about "a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life'" (Sciacca v. Italy, 2006, para. 29, quoting Von Hannover v. Germany, 2004, para. 50-53), and held that the applicant's status as an "'ordinary person' enlarges the zone of interaction which may fall within the scope of private life, and the fact that the applicant was the subject of criminal proceedings cannot curtail the scope of such protection" (Sciacca v. Italy, 2006, para. 29). Because the disclosure of the photograph by the police had been done pursuant to prior practice, but not authorized by any specific law, the court found a violation of Article 8 (Sciacca v. Italy, 2006, para. 30). (Interestingly, as Washington's PRA could be considered such a law, it would survive the initial test at the ECtHR; however, the ECtHR would then have to look at whether the disclosure was done pursuant to a "legitimate aim" or was "'necessary in a democratic society' to achieve that aim" (Sciacca v. Italy, 2006, para. 30) before finding any violation of the applicant's rights).

Subsequently, in 2012, Princess Caroline Von Hannover got another day in court. In Von Hannover v. Germany (II) (2012), she and her husband Prince Ernst August Von Hannover claimed, in reliance on her previous victory, that publication of additional photographs in the German tabloids violated their rights to a private life (Von Hannover v Germany (II), 2012). This time around, the case was heard by the ECtHR's Grand Chamber. The photographs at issue in the second case depicted the applicants out on walks during a ski vacation in St. Moritz and riding the chair lift at the resort. These images were published alongside photographs of other members of the royal family, including Caroline's father, Prince Rainier, who was suffering poor health. In this case, the court found that the German courts had altered how they balanced privacy and freedom of expression after the first Von Hannover decision by recognizing greater protections for personal privacy when contributions to public debate were minimal, and that the Federal Court of Justice and FCC had upheld an injunction barring publication of the photographs not related to stories about Prince Rainier's failing health. On these facts, the ECtHR held that the German courts had acted reasonably and had complied with their positive obligations under Article 8.

Interestingly, despite finding a much broader right to privacy in public spaces, it is unclear how (and whether) the ECtHR's case law would support a conclusion that mandated disclosure of footage or other personal information about individual citizens under the Washington State PRA would be (legally speaking) a violation of privacy. However, given this enhanced recognition of a broader right to privacy for even public activities that are not of great public interest, it is conceivable that the disclosure of certain police recordings (ala body-cameras, for example) might not be permissible under Article 8 of the ECHR.

4.6. Public outrage over public access

It may be useful to situate this current state of affairs in Washington State with a few other recent examples of public disclosure leading to public outcry in the name of protecting privacy interests. These recent developments highlight the building tensions between FOI laws and the personal privacy interests of individual members of the public. As government agencies increasingly collect, use, sell, share, and archive personal information for various purposes (whether to protect national security interests, facilitate more efficient policing, or administer government programs), the informational privacy rights of individuals are potentially threatened. And this threat is only increased when this personal information is also publicly accessible under local or national FOI laws. This apparent tension between privacy and the administration of government programs and government transparency pits these two ideals directly against each other. Open access to government information serves as an important check on government power and abuse; one used by journalists and others for very legitimate reasons. Privacy rights in personal information also provide some check on government overreaching, as demonstrated by the Fourth Amendment's prohibition on unreasonable search and seizure and by the line of decisional privacy decisions handed down by the United States Supreme Court following Griswold v. Connecticut (1965). In some instances, these tensions have been highlighted by the online mapping of publicly accessible geo-spatial information, and these developments have spurred both legal change and public outrage. It should also be noted that this type of willing disclosure by law enforcement indicates either 1) a strong commitment to a high level of departmental transparency, and/or 2) simply an absence (for whatever reason) of any relevant state public records exception that might be used to deny these disclosure requests. The latter is generally the case in Washington, and is specifically the case when considering mandated disclosure of almost all ALPR database information and body-camera footage.

4.6.1. The New York gun map

In response to the tragic shootings at Sandy Hook Elementary in Newtown, Connecticut in December 2012, a suburban New York state newspaper filed public records requests for the personal information of all pistol permit holders within three nearby counties. Subsequently, the paper generated and published an interactive online map that included the names and addresses of each of the individuals who had pistol permits in two of these counties (Rockland and Westchester) (Moos, 2013). The newspaper received the gun permit information through public records requests, and the data was released as publicly accessible information under state FOI law.

Needless to say, the map—sourced from publicly available information—caused quite a controversy. In response, the New York legislature quickly passed the New York Secure Ammunition and Firearms Enforcement Act ("NY SAFE Act"), which amended the state Penal Law to allow gun owners to request that their permit applications become exempt from public disclosure.[31]

Following the enactment of the NY SAFE Act, the newspaper took its map offline (Khouri, 2013). The amended state Penal Law also had some slightly counter-intuitive ramifications. Prior to enactment, pistol permit holders' personal information had been shielded from disclosure to commercial entities seeking to use the information for marketing purposes, but not to the broader public. After the NY SAFE Act came into force, however, this personal information was no longer shielded unless the individual permit holders file the appropriate form seeking an exemption (Coin, 2013). Thus, marketing companies now gain greater access to this personal information, unless individual gun owners take affirmative steps to protect their privacy.

4.6.2. Proposition 8 donor map

While information about donations to political campaigns or ballot initiatives can serve a valuable purpose, releasing this information publicly may also lead to harassment and disincentive political donations from citizens who are concerned about being publicly associated with a sensitive political position (cf. Munson, et al., 2012; 2011). This scenario was played out clearly when personal information of donors to the campaign for California's Proposition 8 in 2008, which would have prohibited same-sex marriages in California, was overlaid onto Google Maps, thus allowing a visual, map-based, searchable database of Proposition 8 supporters (Stone, 2009). As a consequence, supporters were targeted with death threats, scare tactics, and boycotts of supporter-owned businesses (Stone, 2009). California access law made names, zip codes, employer information, and donation amounts public. While exact addresses and contact information were not included in the released data, this information could easily be determined using simple web-based services.

4.7. Conclusion

A clear problem for an absolute right to control the initial release and the subsequent use of personal information is implicated when the information is voluntarily exposed to public view (or is subject to public access, even if not openly exposed). The current state of the law in Washington state aligns itself with the proposition that government agents generally have the legal right to record encounters with civilians (in public or private spaces) and capture images of their license plates. Under the PRA, public agencies, including police departments, are required to disclose much of this information (including personally identifiable information in many cases) to anyone who requests it. If defining informational privacy as the right to control access to and uses of

[31] See "Public Records Exemption - FOIL Form FAQ." New York Division of State Police, http://www.troopers.ny.gov/Firearms/Public_Records_Exemption (last visited Jan. 12, 2015).

personal information is a viable option, this definition could explicitly recognize that individuals should have some rights to control not just access to their personal information, but also some subsequent uses of that information, even after disclosure to (or capture by) third parties in certain circumstances (Moore, 2010, p. 16; 2007, pp. 812-13). This definition also recognizes that certain actions may waive, explicitly or impliedly, a privacy interest. Additionally, the mosaic theory of the Fourth Amendment recently considered in the wake of recent decisions in United States v. Jones (2012) and United States v. Maynard (2010) can also inform this definition. A person's right to limit access to and use of certain personal information (e.g. a person's current or past geographic location) that has not been kept strictly "secret" by virtue of the fact that is was available in a public space could still, in some circumstances, remain legally enforceable under the Fourth Amendment's guarantee of freedom from unreasonable search or seizure.

The holdings in cases such as Von Hannover v. Germany (2004) and Sciacca v. Italy (2006) at the European Court of Human Rights also provides a glimpse at an alternative approach to considering the balance between privacy and access to information. Because the free speech/access concerns at issue in those cases did not necessarily relate to matters of public interest (defined narrowly, and excluding mere curiosity (*see* Moore, 2013)) or further aims of democratic deliberation, the right of privacy (as the right to control the use of personal information) could prevail over the right to free expression. In the succeeding chapters, I explore the proper balance between privacy rights and public access to information against the particulars of the right to record police activity (Chapter 5), the use of body-cameras by police and subsequent disclosure of footage (Chapter 6), and the collection and disclosure of ALPR databases (Chapter 7). Finally, in Chapter 8, I offer my normative conclusions, referring back to the laws outlined in this chapter and applied to real-world scenarios in chapters 5-7, in my development of a particular theory of information policy.

5. Automated license plate recognition, privacy, and public access to government surveillance information

5.1. Introduction

Automated license plate recognition technologies are becoming increasingly utilized for a variety of purposes by both private and public entities. These systems, also referred to as automatic license plate readers or, outside the USA, as automated *number* plate readers (collectively referred to herein as "ALPR"), essentially consist of high-resolution cameras mounted onto vehicles or stationary objects that capture images of the license plates of passing vehicles. These images are interpreted using optical character recognition software and the interpreted plate numbers are compared against national, regional, or local watch lists of license plate numbers associated with vehicles or individuals wanted by the authorities, prompting officers to respond in real-time (or near-real-time) to scans of wanted vehicles whenever a "hit" against one of these databases occurs. Law enforcement departments use the systems to identify stolen vehicles, locate suspects in on-going investigations, and enforce municipal parking regulations, among other things. Private entities have also been amassing their own databases of license plate scan data (whether by scanning plates themselves or by buying database information from other public or private entities), and have been selling the associated information, including plate numbers, geo-location data, and time stamp information, to other commercial interests. These systems, whether in public or private hands, promise the ability to provide meaningful records of the movements of identifiable individuals (although, in the case of shared automobiles, this is obviously not a direct one-to-one match).

ALPR is not generally capable of tracking civilian vehicle movement with the granularity of GPS tracking technologies (e.g. in-car GPS or via the attachment of GPS tracking devices to a vehicle) such as those at issue in United States v. Jones (132 S.Ct. 945), although this is largely a function of limited camera placement rather than technological capability. As the technology proliferates and the longitudinal memory of the resulting databases continues to grow, this situation may well change. With large databases and frequent scans of individual plates, the potential exists for large scale privacy intrusions, which are made more substantial given the ability of police agencies and others to perform predictive analytics or draw meaningful inferences about individuals based on past movement patterns.

On the other hand, car-mounted ALPR systems, like other automated vehicle locator technologies (AVL), can provide very accurate and granular details about the movements of the police vehicle to which it is attached, also possibly raising safety and security concerns. These concerns have recently been raised by law enforcement agencies coming out in vocal opposition to the police-location-reporting features in Google's Waze smartphone app (Newman, 2015; NBC Miami, 2015). The popular app has been used by users to tag the locations of police cars and speed traps, and police agencies claim this crowdsourced location tracking puts them at risk (Newman, 2015; NBC Miami, 2015). In response, police in south Florida have been instructed to flood the app

with false information (NBC Miami, 2015). Apparently, undocumented migrants are also using peer-to-peer text-messaging networks to help each other avoid contacts with police officers by posting information about where police are sighted (Noriega, 2015).

In response to growing public discussion about ALPR adoption, a limited number of states have recently enacted legislation to limit ALPR use and/or data collection. Some jurisdictions have been releasing ALPR databases and related information to members of the press and public under applicable state public disclosure laws. Others, such as the Los Angeles Police Department and Los Angeles County Sheriff's Office, have denied requests for disclosure of ALPR scan data on the basis that the data is "investigatory or security" related, an thus exempt under state public records acts (see e.g. Bibring, Salahi, and Lynch, 2013). Given that this ALPR data is collected on the basis that license plate numbers and vehicle locations on pubic roadways attract no reasonable expectation of privacy, thus falling outside the Fourth Amendment's warrant requirement, the refusal to release this information on privacy grounds is somewhat ironic, to say the least.

It should be noted that the ALPR databases at issue contain much more than just the license plate information of each vehicle scanned by the system; they also frequently include identifying information about the patrol vehicle that facilitated the scan, including precise date, time, and geo-location information of each scan, allowing citizens to track the patrol patterns of police vehicles outfitted with ALPR cameras. Thus, in a very real sense, these surveillance technologies used by the government have become a tool for reciprocal citizen surveillance and a mechanism for democratic oversight. However, the potential of ALPR data collection to increase horizontal visibility of subjects (*vis-à-vis* other private persons) through public disclosure requirements, beyond the explicit vertical visibility to the police who are using the technologies, suggests that increased civilian visibility might be an important (un)intended consequence and collateral damage—in essence, a form of *collateral visibility*. When ALPR data is publicly disclosed, the visibility of the state (in terms of the public oversight made possible by the disclosure) is intricately tied to the visibility of individual subjects of surveillance (who may not be spread out equally within communities and along demographic and/or socio-economic boundaries).

Surveillance is, of course, designed to collect information about subjects, which leads to a potential capacity to develop power in the informed over the subject of the collection. Thus, if government agencies are to be allowed to conduct certain forms of surveillance, reciprocal forms of inverse surveillance are needed to properly balance power, check abuse, and ensure the democratic ability of citizens to self-govern without state domination.[32] Thus, the ability of citizens to record the

[32] Reciprocal surveillance is not the only answer here, of course, as simply limiting state surveillance powers in the first place would also restrict the possibility of state domination. These initial restrictions are entirely appropriate to curtail the possibility of arbitrary interference by the state, but I suggest many of these questions should be answered through democratic civic engagement — as antipower can be increased either by prohibiting surveillance in the first place or by restricting certain dominating forms of surveillance in combination with legal and political protections for inverse surveillance, transparency, and oversight. I approach much of this dissertation from the latter

official public actions of police officers and other state actors, or to access records of such activities, may also serve important oversight purposes and, ultimately, help preserve individual liberty. On the other hand, privacy protections need to put in place—as limits on public disclosure—to protect against the collateral, and often unintended, risks to individual privacy.

In this Chapter, I examine how the law regulates ALPR database disclosures in Washington State, as well as how the law ought to balance the inherent tensions between privacy, access to information, and the effective administration of criminal justice. In doing so, I examine how spatial considerations impact how the law does (and should) differentiate between the interests that each of these values encompass. More specifically, I address how the law ought to address the initial collection of license plate scan data, the subsequent use of such data for prosecuting criminal or civil infractions, and disclosure to third parties. Finally, in Chapter 8, I operationalize a republican conception of political freedom (Pettit, 1996; 1997; 2002; 2011; Skinner, 1984; 1998a; 1998b; 2008), analyze it against the case at hand, and evaluate whether (and to what extent) this theory can adequately inform the way we think about the proper relationship between these competing values. Methodologically, I utilize doctrinal legal research, philosophical argumentation, conceptual methods from Value Sensitive Design, and exploratory analysis of several ALPR databases disclosed under access to information law in Washington State in recent years.

5.2. Methodology

In this chapter, I draw upon legal research, analytic argumentation, Value Sensitive Design, and an analysis of several ALPR data disclosures by the Seattle (Washington) Police Department. In February 2015, I also conducted two ride-alongs with police officers in vehicles equipped with ALPR cameras (each ride was between 4 and 5 hours long). I observed the ALPR technologies in use and conducted informal interviews with the officers about their perceptions of the systems as investigatory tools. Both officers had used the ALPR systems prior to my rides, as each of them was officially assigned to the ALPR-equipped vehicles that we rode in.

5.2.1. Legal research

In developing this chapter, I conducted legal research into the regulation of the use of ALPR technologies by law enforcement agencies in Washington State, including state constitutional law, statutory law, decisions by Washington State courts, and federal case law related to the Fourth Amendment to the United States Constitution. To this end, I searched Washington law using Westlaw® Classic, and I also conducted general Google and Google Scholar (case law) searches to identify other relevant issues. For comparison, I also conducted searches of Westlaw's legal database and referred to the National Conference of State Legislatures website (NCSL, "Automated License Plate Readers," 2015) to determine whether legislatures in other states had

perspective, largely as a practical (and possibly pessimistic) consequence of the fact that I see the continued development and deployment of state surveillance as largely inevitable.

adopted statutory laws regulating ALPR use in their jurisdictions. In Westlaw, I searched for statutes and cases using the following Boolean search string: "*automated license plate*" *OR* "*automated number plate*" *OR* "*license plate reader!*" *OR* "*license plate recognition*". I also conducted searches for Fourth Amendment search and seizure cases decided by the United States Supreme Court. (For a more general discussion of this method, see Chapter 2).

5.2.2. Value Sensitive Design

I utilize value scenarios, the value tensions framework, and conduct a stakeholder analysis. Value scenarios are used, not to predict the future, but as an analytic tool to help anticipate what is at stake with various policy and regulatory options and as a communicative tool to help make the issues more readily comprehendible by placing them into narrative form. The value tensions perspective of VSD fits quite well into the larger framing of this dissertation, and helps to ground the analysis in the reality that the values at stake are complicatedly intertwined and—in some sense—need to be brought into balance (or at least alignment). Identifying stakeholders impacted by ALPR data collection and retention also helps to surface the conflicting values at stake and also makes explicit which stakeholders and values are addressed throughout my analysis. (For a more general discussion of this method, see Chapter 2).

5.2.3. Empirical data collection and analysis

I conduct an exploratory analysis of ALPR data disclosed by the Seattle Police Department. Specifically, I use SQL, ArcGIS, and Tableau Desktop to analyze and visualize the databases of license plate scans to help determine what is contained in these data disclosures and what tensions exist between the relevant values. In particular, I analyze three databases disclosed by SPD. The first (database "A") consists of approximately three years of scan data, from February 2008 until March 2011, amounting to over 7.4 million total scans generated by mobile ALPR systems mounted on patrol cars. The second two databases (databases "B" and "C") consist of overlapping scan data collected by two ALPR systems, spanning 87 and 77 days, respectively, in the period between December 2012 and April 2013, for a combined total of over 1.7 million scans generated by cameras on patrol cars (database "B") and parking enforcement vehicles (database "C"). Combined, these databases include information on more than 9.1 million license plate scans captured by the Seattle Police Department.

5.2.4. Philosophical method

After the presentation of findings, I develop an analytic argument while examining and applying theory to the findings of law and to my initial and exploratory data analysis. This methodology carries over into Chapter 8, where I develop my broader normative arguments based on this Chapter as well as the other two cases presented in Chapters 6 and 7. For more specifics on my application of this methodology, see my expanded discussion in Chapter 2.

5.3. The law and ALPR

5.3.1. The Fourth Amendment, ALPR, and privacy in public

The Supreme Court decision in United States v. Jones (2012) (discussed both *supra* in Chapter 4 at § 4.2, and *infra*, this section) was a landmark decision for Fourth Amendment law in general, and the dicta included in the concurrences by Justices Sotomayor and Alito has provided much fodder for the debate about the extension of Fourth Amendment privacy rights to public movements (see e.g. Henderson, 2013; Kerr, 2012; Slobogin, 2012; Newell, 2014b). Prior to *Jones*, the precedential locational tracking case was United States v. Knotts (1983). In that case, the Supreme Court held that police use of a "beeper"—a much more rudimentary and non-exact form of tracking a suspect by radio transmissions (United States v. Knotts, 1983, p. 277)—did not violate the Fourth Amendment because a person does not have a reasonable expectation of privacy in their movements on a public road (United States v. Knotts, 1983, p. 282). In that case, police officers placed the beeper at issue in a container of chloroform prior to one of the codefendants (Petschen) purchasing the container and placing it in his car. In the decision, the court stated that:

> [v]isual surveillance from public places along Petschen's route or adjoining Knotts' premises would have sufficed to reveal all of these facts to the police. The fact that the officers in this case relied not only on visual surveillance, but on the use of the beeper to signal the presence of Petschen's automobile to the police receiver, does not alter the situation. Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case (United States v. Knotts, 1983, p. 282).

This decision granted the government the authority to amplify, or replace, their own visual surveillance of a suspect moving in public spaces with electronic surveillance on the rationale that all of the surveillance could have been done lawfully by actual officers tailing and observing the suspect's movements. This holding, in conjunction with the more general principle (discussed more substantially in Chapter 4) that activities in public spaces do not attract reasonable expectations of privacy, have paved the way for widespread law enforcement use of ALPR technologies.

However, The *Knotts* holding also did more than just allow police to augment pre-existing visual possibilities—despite the comparatively limited information produced by the beeper as compared to modern GPS tracking technologies. For example, at one point the officers in *Knotts* lost sight of the car they were tailing and subsequently fell out of range of the beeper, effectively losing their target (United States v. Knotts, 1983, p. 278). They later found the device using a helicopter to sweep the area scanning for the beeper's signal and located the device near a cabin occupied by Knotts (United States v. Knotts, 1983, p. 278). This use of the location tracking technology did more than simply augment the sensory capabilities of the officers—it allowed them to locate a suspect using purely technological means after the initial tracking had failed. More recently, the more sophisticated use of covert GPS tracking technologies in the *Jones* and *Maynard* cases provides stark contrast to the limited technological capabilities that existed at the time *Knotts* was

decided. As such, the statements by Justices Sotomayor and Alito in *Jones* are particularly important as courts review location-tracking cases in the future.

The facts of (and differing opinions offered in) *Jones* (and that of Judge Ginsburg in United States v. Maynard (2010)) are particularly telling in regards to how current Fourth Amendment treats privacy in public spaces. The *Jones* and *Maynard* cases (which were consolidated at trial) arose after the appeals from the joint convictions of Lawrence Maynard and Antione Jones. In 2004, Maynard managed a nightclub in the District of Columbia that was owned by Jones. That year, an FBI-Metropolitan Police Department task force began investigating the two men (and several other alleged co-conspirators) for narcotics violations. During the course of the investigation, officers conducted visual surveillance of the nightclub, installed a video camera focused on the front door of the club, captured pen register information, and instituted a wiretap of Jones's cellular phone (United States v. Jones, 2012, p. 948). Based on information gathered during this initial surveillance, the officers applied for and obtained a warrant to place an electronic GPS tracking device on an automobile regularly used by Jones (but registered to his wife) (United States v. Jones, 2012, p. 949). The warrant authorized the government to install the device on the vehicle within the District of Columbia within a ten-day time period. Eleven days later, the officers installed the device while the vehicle was in Maryland in violation of the terms of the warrant—a claim the government admitted to in the litigation, while still maintaining that a court order was not required by law in the first place. Eventually, Maynard and Jones were tried jointly and convicted of various drug related offenses.

On appeal, the Circuit Court for the District of Columbia reversed Jones's conviction based on his claim that the government's warrantless GPS tracking of his vehicle 24 hours a day for 28 days violated his Fourth Amendment rights (United States v. Maynard, 2010, p. 558). Importantly, while announcing what has become called the "mosaic theory" of the Fourth Amendment, Judge Ginsburg found that:

> Unlike one's movements during a single journey, the whole of one's movements over the course of a month is not *actually* exposed to the public because the likelihood anyone will observe all those movements is effectively nil… [and] the whole of one's movements is not exposed *constructively* even though each individual movement is exposed, because that whole reveals more—sometimes a great deal more—than does the sum of its parts (United States v. Maynard, 2010, p. 558).

Traditionally, the legality of government searches has been determined by what Orin Kerr calls the "sequential approach" (Kerr, 2012, pp. 314). Under this approach, courts "analyze whether government action constitutes a Fourth Amendment search or seizure [by taking] a snapshot of the act and assess[ing] it in isolation" (Kerr, 2012, pp. 315). According to Kerr, the "step-by-step" or "frame-by-frame analysis" is inherent in and foundational to evaluating Fourth Amendment claims (Kerr, 2012, pp. 316). However, in *Maynard*, Judge Ginsburg "likened the aggregate of Jones's movements to a mosaic, where the whole is more than the sum of its parts" (Dickman, 2011, p. 736). Ginsburg compared this case of prolonged modern surveillance with prior national security

cases where the government regularly invoked the "mosaic theory" to shield certain otherwise public records from disclosure under the Freedom of Information Act because, "[w]hat may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene" (United States v. Maynard, 2010, p. 558, *quoting* CIA v. Sims, 1985, p. 178). Thus, according to Ginsburg, the difference between the whole array of potentially public information and any distinct part "is not one of degree but of kind" (United States v. Maynard, 2010, p. 562). Judge Ginsburg continued by stating that:

> [p]rolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts (United States v. Maynard, 2010, p. 562).

Apparent support for these ideas by some of the Justices at the Supreme Court (*see* United States v. Jones, 2012, Sotomayor J. concurring) may signal that the court is open to reform the Fourth Amendment analysis in line with the mosaic theory—although in subsequent decisions the Court has not yet done so, relying again on the trespass doctrine in Florida v. Jardines (2013).

In his opinion in *Maynard* (2010), Judge Ginsburg of the D.C. Circuit focused on whether the government's investigation caused them to learn "more than a stranger would have observed" (Kerr, 2012, p. 330). Early commentary has resulted in both academic praise and criticism of the idea of a mosaic theory. Considering information collection and government surveillance practices in the aggregate could potentially help modernize existing theory. Doing so also reflects a pragmatic approach to respecting forms of informational privacy that may comport with legitimate expectations of privacy despite not necessarily being consistent with existing Fourth Amendment jurisprudence. However, critics express concern that implementing this new theory would throw Fourth Amendment law into deeper chaos and will require the courts to confront an expansive array of practical questions and draw more arbitrary lines without precedential guidance (Kerr, 2012, pp. 314-15).

Some scholars have claimed that recent (and even not so recent) advances in digital technologies and surveillance capabilities mean that we should rethink whether we can maintain any legitimate expectations of privacy while out in public—or in "public facts." In these cases, spatial considerations—often all on their own—are the primary consideration referred to when determining whether the information is public or private. In *Jones*, Justice Sotomayor proposed that the secrecy/no-secrecy dichotomy should be abandoned (or at least rethought) in the face of

confronting Fourth Amendment challenges related to investigative use of new technologies (United States v. Jones, 2012, p. 957, Sotomayor J. concurring). Justice Alito's separate concurrence in *Jones* expressed concern about the robustness of the "reasonable expectations of privacy test"—even while advocating its use in that case—because of the potential that the widespread use of new surveillance technologies could resign the populace to subjectively expect less privacy than should be afforded under the Constitution (United States v. Jones, 2012, p. 962-63, Alito J. concurring). Indeed, geolocation tracking technologies—which have now been used by law enforcement agencies for some time—allow law enforcement to easily compile thousands of pages (or rows) of information about our present and past travels—in very exacting detail—and to mine that information indiscriminately for patterns (United States v. Jones, 2012, p. 948; see also e.g., People v. Weaver, 2009, p. 1199). These realities have undoubtedly changed the privacy calculus confronting individuals when they enter public spaces, for engaging in necessary activities (e.g. to work, eat, go to school) or for purely consensual recreational reasons, as technology—and its attendant surveillance capabilities—have made anonymity and targeted visibility much more likely.

Expressing a similar concern, Justice Sotomayor stated:

> In cases involving even short-term monitoring . . . GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. The Government can store such records and efficiently mine them for information years into the future. And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility" (United States v. Jones, 2012, p. 955-56, Sotomayor J. concurring).

Despite the radical shift that such dicta might indicate for the future of Fourth Amendment doctrine, Justice Sotomayor's call for greater protections for some activity occurring in the public sphere is not the first time the idea has been suggested in the courts. In the *Katz* decision itself, Justice Stewart stated that:

> [w]hat 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 (Katz v. United States, 1967, p. 351 (emphasis added; citations omitted)).

Despite the recent move by the court back to a focus on physical trespass, it is likely the court may hear another case in the not-too-distant future that requires an examination of the reasonable expectations of privacy test in the context of location tracking.

5.3.2. ALPR regulation by state law

Relatively few states have passed legislation that specifically regulates the use of ALPR systems, either by public or private entities (Newell, 2014b), and Washington State is not among them. In 2014, at least 19 states had legislation introduced or pending, and in 2015 (as of February 19, 2015)

legislation has been introduced or was pending in 13 states (NCSL, "Automated License Plate Readers," 2015). Presently, only ten states in the U.S. have laws on the books that directly regulate the use of ALPR systems in some way by law enforcement (see Crump, 2013, p. 31 (noting only five states had ALPR legislation at the time)) and at least two others have regulated ALPR use by a directive from the state Attorney General's office (Dow, 2013). Most of these laws were adopted in 2013 or 2014. Additional states have toll collection or traffic stop statutes that refer to ALPR (see Arizona Revised Statutes § 28-7751(3), (16); Maryland Code, Transportation § 25-113(a)(6)(ii)(4)), and some states have case law precedent related to the use of ALPR for various purposes, including traffic stops (see Hernandez-Lopez v. State, 2013; People v. Davila, 2010). In the six states with enacted legislation, regulation is not at all consistent.

Washington State law does not directly address ALPR use or data collection. This fact has contributed to the resulting routine disclosure of ALPR databases by police agencies within the state. Until recently, Minnesota also permitted disclosure of ALPR data. However, after the public disclosure in 2012 of an ALPR database and the subsequent publication of the location of 41 scans of the Mayor's license plate contained in the data (see Figure 1) (Crump, 2013, p. 3; Roper, "City Cameras," 2012; Roper, "Police Cameras," 2012) the state instituted a temporary data classification that exempts ALPR data from public disclosure in that state until August 1, 2015, or until the Minnesota Legislature acts on the issue, whichever occurs first (Minnesota Department of Administration, "Current Temporary Classifications").

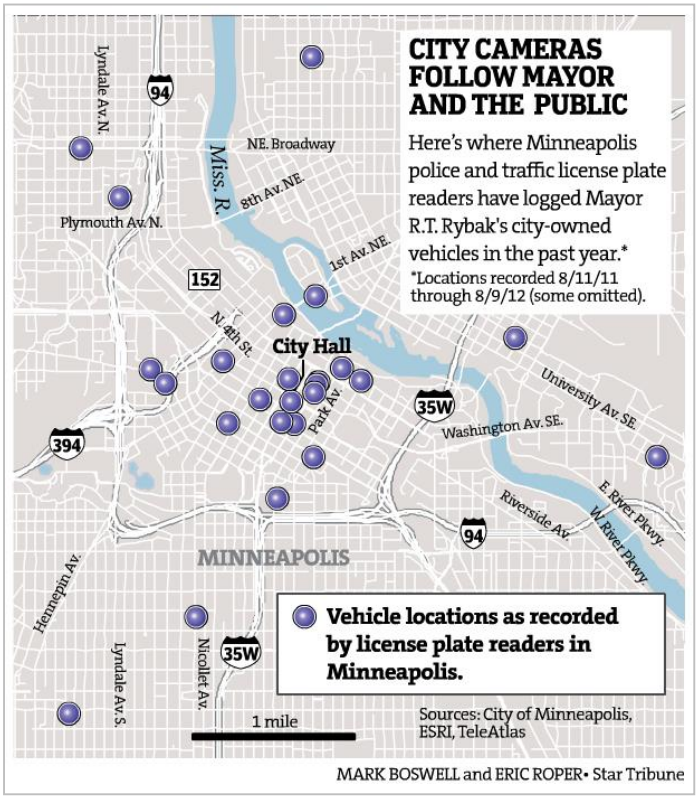


Figure 1. The Star Tribune published this graphic on Aug. 17, 2012, leading to the temporary exemption of ALPR data from public disclosure.

The American Civil Liberties Union applauded the temporary classification in Minnesota (Crump, 2013). At present, both the Minnesota House and Senate have proposed and passed bills that would classify ALPR data as private (with the exception of administrative information, such as the number of ALPR cameras in use). Neither of these bills has yet been signed into law.

The following subsections outline the approach taken on those jurisdictions that do have some ALPR regulation in place.

5.3.2.1. Arkansas

In 2013, the Arkansas General Assembly enacted House Bill 1996, the Automatic License Plate Reader System Act, to regulate the use of ALPR systems within the state (see Arkansas Code § 12-12-1801 *et seq*.). The Arkansas law also prohibits ALPR use, both by private and public entities (Arkansas Code § 12-12-1803(a)), and provides a number of exceptions where such use is permitted for certain purposes (Arkansas Code § 12-12-1803(b)). It also limits the use of ALPR data as evidence in court when the act is violated, and provides for a private cause of action (Arkansas Code § 12-12-1807(a)), including a clause allowing costs and the greater of actual damages or $1,000 per violation, for violations of the ALPR limitations (Arkansas Code § 12-12-1807(b)). Private use is only permitted when such systems are used to control access to secured areas not accessible to the public (Arkansas Code § 12-12-1803(b)(3)) or to regulate the use of parking facilities (Arkansas Code § 12-12-1803(b)(2)). However, government parking and law enforcement agencies can also use ALPR systems to regulate the use of parking facilities or to compare captured plate data against hot listed plate information from certain specified sources, respectively (Arkansas Code § 12-12-1803(a)-(b)).

The Arkansas law also provides some thoughtful regulation of the retention and sharing of captured plate data. Generally, ALPR data captured may not be shared, sold, or disclosed to other entities (Arkansas Code § 12-12-1804(d)(1)), except that law enforcement may share captured plate data with other law enforcement agencies as long as the scan data is evidence of an offense (Arkansas Code § 12-12-1804(d)(2)). Otherwise, captured plate data may not be used for purposes other than those discussed above. Non-hit data must also be deleted within 150 days of initial capture (Arkansas Code § 12-12-1804(a)) and, to help ensure compliance, the law also requires law enforcement to update their databases every 24 hours (Arkansas Code § 12-12-1804(c)). However, data collected by law enforcement that is related to an on-going investigation may be retained until the conclusion of criminal proceedings (Arkansas Code § 12-12-1804(b)).

The Arkansas Act does generally exclude public access to actual ALPR scan data, and restricts disclosure only to, or with the consent of, the person to whom the vehicle is registered (Arkansas Code § 12-12-1808(a)(1); *see also* § 12-12-1805(b)(4)). The law also requires entities using ALPR systems to promulgate official policies (Arkansas Code § 12-12-1805(b)(4)), and to compile and retain regular statistical reports to provide the public with information about the use and efficacy of the technology (Arkansas Code § 12-12-1805(a)). In particular, the law requires disclosure of the total number of scans, the number of scans resulting in arrest and prosecution, the names of the hot list categories that plate data was compared against, the number of confirmed hits or matches with information in the hot listed categories, and the total number of false positives (e.g. matches improperly made due to faulty character interpretation by an ALPR system's character recognition software) (Arkansas Code § 12-12-1805(b)(1)-(3); *see also* § 12-12-1808(a)(2)).

5.3.2.2. California

California's Vehicle Code authorizes the California Highway Patrol (CHP) to utilize ALPR data but limits retention to 60 days, unless the "data is being used as evidence" in a felony case

(California Vehicle Code § 2413(b)). The Code mandates internal monitoring for unauthorized use of ALPR data (California Vehicle Code § 2413(d)) and also specifies that the CHP,

> shall not sell LPR data for any purpose and shall not make the data available to an agency that is not a law enforcement agency or an individual who is not a law enforcement officer. The data may be used by a law enforcement agency only for purposes of locating vehicles or persons when either are reasonably suspected of being involved in the commission of a public offense (California Vehicle Code § 2413(c)).

The CHP must also submit information about ALPR usage (including data disclosures) to the state legislature as part of its annual vehicle theft report (California Vehicle Code § 2413(e)). In addition to CHP usage, many other jurisdictions in California maintain ALPR systems, and the Northern California Regional Intelligence Center (NCRIC) coordinates ALPR data from over 20 police departments (see Crump, 2013, p. 22).

5.3.2.3. Colorado

In April 2014, Colorado enacted new limits on the retention of "passive surveillance records," including ALPR scan data (Colorado Revised Statutes § 24-72-113(1)). The statute generally limits retention to three years, and regulates access to the records after the first year, post-creation of the records (Colorado Revised Statutes § 24-72-113(2)(a)). Under the law, government employees can only access records that are more than one year old,

> "if there has been a notice of claim filed, or an accident or other specific incident that may cause the passive surveillance record to become evidence in any civil, labor, administrative, or felony criminal proceeding" (Colorado Revised Statutes § 24-72-113(2)(a)).

In these circumstances, records may be retained for beyond three years (Colorado Revised Statutes § 24-72-113(2)(a)).

Importantly, the law does not apply to toll collection records (e.g. ALPR use for toll collection purposes), to non-routine surveillance only conducted in response to specific events (Colorado Revised Statutes § 24-72-113(1)), or to records created by corrections facilities, jails, juvenile facilities, and private prisons, or records mandated by federal law (Colorado Revised Statutes § 24-72-113(2)(b)).

5.3.2.4. Florida

In June 2014, Florida adopted Senate Bill 0226 (Florida Statutes § 316.0777), which retroactively makes "personal identifying information" captured or created by ALPR systems exempt from public disclosure under state law (Florida Statutes § 316.0777(2)(a)-(b), (4)). The exemption does not apply to official use within criminal justice institutions, or to disclosure to the individual subject of the data collection, unless "unless such information constitutes active criminal intelligence information or active criminal investigative information" (Florida Statutes §

316.0777(3)(b)). The law will automatically be repealed, due to the law's sunset provision, on October 2, 2019 (Florida Statutes § 316.0777(5)).

5.3.2.5. Maine

Maine's Motor Vehicle Code prohibits private use of ALPR technology and places restrictions on government use of such systems (see Maine Revised Statues, Title 29-A § 2117-A). Interestingly, Maine's statute covers a much more limited set of technologies than the New Hampshire law, defining ALPRs more narrowly. Another section of the code, however, also restricts the ability of government agencies from enforcing traffic violations through the use of red-light or other traffic surveillance cameras (Maine Revised Statues, Title 29-A § 2117). Under the Maine law, ALPR is defined as a "system of one or more mobile or fixed high-speed cameras combined with computer algorithms to convert images of registration plates into computer-readable data" (Maine Revised Statues, Title 29-A § 2117-A). Exceptions allow law enforcement and the Maine Turnpike Authority to use ALPR for toll enforcement (Maine Revised Statues, Title 29-A § 2117-A(1)). The statute also allows the Maine Department of Transportation, the Department of Public Safety's Bureau of State Police, and other state and local law enforcement agencies to utilize ALPR for certain stated purposes (Maine Revised Statues, Title 29-A § 2117-A(3)).

To alleviate privacy concerns, the statute restricts the ability of law enforcement officers to enter data into the system that does not relate to an ongoing investigation or that is not based on articulable facts suggesting safety concerns or criminal wrongdoing (Maine Revised Statues, Title 29-A § 2117-A(3)), and any non-hit data (or data not retained by the Bureau of State Police for motor vehicle screening purposes) must be purged from the database within 21 days from initial capture (Maine Revised Statues, Title 29-A § 2117-A(5)). The statute also specifically exempts ALPR data from public disclosure under the state FOI law (Maine Revised Statues, Title 29-A § 2117-A(4)), which obviously protects the privacy of individual drivers and vehicle owners but limits the availability of data that could be used as a tool of public oversight.

5.3.2.6. Maryland

In Maryland, captured ALPR data is at least partially managed by the Maryland Coordination and Analysis Center (MCAC), a fusion center established shortly after 9/11, to coordinate "the efforts of federal, state and local agencies to gather, analyze, and share intelligence information with law enforcement, public health, and emergency responder personnel" (MCAC, "About"; Maryland Code § 3-509(a)(5), (c)(2)). Under the law, law enforcement agencies "may not use captured plate data unless the agency has a legitimate law enforcement purpose," and individual employees who violate this provision are subject to possible imprisonment for up to one year and a $10,000 fine (Maryland Code § 3-509(b)(1)). Agencies who use ALPR must establish certain policies and audit procedures (Maryland Code § 3-509(c)).

In terms of transparency, the Maryland Public Information Act generally exempts ALPR data from disclosure (Maryland Code § 4-236; Maryland Code § 3-509(d)). Beginning in 2016, agencies

within the state that use ALPR technologies will be required to provide reports on ALPR use to the state legislature (Maryland Code § 3-509(d)).

5.3.2.7. New Hampshire

In New Hampshire, the state's Highway Surveillance law strictly prohibits the use of ALPR systems (New Hampshire Revised Statutes § 261:75-b), as well as other forms of technologically-aided means of "determining the ownership of a motor vehicle or the identity of a motor vehicle's occupants on the public ways of the state or its political subdivisions" by state or local government agents (New Hampshire Revised Statutes § 236:130(I)). This prohibition extends to the use of "any" device, including cameras or other imaging devices, a "transponder, cellular telephone, global positioning satellite, or radio frequency identification device," when used to determine the ownership of the vehicle or identity of a person inside the vehicle (New Hampshire Revised Statutes § 236:130(I)).

The law does provide for a number of exceptions, however, and new exceptions became effective in the latter half of 2013. These exceptions allow state agents to conduct such surveillance to facilitate operation of toll collection systems (New Hampshire Revised Statutes § 236:130(III)(e)), to provide security for three named bridges in Portsmouth (New Hampshire Revised Statutes § 236:130(III)(f)), when such surveillance is incidental to state monitoring of state-controlled buildings (New Hampshire Revised Statutes § 236:130(III)(d)), is undertaken "on a case-by-case basis" to investigate specific crimes (New Hampshire Revised Statutes § 236:130(III)(b)), or when images and data are viewed in connection with a specific incident on a public roadway (but recording is not allowed) (New Hampshire Revised Statutes § 236:130(III)(c)).

Importantly, the law also prohibits the state and its political subdivisions from obtaining any information—specifically, ALPR and related data—that it could not collect on its own, regardless of whether the information is from private corporations or other federal or state entities (New Hampshire Revised Statutes § 236:131). This clause limits the ability of law enforcement agencies within New Hampshire to access national license plate scan databases or to receive license plate information from agencies in other states, unless the information-sharing was undertaken in order to investigate a specific crime (or under another exception as noted above).

5.3.2.8. Tennessee

In 2014, Tennessee enacted legislation that limits government ALPR data retention to 90 days, unless it is related to an ongoing investigation—in which case it must be deleted at the conclusion of the investigation or criminal prosecution to which it is related (Tennessee Code § 55-10-302).

5.3.2.9. Utah

Utah also passed ALPR legislation in 2013, with the enactment of the Automatic License Plate Reader System Act with the passage of Utah Senate Bill 196 (2013), which regulates the use of such systems and also amended the state public records law to exclude public access to ALPR data (Utah Code § 63G-2-305(65); see also § 41-6a-2004(1))—with certain exceptions under the state

protected records provisions (Utah Code § 63G-2-202(4); see also §§ 63G-2-2002(4)-(7)) or via certain court orders or a judicial warrant (Utah Code § 41-6a-2004(1)(d)). In 2014, the Utah legislature amended the law by approving two more bills related to ALPR. Utah law also defines ALPR narrowly, with almost identical language as that used in the Maine and Arkansas laws (Utah Code § 41-6a-2002(1) (defining an "[a]utomatic license plate reader system" as "a system of one or more mobile or fixed automated high-speed cameras used in combination with computer algorithms to convert an image of a license plate into computer-readable data.")), and other sections of the law track the language used in the Arkansas law as well. The Act allows broader exceptions than the Arkansas law, however. In addition to allowing law enforcement to compare ALPR scan data with hot list databases, the Utah law also allows police to use ALPR systems "for the purpose of protecting public safety, conducting criminal investigations, or ensuring compliance with local, state, and federal laws" (Utah Code § 41-6a-2003(2)(a)).

The Utah law also allows ALPR use for enforcing parking regulations, to regulate use of parking facilities, controlling access to secure areas, for collecting electronic tolls, and for "enforcing motor carrier laws" (Utah Code §§ 41-6a-2003(2)(a)-(f)). Public agencies must delete data within nine months, unless the data is subject to a preservation request, disclosure order, or properly issued warrant (Utah Code § 41-6a-2004(c)). The law also prohibits selling or sharing ALPR data for reasons not enumerated in the statute, and allows—but does not require—ALPR users to compile aggregated reports or compilations of ALPR data and to conduct statistical analysis of the captured data, as long as the records are anonymized (Utah Code §§ 41-6a-2004(2)(a)-(c)). Finally, the law contains provisions for preservation orders requiring agencies to preserve captured data under certain circumstances (Utah Code § 41-6a-2005). (The 2013 law applied restrictions on ALPR use to private entities as well as governmental agencies, but language limiting private use of ALPR was removed in 2014) (see Utah Senate Bill 51, 2014).

5.3.2.10. Vermont

Vermont's ALPR law was also enacted in 2013 (Vermont Statutes, Title 23 § 1607). It defines an ALPR system just as in Maine, Arkansas, and Utah, but differentiates between "active" and "historical" data (Vermont Statutes, Title 23 § 1607(a)). Active data includes plate information entered into system hot lists and plate data captured by routine use of ALPR systems, whereas historical data is defined as any ALPR data "stored on the statewide ALPR server operated by the Vermont Justice Information Sharing System of the Department of Public Safety" (Vermont Statutes, Title 23 §§ 1607(a)(1)-(3)). Thus, Vermont has legislatively authorized a statewide ALPR database that facilitates information sharing between state and local agencies. As evidenced by an ALPR End User Agreement obtained by the American Civil Liberties Union of Vermont in 2012, the State stored plate information for four years (Vermont Department of Public Safety, "ALPR End User Agreement") prior to enactment of the ALPR law, which limited retention to 18 months in most cases (Vermont Statutes, Title 23 § 1607(d)(2)). This database is the primary repository for ALPR data collected within the state, as the law requires law enforcement agencies using ALPR systems to upload their scan data to the statewide server (Vermont Statutes, Title 23

§ 1607(d)). The Vermont law allows the Vermont Information and Analysis Center, which manages the database, to share historical ALPR data with both Vermont and out-of-state law enforcement agencies for certain law enforcement purposes (Vermont Statutes, Title 23 § 1607(c)(2)(A)).

The statute also requires officers to be certified to operate an ALPR system (Vermont Statutes, Title 23 § 1607(a)(4)), and restricts use of ALPR systems to certain enumerated "legitimate law enforcement purposes" (Vermont Statutes, Title 23 § 1607(a)(5) ("'Legitimate law enforcement purpose' applies to access to active or historical data and means investigation, detection, analysis, or enforcement of a crime, traffic violation, or parking violation or operation of AMBER alerts or missing or endangered person searches"). Officers are also prohibited from accessing active ALPR data or inputting plate information for non-legitimate purposes (Vermont Statutes, Title 23 § 1607(c)(1)(B)). The law requires written requests to review data and limits access to ALPR information collected more than seven days prior to the request (Vermont Statutes, Title 23 § 1607(c)(1)(C)).

For oversight purposes, the law requires the Department of Public Safety to institute internal safeguards to ensure that law enforcement are using the systems in accordance with the law, and also requires the Department to submit an annual report to the State legislature detailing the number of ALPR units in operation statewide, the number of units transmitting data to the state servers, the total numbers of scans submitted by each agency to the state servers, the total number of scans contained in the 18-month state-run repository, the total number of requests for ALPR data from the state database, and the number of these requests fulfilled (for domestic and out-of-state requestors).

5.3.2.11. Virginia

In Virginia, the state Attorney General has issued an opinion limiting state law enforcement from collecting passive ALPR data (i.e. passively scanning and storing every plate passing by) under the Government Data Collection and Dissemination Practices Act (Virginia Code § 2.2-3800). Instead, law enforcement can only use license plate readers to "actively" scan and store plates that have been particularly identified, "evaluated and determined to be relevant to criminal activity" (Cuccinelli, 2013, p. 1).

5.3.2.12. New Jersey

In New Jersey, law enforcement use of ALPR systems is regulated by an Attorney General Directive promulgated in 2010 (Dow, 2010). The Directive itself explicitly recognizes the role of mining ALPR data for detecting suspicious patterns—a form of predictive policing (Dow, 2010, p. 2 ("A careful analysis of stored ALPR data can also be used to detect suspicious activities that are consistent with the modus operandi of criminals")). It also provides guidelines for ALPR use by state and local law enforcement agencies, and requires them to develop policies consistent with these guidelines. These guidelines attempt to ensure that plate numbers are only entered into ALPR hotlist databases for legitimate law enforcement purposes, that ALPR data is only accessible

by appropriate personnel, and to ensure data is "purged after a reasonable period of time" (Dow, 2010, p. 1). Additionally, the guidelines state that law enforcement policies should be designed to permit a thorough analysis of stored ALPR data to detect crime and protect the homeland from terrorist attack while safeguarding the personal privacy rights of motorists by ensuring that the analysis of stored ALPR data is not used as a means to disclose personal identifying information about an individual unless there is a legitimate and documented law enforcement reason for disclosing such personal information to a law enforcement officer or civilian crime analyst (Dow, 2010, p. 1).

5.3.3. ALPR in Canada and the UK

ALPR technology was originally developed in the UK, at Cambridge University, in response to threats from the Irish Republican Army (Gaumont, 2008). Recently, the UK Information Commissioner found that the use of ALPR cameras at every entry and exit point to a small British city (a so-called "Ring of Steel") violated the UK Data Protection Act as being unlawful and excessive (UK Information Commissioner, 2013a; 2013b).

Canadian law enforcement has also been utilizing ALPR systems since initial RCMP testing in 2006 (Denham, 2012). Most recently, and most relevant to the present discussion, the British Columbia Information and Privacy Commissioner (BCIPC) conducted an investigation of the use of ALPR by the Victoria Police Department (VPD) and RCMP in late 2012, concluding that certain practices violated provincial privacy law (Denham, 2012). In particular, the BCIPC concluded that VPD retention of non-hit plate information, and subsequent sharing of this information with the RCMP, violated the Freedom of Information and Protection of Privacy Act (FIPPA). Importantly, the BCIPC stated that:

> FIPPA authorizes the collection, use, and disclosure of personal information for a law enforcement purpose. VICPD collects personal information for the purpose of comparison against the alert listing. Once this comparison is accomplished, the authorized use of information associated with non-hits and obsolete-hits has been exhausted. FIPPA does not authorize VICPD to continue to use this information unless it obtains the consent of the individual that the information is about. VICPD is likewise not authorized to disclose this information to the RCMP (Denham, 2012, p. 6).

This approach, codified in British Columbian law and the equivalent federal legislation, takes significant steps toward respecting personal information privacy as the right to control access to and uses of personal information, even requiring consent for the continued storage and analysis of personal information gathered in a public space. Against the backdrop of recent legal American developments in the D.C. Circuit and Supreme Court—e.g. the *Maynard* and *Jones* decisions—this approach will be well suited to inform the future of Fourth Amendment reform in the United States.

5.4. Value Sensitive Design

Many types of information stored in government records have historically been considered public records—that is, members of the public could demand access to them—but the ease of access to these records has increased dramatically in recent decades as technology has enabled easier ways to access, combine data, and analyze the information (see Munson, et al., 2012, pp. 99, 100; 2011). As the New York Gun Map, Proposition 8, and Minneapolis ALPR examples (see Chapter 4 at s. 4.6, supra) demonstrate, historically public information may see increased exposure through initiatives to collect and visualize the information in easily useable mashups online—which also casts greater visibility on the individuals whose personal information is contained in those records.

Previous VSD literature has explored the tensions between privacy and transparency implicated by the disclosure of public records (Munson, et al., 2012; 2011; Johri and Nair, 2011). In Munson, et al. (2012), the researchers make the important observation that "the common [Human-Computer Interaction] solution of giving users more and better control of their information" may actually work in direct opposition to transparency (p. 100). The "rush to improve the availability of many types of public records by placing them online" also creates considerable tensions between government transparency and privacy that "may have been overlooked" (Munson, et al., 2012, p. 100). Scholars in different disciplines have also raised these concerns as well, including notable work by Helen Nissenbaum (2004) and Daniel Solove (2002)—both critical of public records laws and processes that can potentially violate individual privacy.

In the following paragraphs, I develop two value scenarios to help surface the relevant tensions raised by the collection and public disclosure of ALPR data, to aid in identifying needs and problems associated with these phenomena. In doing so, I focus on elaborating narratives with relevance to the "five key elements" that ought to be addressed in the application of value scenarios under the VSD framework to "develop provocative sketches of the future: stakeholders, pervasiveness, time, systemic effects, and value implications" (Nathan, Klasnja, and Friedman, 2007, p. 2587) and I also identify the stakeholders relevant to each scenario. Both of the following scenarios are based in the possible future described below.

5.4.1. ALPR value scenarios: Overview of a possible future

ALPR cameras have proliferated in recent years. All major cities in the United States now include widespread ALPR camera placement at all street lights and on all police department patrol vehicles. Because of the effectiveness of the technology at locating stolen vehicles and tracking the movements of vehicles suspected of being tied to criminal activity, auto theft rates have dropped considerably, at least within urban environments. Typical legal regulation allows data to be retained by the police for up to 90 days, and allows the police to share current data with local, regional, and national fusion centers that coordinate cross-state information sharing during criminal investigations. The most recent 30 days of ALPR data is also posted publicly to the city's OpenData portal and updated nightly; effectively granting the public immediate access to the databases at no charge as long as they have an internet connection. City crime data and census information are also available via this portal.

5.4.2. Value scenario 1: ALPR disclosure as a tool for citizen oversight

Scenario. Jason and Tina live in a large urban city in the United States that has recently experienced a great deal of police violence and civilian protests. They have become concerned that the local police have been profiling minorities and over-policing neighborhoods—like their own—with large minority populations. Tina and Jason, as computer and database programmers, have the skills to conduct sophisticated analyses of the ALPR databases their city makes available online. Over the course of a year, they repeatedly download the continually updated ALPR database from the OpenData portal and compile the data into one large database. By mapping and running statistical analyses of the scan data, which includes precise latitude and longitude information, they are able to determine that their local police have patrolled neighborhoods with higher minority populations twice as often as largely white neighborhoods. They also find that the police are scanning poorer neighborhoods at a higher rate than more affluent neighborhoods, and that this ratio has been increasing over the past six months despite the fact that crime has been rising in some of the more affluent neighborhoods and decreasing in the neighborhoods with the higher scan rates. The system is also flagging "hits" of wanted vehicles at an equal rate across all parts of the city. Comparing these findings with other police records, Jason is also able to calculate that the police are statistically more likely to respond to a stolen vehicle alert from an ALPR camera when the vehicle's owner lives in a richer neighborhood. They post their findings to their blog, and send them to their city council representatives and the local newspaper. The resulting political backlash causes the city to institute police reforms and a formal process of periodically auditing police ALPR data collection in the future.

Discussion. This first scenario highlights some of the potential oversight possibilities offered by the combination of widespread coverage of ALPR cameras and liberal public disclosure practices. The direct stakeholders appear to include the police department and its staff with direct contact to the ALPR (including officers patrolling with active cameras and the OpenGov portal employees). However, in some sense, any member of the public who accesses and uses the ALPR data can also be considered a direct stakeholder (these individuals may not be limited by proximity, citizenship, etc. but there may be some division by, for example, socio-economic status and the level of internet penetration in lower-income neighborhoods). Indirect stakeholders—those not directly in contact with the technology but "whose lives are affected by various interactions around the technology" (Nathan, Klasnja, and Friedman, 2007, p. 2587)—might include any other member of the community whose information is collected by the system and/or exposed to further visibility by virtue of the public records laws. For example, this could include a person whose plate was scanned resulting in a stolen vehicle alert—a alert which is visible in the database and tied to a specific plate number—despite the system misreading the person's plate number by interpreting a "0" (number) in place of an "O" (letter). However, the outcome here is increased citizen oversight and police reforms that decrease biased and unfair policing practices. Besides privacy and transparency, the efficacy of pervasive ALPR at lowering car theft rates (and possibly increasing arrest and prosecution rates) also implicates values related to maintaining an effective and efficient criminal justice system as well as increasing public safety. Interestingly, even with limited

government data retention policies (in this case, 90 days), public disclosure allows for the expansion in public memory, as requestors could repeatedly request updated information and compile complete historical records over long periods of time even when state agencies are required to destroy the information. This *permanent memory effect* of public disclosure essentially eviscerates the purpose (and privacy protections built into) mandatory data retention limits and increases civilian visibility. For example, even if we required state agencies to purge ALPR data on a daily basis, a requestor under state FOI law could still automate a daily request for data and compile years' worth of data that would otherwise quickly disappear. Thus, limits on data retention—at least on their own—are not an effective means of achieving obscurity and limiting the collateral visibility of civilians. Building self-destruct timers into data that would limit access after a certain period of time would also likely be overcome and would not always guarantee desired results. It would appear that exempting certain types of information (e.g. personally identifiable information, including information that could possibly be used to re-identify or de-anonymize data subjects) contained in these databases would still be a necessary part of an appropriate policy response.

5.4.3. Value scenario 2: ALPR as a tool for stalking and surveillance

Scenario. In the same city as described in the first scenario, above, Terry is part of an informal group of citizens who are generally suspicious of police officers and severely critical of the growing Muslim population in certain parts of the city. Not generally technologists, the group is still capable of utilizing apps that allow them to crowd-source the current locations of police officers and the locations of Islamic sites of interest within the city. After struggling for some time to figure out a use for the ALPR data, Terry figures out that by isolating license plates scanned near mosques and other popular gathering sites for the local Islamic community, they may be able to compile a list of the license plate numbers of many of the Muslim members of the community, as well as when the sites are most likely to have a high number of visitors. Applying these same techniques to determine where police officers generally take their breaks, and where they usually congregate during periods of inactivity, they can also map and predict when and where police officers may arrive at certain locations around the city. Terry posts this information to the group's webpage and various sympathetic online forums, and updates it occasionally when he has the time. Although his group doesn't take any further direct action based on this information, another group uses the license plate numbers of suspected Muslims to identify individuals and send threatening letters. Later, the group uses the information to stage an attack on a local mosque at a time when police presence in that area is predicted to be lighter than usual.

Discussion. This scenario clearly elucidates how the public disclosure of ALPR data can negatively impact innocent third parties (the indirect stakeholders), especially when data covering long periods of time is publicly available (or when public disclosure extends the effective retention of this data, as discussed above). Additionally, the public disclosure of multiple distinct databases, each containing a limited period of scans, can be collected and aggregated over time, remaining even after the law has required the police to delete the data (e.g. after 90 days). As discussed in

response to the first scenario, above, the limited memory intended by the legal requirement for data destruction is overcome by the potential for perpetual memory of the information made possible by public disclosure. As a consequence, any expectation that even innocent scans—i.e. those not triggering any matches against a watch list—will not subsist for long periods of time is unfounded. This scenario also incorporates elements implicating values besides just privacy and transparency, including public safety and officer safety. When any member of the public—a "public" not bounded by geographical constraints—has access to large amounts of longitudinal data about the movements of police officers and the locations of civilians, we allow anyone to create a mosaic of information that can be analyzed to detect patterns and potentially predict future movements, implicating security threats for both police as well as other organizations or individuals (e.g. the mosque and Muslim community cited in the scenario).

5.5. Exploratory empirical findings

5.5.1. Field observation

My field observation of ALPR cameras in operation was minimal, limited to two rides with officers using the systems in February 2015, for a total of about nine hours. The officers demonstrated the cameras to me, and walked me through how the system worked on their on-board laptop computers. Both officers suggested that the cameras were generally useful, primarily for locating stolen vehicles. One of the two officers seemed more positive about the cameras, apparently a consequence of having used it to find a number of stolen cars. As we drove around the officers' assigned beat areas scanning the streets and sidewalks for suspicious persons or those known to be wanted on outstanding warrants, the ALPR system would periodically beep as it scanned most passing plates. During the first few hours, the system did not identify any scanned plates as matching those on one of the relevant watch lists. However, during my ride with the second officer, the system scanned a plate as we were driving through a residential alleyway, and the computer instantly provided an audible "high alert" warning—indicating a possible match—and displayed the scanned plate information on the laptop's screen. The officer backed the patrol car up until we had a good view of the parked suburban that had prompted the hit, and proceeded to compare the plate on the vehicle with that displayed on the screen. "False alert," the officer stated, pointing to the screen. "The system misread the plate." Comparing the two numbers, it was apparent the system had interpreted the letter 'O' instead of recognizing the number '0' on the actual plate. No other hits were initiated during my rides, however officers did manually enter license plates that were sent out over dispatch during the day into the local watch list, as these plates would not be added automatically until the system updated later that evening.

5.5.2. ALPR database analysis and visualization

In this subsection, I present the initial findings from an analysis of ALPR database disclosures by the Seattle (WA) Police Department ("SPD"). The first database includes more than 7.3 million scans from February 2008 to April 2011 (database "A"). The second set of database disclosures includes scan data generated by two different ALPR systems operated concurrently by the SPD in late 2012 and early 2013 (databases "B" and "C"). These two databases cover slightly different

time periods, but do contain about five weeks of overlapping data. The first of these two more recent databases (database "B") consists of ALPR cameras mounted on SPD patrol cars. It is the larger of the two more recent databases in terms of number of scans recorded, with over 1.5 million license plate scans recorded over a period of 87 days from January to April 2013. The remaining database (database "C") contains fewer scans, at just over 277,000 during a 77-day period from December 2012 to February 2013, but also includes photographs of the vehicles scanned (database B also contained photos, but they were not disclosed in this case, though they would have been made available if requested).

Database	A: SPD Patrol Car Database	B: SPD Patrol Car Database	C: SPD Parking Enf. Database	Totals (B+C)
Date range of scan data:	02.08.2008 – 04.11.2011 01.01.2009 – 04.11.2011**	01.09.2013 – 04.05.2013	12.01.2012 – 02.15.2013	-
Span in days (days w/ scans):	1159 (1029)* 831 (815)**	87	77 (63)*	-
Total no. of scans:	7,376,660 7,371,477	1,501,547[33]	277,718	1,779,265
Avg. scans per day:	6365 (7169)* 8871 (9045)**	17,259	3,606 (4408)*	20,865 (21,667)*
Total no. hits:	7,244	3,775	5,885	9,660
Avg. hits per day:	6.25 (7.04)* 8.72 (8.89)**	43.4	76.4 (93.4)*	119.8 (136.8)*
Percent hits:	0.1%	0.25% (less than 1%)	2.1%	1.2%

Parentheticals indicate figures for days when scans actually occurred in the database, as sometimes no scans are represented on specific days.

****The second line of data under Database "A" are figures that represent only the scans in 2009, 2010, and 2011, as the number of scans in 2008 was significantly lower than in the three succeeding years. This data is provided simply as way to visualize how the data collection ramped up after a slower initial period.***

Table 1. The first column presents data from a single disclosure of over three years of data from the SPD from 2008-2011. The remaining columns present information about two databases operated simultaneously by the SPD in 2012 and 2013. Column two contains data acquired through cameras mounted on patrol cars (database "B"). This database was created by the same system that generated the data in Database "A" in column one. The second (database "C") represent data collected by an ALPR system mounted on SPD Parking Enforcement vehicles. Since these systems are operated during an overlapping time period, totals are presented in the far right column.

[33] These totals exclude lines filled with NULL in each column; other system reads are not excluded, so this number may be higher than actual license plate scans.

Each of the three databases contains un-redacted license plate numbers from the scanned vehicles, officer login IDs (or another form of information identifying a user or vehicle), timestamps, latitude and longitude information, as well as other information about which scans resulted in hits. Database A gives a good view of how the use of ALPR in Seattle ramped up over time. Because the two later databases overlap in time (from January 9 to February 15, 2013) they give a fairly accurate depiction of how the two systems were used and deployed during that time period. Consistent with numbers reported by other agencies to the ACLU (*see* Crump, 2013, p. 13), these databases indicate that hits occurred only a fraction of the time (combined, at 1.2 percent of total scans). Interestingly, the three databases only recorded hits between 10 and 210 times every 10,000 scans (representing 0.1% to 2.1% of all scans). The three systems were highly active, especially after January 1, 2009. The two more recent databases suggest SPD's systems were scanning an average of 20,865 license plates every day over the represented time periods. On January 9, 2013, one officer alone scanned over 7,000 plates in a single shift. Together, these mobile systems canvassed a large portion of the city, as represented in Figure 2, above, although certain neighborhoods remained remarkably under-scanned in comparison.

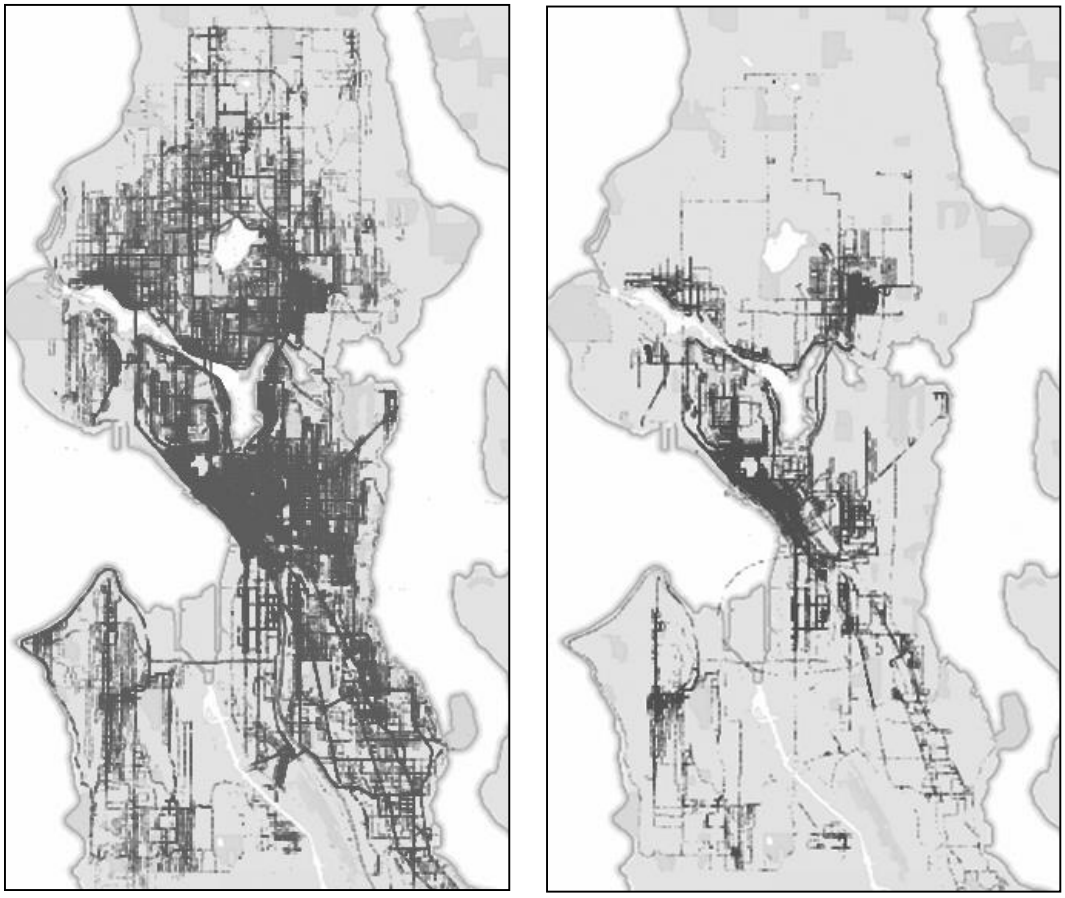


Figure 2. Mapped ALPR data from SPD ALPR databases B and C (cropped to include only Seattle city limits). On the left, the larger patrol car database (B). On the right, the parking enforcement database (C).

Figure 3, below, shows scans made in downtown Seattle by each of the two more recent databases (B and C).

Figure 3. Mapped ALPR data from both the patrol car system (left) (database "B") and the parking enforcement system (right) (database "C"). Each scan is represented by a circle at 20% opacity. Maps do not include roads, so lighter lines represent less dense—but present—scanning activity.

Although scans are concentrated within city limits, the cameras have been used outside Seattle quite frequently. In database A, there is evidence that a police vehicle travelled to Portland, Oregon, scanning plates the entire time. The databases indicate that multiple SPD officers scanned plates outside the Seattle city limits, and one scanned passing plates into the relatively distant cities of Snohomish, Port Orchard, and Fife. Other officers scanned plates in Burien, WA and onto Bainbridge Island (including scanning plates while on the ferry between Seattle and Bainbridge). Because of the detailed nature of the data, it is possible to calculate an officer's rate of speed and to determine which exits were taken and at what times. This information has numerous uses to determine whether the systems are being used in appropriate ways, and also raises a host of interesting questions related to privacy (of the officers and of innocent citizens, including those scanned in areas outside SPD jurisdiction).

Even a single day of data can lead to interesting exploratory findings and provide a glimpse of how the systems are utilized throughout the city. Tables 2 and 3, below, present scan data from both databases on a single day, January 23, 2013. Table 2 presents information from the ALPR cameras mounted on patrol vehicles, while Table 3 presents data from cameras mounted on traffic enforcement vehicles.

User/Login	# Scans	# Hits	% Hits	Scanning Time	Hours	Scans per hour
A	6840	18	0.3%	6:23am – 4:11pm	9:48	698
B	5757	13	0.2%	5:34pm – 11:59pm	6:25*	896.7
C	811	2	0.2%	12:00am – 2:55am	2:55*	278.1
(two shifts)	1046	3	0.3%	7:58pm – 11:59pm	4:01*	260.4
D	1687	5	0.3%	11:48am – 7:47pm	7:59	211.3
E	848	0	0.0%	12:34pm – 6:49pm	6:15	135.7
F	807	2	0.2%	8:32pm – 11:43pm	3:11*	253.5
G	752	1	0.1%	12:25pm – 7:34pm	7:09	105.2
H	428	6	1.4%	7:42pm – 11:56pm	4:14*	101.1
I	221	0	0.0%	12:02am – 12:37am	0:35*	379.1
J	152	0	0.0%	12:10am – 3:35am	3:25*	44.5
K	128	0	0.0%	1:49am – 3:15am	2:26 *	52.7
L	7	5	71.4%	8:49am – 1:13pm	4:24	1.6
Totals	**19484**	**55**	**0.28%**	-	**62:47**	**310.3**
Total (all days in db)	1,501,547	3773	0.25%	-	-	-

*** Partial shift. Additional scans take place prior to, or after, 12:01am or 11:59pm on Jan. 23, 2013**

Table 2. Scan data for scans on January 23, 2013 (Database "B").

Unit	# Scans	# Hits	% Hits	Scanning Time	Hours	Scans per hour
1	3814	99	1.9%	7:21am – 2:36pm	7:15	529.7
	134			4:42pm – 5:01pm	0:19	
	447			8:25pm – 9:43pm	1:18	
	779			11:00pm – 11:54pm	0:54*	
2	4000	45	0.8%	7:56am – 3:08pm	7:12	472.8
	645			4:47pm – 5:44pm	0:57	
	1052			7:59pm – 11:53pm	3:54*	
Totals	10,871	144	1.3%	-	21:54	496.4
Total (all days in db)	277,718	5,885	2.1%	-	-	-

* Partial shift. Additional scans take place prior to, or after, 12:01am or 11:59pm on Jan. 23, 2013

Table 3. Scan data for scans on January 23, 2013 (Database "C"). Broken out when breaks > an hour.

Figure 4, below, drawn from scan data in database B, presents graphically the geographic coordinates of each scan created by two of the SPD patrol cars on the same date.

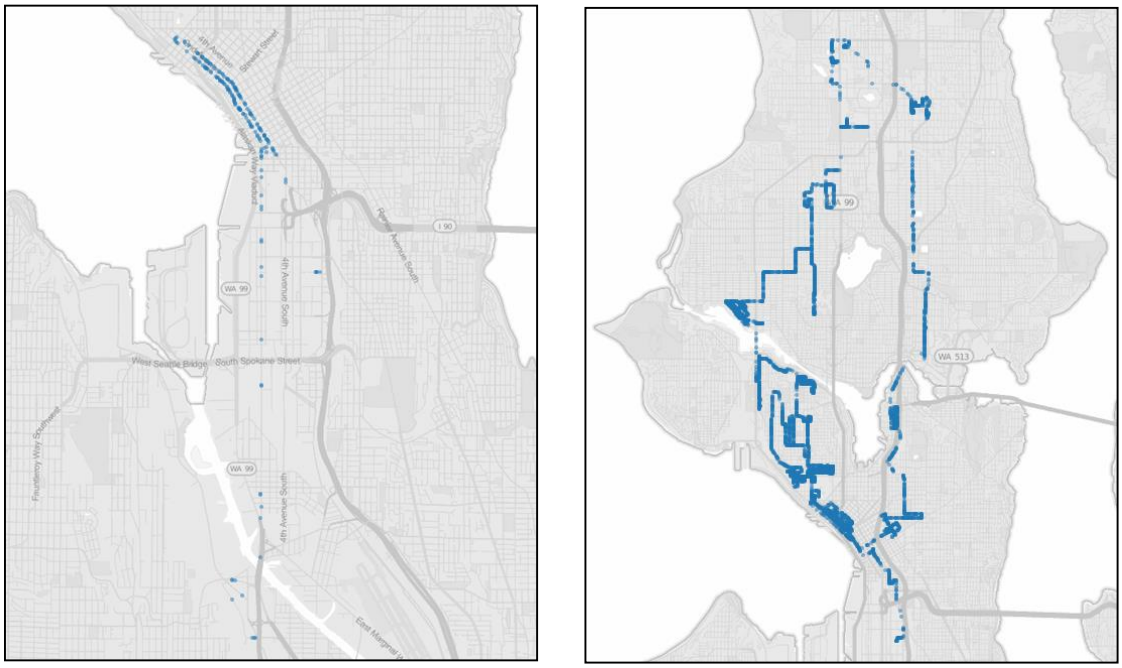


Figure 4. Scans on January 23, 2013 by individual scanning units. From database "B". User/Login (correlated to the identifiers from Table 3, above) "I" on the right (n=221); "B" on the left (n=5757). The data from these two officers on this specific day were chosen because they showed a contrast between the visualization of a small versus a larger amount of scans. In the data represented on the left, turn-by-turn tracking is not readily ascertainable, while it is in the example on the right.

Not every scan returned geolocation coordinates, although most did (76.5 percent for database B; 99.9 percent for database C). On average, the PIPS system also calculated an 87 percent confidence rate in the optical character interpretation; rising to 91 percent for scans resulting in hits. Because each database contains information about individual officer logins (41 unique login IDs in database B; 91 in database C), and many of these officers scan hundreds or thousands of cars in any given shift, the time and location of each scan paints a very accurate picture of officer movements over time.

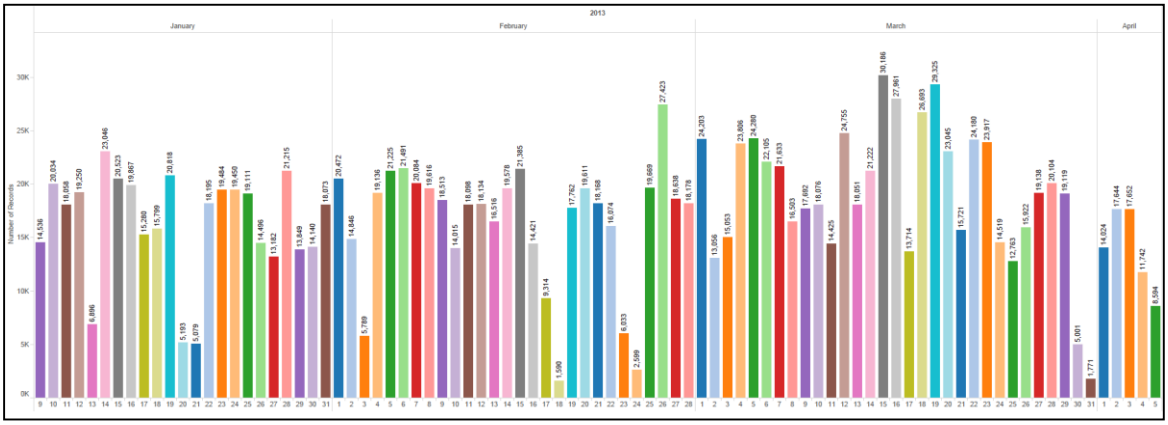


Figure 5. Number of ALPR scans on a daily basis from Jan. 9, 2013 to Apr. 5, 2013, as contained in the SPD PIPS Database (database "B"). Number of days with no scan data: 0. High: 30,186 scans on Mar. 15, 2013.

The following visualization, figure 6, is a color-coded presentation of which U.S. Census Tracts within the city limits contained the highest number of scans (based on data from database B).

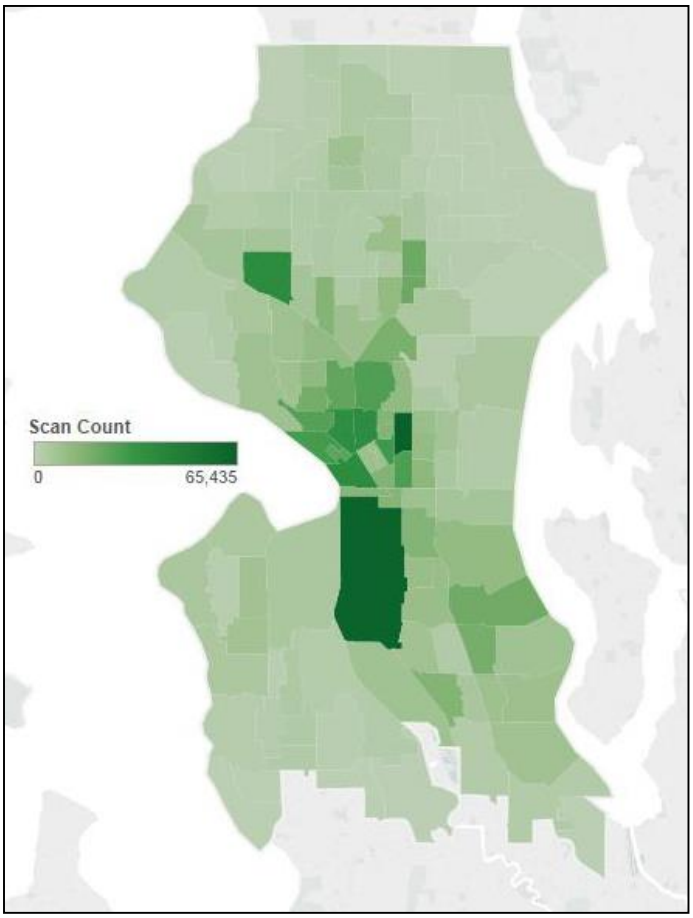
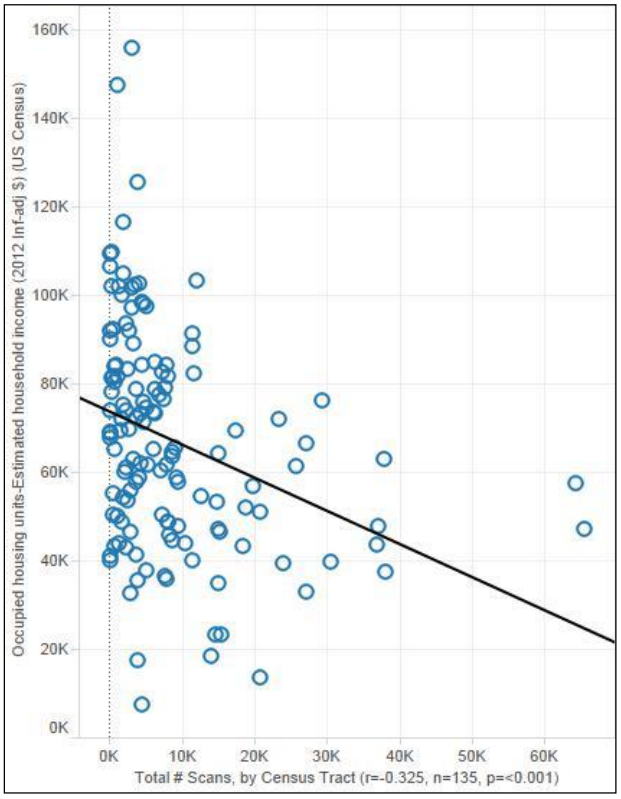


Figure 6. Heat-mapped total scans in each census tract within Seattle city limits contained in database B. Darker value equals higher number of total scans within that area.

Further statistical analysis of this data shows that scan frequency during the time period represented in the database has some correlation to estimated household income ($r = -0.325$, $n = 135$ (tracts), $p < 0.001$) (see Figure 7, below). That is, there is a small, but detectable, correlation between lower income neighborhoods in the city and more frequent ALPR scanning activity (although there appears to be little correlation at the left extreme, when scan density is low). When scan numbers per tract are normalized by geographic land area (in square miles), this relationship remains fairly similar, though the correlation increases slightly ($r = -0.339$, $n = 135$ (tracts), $p < 0.0001$).



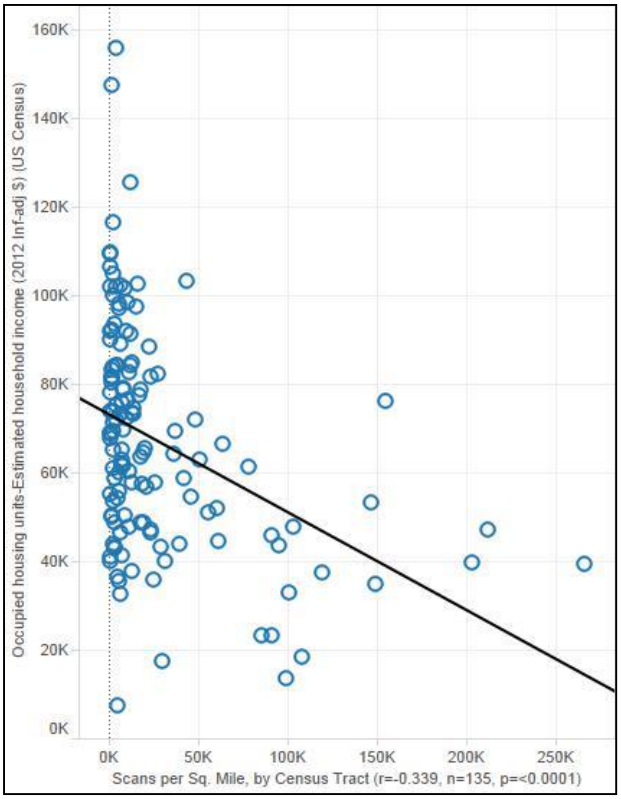


Figure 7. Plotted number of total scans by US Census Tract (of data in database B) by estimated household income. The X axis represents the Census figures for Estimated Household Income for Occupied Housing Units (adjusted). The Y axis is total number of ALPR scans in the database (total n = 1,501,547).

5.6. Discussion

Since the Fourth Amendment generally does not protect against the government's collection of information and mass surveillance in public spaces, many forms of surveillance (e.g. use of drones, surveillance cameras, and license plate readers) may not be subject to any real scrutiny through democratic processes or legal proceedings in courts of law. The legal and practical restrictions on citizens wanting to document or access information about government conduct, combined with the power of government to watch its citizens, represents an imbalanced situation where citizens lack the antipower they might otherwise command. As a result, we should question whether this is a situation in which,

> The powerless are not going to be able to look the powerful in the eye, conscious as each will be—and conscious as each will be of the other's consciousness—of this asymmetry. Both will share an awareness that the powerless can do nothing except by the leave of the powerful: that the powerless are at the mercy of the powerful and not on equal terms. The master-slave scenario will materialize, and the asymmetry between the two sides will be a communicative as well as an objective reality (Pettit, 1996, p. 584).

Of course, one answer in response to this position is that the democratic process, and the potential for participatory democratic governance, has not been curtailed. The people have not been denied access to their representatives or to the courts. However, as exemplified by jurisdictions that have applied blanket exemptions to ALPR data disclosure, the people do not have access to all of the information that supposedly supports the government's need to conduct electronic surveillance and they do not have full access to information about what the government has done with the powers it has been given. This is inherently problematic, especially under the neorepublican position that governments should protect their peoples' freedoms and ensure that the state does not come to dominate its people in any arbitrary fashion. Without some form of effective democratic check in place—some way for the public to make informed, deliberative choices based on real information—abuse (and domination) is always a real possibility. Additionally, when personally identifying information within ALPR databases is subject to public disclosure under FOI laws designed to keep government power in check, violations of individual privacy become part of the unintended collateral damage to these ends of transparency and accountability and civilians have become increasingly visible in the process—a form of what I have called *collateral visibility*. Robust privacy rights, speech, and democratic self-governance, in my view, all fit within the core of what it means for human beings to live flourishing lives—they are all instrumental in supporting and sustaining freedom and antipower.

In terms of ALPR use, deployment, and disclosure, we must strike a balance between allowing large-scale ALPR deployment and the privacy rights of individual citizens or we must limit the use of ALPR in the first instance. Because ALPR deployment has already occurred on a large scale and is unlikely to be abated, and because quickly overturning long-lived legal conclusions about privacy not existing in public spaces, most of my analysis focuses on providing a response to limit the dominating affects of already deployed technologies through arguments in favor of

transparency and preserving civilian privacy by limiting collateral visibility. The disclosure of, for example, un-redacted license plate scan information can easily identify and provide details about specific individuals or groups of individuals (including police or individuals affiliated with religious or other organizations). Public access to this data also risks officer privacy, and limiting access would eviscerate the public's ability to conduct certain types of oversight made possible by access to detailed officer movements—the benefits described in response to the first value scenario, above. Despite all these competing interests, a few conclusions seem apparent, given the obvious perspectives expressed throughout this project. These conclusions do limit public access, but they do so to preserve the privacy rights of innocent citizens and, as a consequence, also protect the privacy of individual police officers.

As a first step, we ought to limit data retention on non-hit scans to a reasonable amount of time. This would have two consequences: 1) it would protect the privacy of innocent citizens (those whose plates are not legitimately on any law enforcement hot list) by limiting the ability of the police to conduct after-the-fact analysis of these individuals' historical movements and, 2) it would limit the ability of anyone to track an officer's precise movements with such great accuracy. There are two potential options for this solution: either we require non-hot data to be purged from the database within a reasonable amount of time[34] or we require the anonymization of non-hit entries in the database (e.g. redacting or randomly altering license plate numbers from the data).

Due to fears of re-identification, we might promote the first option: complete redaction. This option preserves the privacy of innocent motorists as well as the individual officers. On the other hand, this option also significantly limits the citizens' ability to monitor officer use of these systems as only a small fraction of the overall scans would remain, giving a much less accurate picture of policing patterns. The second option would maintain a larger corpus of data, for use both by citizens and the police departments themselves, facilitating data-driven and predictive policing efforts as well as citizen oversight, but does so at the risk of re-identification. For present purposes, without a more detailed analysis of the re-identification risks involved, either of these options represents a drastic improvement in general practice. However, as stated above in the discussion of the first value scenario, information that could be used to identify a specific individual should be redacted prior to public disclosure, in addition to short retention periods, especially for non-hit entries in the database. On the other hand, anonymized ALPR data should not be exempted from public disclosure *in toto*. As evidenced in value scenario 1, above, some disclosure does support vital interests in government transparency. This policy would allow some oversight through public disclosure, and would allow the public to conduct an informed debate about the efficacy and cost of the use of these systems in their communities while also seeking to protect against unnecessary collateral visibility by preserving some elements of obscurity and

[34] In British Columbia, for example, the VPD is required to redact this information at the end of every shift, prior to sharing data with the RCMP.

limiting perfect police memory in an attempt to support Cohen's (2012; 2013) ideas about making room for a "state of play."

Importantly, there are strong reasons to push back against the trend to pull a curtain of secrecy over ALPR data all together. This privacy-weighted conclusion is warranted, to some degree, by the importance of recognizing greater rights of privacy in public spaces, especially when it concerns subsequent aggregation and data-mining of otherwise innocent peoples' personal information. Modern surveillance technologies make it incredibly easy for government agents to track individual citizens discretely and comprehensively for very long periods of time and, as shown in Value Scenario 2, above, the public disclosure of ALPR databases can pose significant safety and privacy issues when the data is used by private citizens or other entities for illicit purposes. If we instituted a policy like that announced here, we would preserve many of the benefits described under scenario 1 while decreasing the potential impact of the *permanent memory effect* on personal privacy. Citizen oversight could still include analyses of ALPR deployment and effectiveness, while not including information connected directly to identifiable civilians. In terms of scenarios 2, not disclosing specific license plate numbers would limit the ability of the group to identify specific plates (or individuals) to potentially sensitive locations such as religious centers. However, should police be scanning mosque parking lots or minority neighborhoods at disproportionately high rates compared to other parts of the community, for example, the redacted data could still support these findings.

5.7. Conclusion

Court decisions finding that citizens do not maintain legitimate expectations of privacy in their public movements and strict application of the third-party doctrine to aggregated forms of government information gathering need to be rethought and critically examined in light of modern technological advances. The unrestricted ability of law enforcement to engage in mass amounts of geolocational surveillance that captures the personal information of innocent individuals, including the use of ALPR, threatens individual privacy and bypasses traditional checks on abusive government actions. The nature and amount of data available about most people's movements—both present and long into the recent past—allows law enforcement to draw inferences about other personal information, and should be subject to the probable cause warrant requirement of the Fourth Amendment. The mosaic theory provides one useful lens and framework for analyzing these sorts of cases. It also "protects the Fourth Amendment from innocuous erosion by society's ready adoption of such technology" even as governmental "use of GPS devices becomes a social norm" (Dickman, 2011, p. 738). The connections between the mosaic theory, Cohen's (2013; 2012) space for a state of play encapsulated within her case for semantic discontinuity, and the concept of obscurity (Hartzog and Stutzman, 2013a; 2013b; Selinger and Hartzog, 2014; 2013) all support reducing state ability to collect (or at least retain in useable form) large amounts of information about civilians without proper justification. These theories would also appear to support redacting personal information prior to disclosure. Both of these requirements—limited retention and non-disclosure—support antipower and limit domination because they limit the

ability of the state and other entities from gaining potentially dominating power over individual data subjects.

On the other hand, advancing technologies and data-mining potentially offer law enforcement greater ability to detect, investigate, and prosecute criminal activity. These concerns for personal information privacy and the efficacy of law enforcement are both very important in contemporary society. The tensions between these legitimate aims is substantial and, in the context of police use of automated license plate recognition (ALPR) systems, limiting the scope of law enforcement data retention to protect citizen privacy might also protect the privacy of the police officers using these systems. Thus, we can serve the interests behind FOI laws, including the implicated First Amendment rights to gather information about government conduct, and personal privacy rights, by limiting long-term retention and the sharing of any non-hit license plate information with other agencies or private companies. The recent practice of the Seattle Police Department demonstrates an applaudable commitment to transparency and, if combined with more limited data retention and laws allowing greater redaction of personal information, of the type described above, would provide a compelling example for managing the risks and benefits of ALPR use.

In the end, perhaps it is best—even essential—that citizens grant their governments some power to restrict public access to information for privacy reasons. Security reasons may also play some role in allowing greater secrecy in some limited cases—though this seems less vital for crime control at the local state or municipal level than when confronting claims of national security—but this does not mean that citizens should not have the right to insist on safeguards, and the right to ensure the government complies with constitutional requirements in the exercise of its power. If that were so, the exercise of power would cease to be arbitrary, and the action would not be subjugating. The people would retain antipower.

6. Civilian (bystander) video and the right to record

6.1. Introduction

In recent years, police officers and law enforcement agencies have been conducting increasingly sophisticated (and intensive) information gathering through visual and spatial surveillance of civilians in public spaces. Law enforcement's past reliance on public and private CCTV for visual evidence of criminal conduct or officer-civilian encounters has now been augmented by the widespread adoption of officer-mounted wearable cameras and dashboard cameras mounted in patrol vehicles. At the same time, however, law enforcement has also been forced to respond to new forms of police visibility enabled by increased civilian-initiated video surveillance of police officers in these same public areas—an example of "sousveillance" (surveillance from underneath) (Ganascia, 2011, p. 489; Mann, Nolan, and Wellman, 2003, p. 332) discussed in the surveillance studies literature. On one hand, the ubiquity of handheld video recording has led to increased visibility of police officer misconduct—such as in the shooting of Walter Scott by an officer in South Carolina in 2015 (New York Times Editorial Board, 2015), the choking death of Eric Garner at the hands of NYPD officers in 2014 (Goldstein and Schweber, 2014; Wasserman, 2015; 2014), officers spraying pepper spray into the faces of non-violent protesters on the UC Davis campus (see Federated Univ. Police Officers Ass'n v. Superior Court, 2013; Chander and Sunder, 2012, p. 1605; Lautt, 2012, pp. 376-377), the shooting of Oscar Grant on a San Francisco subway platform (Antony and Thomas, 2010, pp. 1280-1281), and the death of Ian Tomlinson during the London Riots in 2011 (Greer and McLaughlin, 2010, p. 1049)—but it has also provided law enforcement with a great source of civilian-sourced evidence after unlawful events (such as in the post-event investigations of the Boston Marathon bombings in 2013 (Ackerman, 2013; Wadhwa, 2013; Stroud, 2013; Klontz and Jain, 2013a; 2013b) and the Vancouver Stanley Cup Riots of 2011 (Vancouver Police Department, 2011, pp. 14, 71, 92; Rizza, Pereira, and Curvelo, 2013, pp. 411-412)) that has led to a number of important criminal prosecutions (Vancouver Police Department, 2013). Thus, widespread civilian-initiated visual surveillance through the use of audio-visual recording devices—what I refer to herein as "civilian video"[35]—poses a threat to law enforcement image management and promises both a method of holding individual officers accountable for misconduct and for crowd-sourcing visual surveillance to aid in investigating crime and terrorism.

As the proliferation of high-resolution smartphone and wearable cameras (including technologies like Google Glass with embedded cameras, WiFi connectivity, and information rich data presentation on its lenses) continues, these problems will only increase in importance and

[35] In many places, this is referred to as "bystander video" or "citizen video." I have chosen the term *civilian video* because not all recordings are made by citizens (e.g. some may be made by undocumented immigrants, tourists, permanent residents, or others with various legal status) and not all videos are recorded by bystanders (e.g. they may also be made by the person directly interacting with the police at the time—the suspect him/herself). This choice, however, is complicated by the fact that, when speaking about constitutional rights in the American context, some rights may only be available to citizens—not all civilians—or, even if this were not the case, the non-citizen might have even more to lose should they attract attention for filming police.

visibility. The powerful promise of civilian media to expose state wrongdoing is also underscored by the potential for such footage to go viral on video-sharing websites such as YouTube and on online social media networks. The increased, even ubiquitous, rise in the number of video recording devices regularly recording in public spaces has generated sometimes fierce objection by officers who do not wish to be recorded, and it has also altered the way in which the traditional media reports on policing activity (often with negative implications for police organizations and individual officers) (Greer and McLaughlin, 2010, pp. 1050-1051). However, the ability of civilians to record the official public actions of police officers and other state actors may also serve an important oversight purpose and, ultimately, help preserve individual liberty more broadly. As such, such action ought to be protected by the First Amendment in a way that also preserves personal privacy.

The rise of civilian video—and the related concepts of citizen/civilian media and citizen journalism—has also brought about a wealth of discussion about how existing laws do, or should, protect the rights of civilians to document newsworthy police-civilian interactions and whether (and when) the traditional news media should be afforded greater legal protections than civilians engaged in civilian video-related activities (EFF, "Bloggers' Rights") that might often be described as journalistic to some extent. These debates have ranged from issues regarding bloggers' rights to shield sources (see Obsidian Finance Group, LLC v. Cox, 2011, pp. *2-*3; Johns-Byrne Co. v. TechnoBuffalo, LLC, 2012), state and local statutory definitions of "journalist" (Leslie, 2009, p. 4), and the rights of civilians to record police officers and other public officials engaged in carrying out their official duties (see e.g. ACLU of Illinois v. Alvarez, 2012; Glik v. Cunniffe, 2011). In some states, the act of recording an officer in public may violate state eavesdropping laws and put the offender at risk of criminal charges, even when an officer has no reasonable expectation that the conversation is private (see e.g. Illinois Compiled Statutes § 5/14-1(d); ACLU of Illinois v. Alvarez, 2012, p. 595). In other states, overtly recording officers in public spaces is generally allowed, whether by judicial decisions or more lenient statutory frameworks (see e.g. Gericke v. Begin, 2014; ACLU of Illinois v. Alvarez, 2012; Glik v. Cunniffe, 2011; Smith v. City of Cumming, 2000, p. 1333; Fordyce v. City of Seattle, 1995, pp. 438-439; State v. Flora, 1995; see also Kramer, 2011, pp. 367, 369). In recent years, the increase in civilian media production and the proliferation of camera-enabled mobile technologies like cellphones has impacted the public perception and media portrayal of policing tactics used during large-scale protests and riots, as well as in more ordinary policing situations (Antony and Thomas, 2010, p. 1292).

Video filmed by civilians has found its way into the popular discourse about accountability of policing and government, and millions have witnessed shocking events of alleged police misconduct via online video-sharing websites, the websites of traditional media and press outlets, blogs, and social media. Conflicts between police officers and civilian journalists leading to police arresting civilians for violations of state wiretapping and eavesdropping laws in some states (felony offenses in some cases) (Illinois Compiled Statutes § 5/14-4(a)) are not uncommon (see Lithwick, 2012). Reports of these occurrences have continued to come to light even in some jurisdictions where police departments have explicitly promulgated department policies that recognize that

citizens have constitutional rights to film officers and that have instituted or increased officer training (Fenton, 2013).

As a consequence, state and federal courts have begun to weigh in on the legal rights of civilians to document police action—and the constitutionality of the state wiretapping laws that prohibit such conduct. These decisions have generally recognized a constitutional First Amendment right to film police in public spaces (see e.g. Gericke v. Begin, 2014; ACLU of Illinois v. Alvarez, 2012; Glik v. Cunniffe, 2011; Smith v. City of Cumming, 2000; Fordyce v. City of Seattle, 1995, p. 439; Kramer, 2011, pp. 367, 369). However, the continued proliferation of smartphone applications designed to allow civilians to *covertly* record encounters with police officers in efforts to hold public officials accountable may place some users (perhaps even unwittingly) at serious legal risk. Indeed, activists and organizations such as the New York Civil Liberties Union and the American Civil Liberties Union (ACLU) of New Jersey have distributed smartphone applications designed to allow civilians to covertly record encounters with police officers as part of law enforcement accountability programs, while also actively pursuing litigation (along with other organizations like the National Press Photographer Association) in behalf of photographers and civilian journalists arrested for recording officers (see Lee, 2012). Police agencies are also increasingly adopting their own video recording policies and practices, such as the utilization of dashboard cameras or body-mounted cameras (see Chapter 7 *infra*), as a way to dispel potential violence and document police-civilian encounters (both to provide evidence and protect officers from false complaints) (see Noble, 2013).

Because of the overlap and potential inconsistency between state eavesdropping laws and judicial interpretations of the First Amendment, at least in the states that criminalize the recording of conversations without the consent of all parties to the conversation, the production and practice of civilian media—whether covert or not—raises interesting and important legal issues. In this Chapter, I examine how the law regulates civilian video generally in the United States and specifically in Washington State, as well as how the law ought to balance the inherent tensions between officer and civilian privacy, rights to document and access information about government conduct, and the effective administration of criminal justice. In doing so, I examine how spatial considerations impact how the law does (and should) differentiate between the interests that each of these values encompass. Finally, in Chapter 8, I operationalize a republican conception of political freedom, analyze it against the case at hand, and evaluate whether (and to what extent) this theory can adequately inform the way we think about the proper relationship between these competing values in this context.

6.2. Civilian video and the right to record

In the early hours of the morning on March 3, 1991, George Holliday, from his nearby apartment, covertly recorded Los Angeles Police Department officers beating Rodney King with batons (Gonzalez, 2012). After Holliday sent a copy of the nine-minute video recording to a local television station, it became a media sensation (Myers, 2011). The public outcry over the incident and claims of race-based police brutality—driven in large part by the widespread distribution and

consumption of the recording—ultimately contributed, a year later (after the officers were acquitted of all state law charges), to large-scale riots in Los Angeles and smaller demonstrations in other locations around the country (Myers, 2011). Since 1991, the availability of low-cost handheld video cameras has skyrocketed, as have the number of civilian-produced recordings of alleged police brutality (see Vanhemert, 2010). In many cases, these videos quickly find their way onto prime-time television as well as video-sharing websites like YouTube and are discussed in a wide variety of traditional and emerging media, from print and online newspapers to blogs, Twitter feeds, and Facebook pages (Antony and Thomas, 2010, pp. 1280-1281).

In the past few years, a number of examples of civilian video documenting police violence have surfaced with large amounts of media attention. For example, on January 1, 2009, a number of Bay Area Rapid Transit (BART) passengers recorded BART Officer Johannes Mehserle shooting and killing a young man named Oscar Grant in the back while Grant was lying on a subway platform, supposedly resisting restraint while the officers were attempting to place handcuffs on him at the Fruitvale BART station in Oakland, California (Antony and Thomas, 2010, pp. 1280-1281). Multiple recordings of the killing were uploaded to YouTube, despite officer attempts to confiscate cameras in the vicinity, and the reaction to the videos and news reports fueled both peaceful and violent protests in the days following the incident (McKinley, 2010). In 2010, when Mehserle was convicted of involuntary manslaughter rather than the murder to which he was accused, additional riots broke out across the city of Oakland (see MacAskill, 2010). More recently, on July, 17, 2014, on Staten Island in New York, civilian video captured the arrest and death of 43-year-old Eric Garner after NYPD Officer Daniel Pantaleo put him in a chokehold for refusing arrest "for selling loose cigarettes" (Newman, 2014; Murray, et al., 2014). On December 3, 2014, a grand jury failed to indict Officer Pantaleo for criminal homicide, despite the presence of the video and the fact that chokeholds were against NYPD policy (see Goodman and Baker, 2014). Once again, violent protests broke out in the aftermath of the decision (Goodman and Baker, 2014).

On the other hand, recent controversies surrounding recordings made in public spaces—and the eventual posting of such recordings to the Internet—have not been limited to recordings of police officers. Reports of online vigilantism and public shaming of private individuals have also begun to claim widespread notoriety (see Clune, 2013). So called Internet vigilantes have recorded images and video of people doing stupid things and posted them to the Internet, or have identified individuals from already posted videos or images (see Madrigal, 2013). The subjects of these recordings have been publicly shamed, in many cases their personal and contact information has been posted online, resulting in harassment, embarrassment, or detention by government authorities (see Kalaf, 2012). In one case, a young South Korean woman was nicknamed the "dog poop girl" after she was photographed refusing to clean her dog's mess on the floor of a subway car (Krim, 2005). The image was posted online, and within days the woman's name and address were posted as well. She was subjected to vicious online ridicule and apparently also withdrew from university and considered suicide because of the impact the story had on her personal life (Krim, 2005).

Thus, questions about what conduct is morally acceptable when recording others in public spaces—and what one should do with captured footage or images—is a much broader question than that answered in this Chapter. However, the conflict between certain state eavesdropping laws and a growing body of First Amendment case law provides an important context within which to frame this discussion. Filming police officers and other public officials raises additional and important constitutional issues about what right civilians should have to document and disseminate information about government conduct and the state's ability to prohibit recordings by private civilians. These recordings have proved to be an important and vital tool to hold officials accountable for gross misconduct and the violation of civilians' rights, but the remaining legal and practical uncertainty still means that civilians remain at substantial risk when deciding whether to pull out their smartphones and record the scenes unfolding around them. This is a risk that also implicates an improper intrusion into individual liberty.

6.3. Methodology

In this Chapter, I utilize doctrinal legal research, philosophical argumentation, and conceptual methods from Value Sensitive Design to examine my primary and secondary research questions, posed above in Chapter 1, in the context of the right of civilians to record police officers.

6.3.1. Legal research

In developing this chapter, I conducted legal research into the regulation of civilian (and other) video in Washington State and in other jurisdictions that have all-party consent requirements in their eavesdropping laws, including state constitutional law, statutory law, decisions by Washington State courts, and federal case law related to the First Amendment and interpretations of the constitutional constraints on state laws limiting the right to record. To these ends, I searched both statutory and case law using Westlaw® Classic, and I also conducted general Google and Google Scholar (case law) searches to identify other relevant issues and emergent cases. In addition, I also referenced and verified information contained in reference material provided by the Congressional Research Service (Stevens and Doyle, 2012), Reporter's Committee for the Freedom of the Press (Rasmussen, Komperda, and Baldino, 2012), and the Digital Media Law Project's Legal Guide (DMLP, "Legal Guide").

6.3.2. Value Sensitive Design

I utilize value scenarios, the value tensions framework, and conduct a stakeholder analysis. Value scenarios are used, not to predict the future, but as an analytic tool to help me anticipate what is at stake with various policy and regulatory options and as a communicative tool to help make the issues more readily comprehendible by placing them into narrative form. The value tensions perspective of VSD fits quite well into the larger framing of this dissertation, and helps me to remain grounded in the reality that the values at stake are complicatedly intertwined and—in some sense—need to be brought into balance (or at least alignment). Identifying stakeholders impacted by civilian video also helps to surface the conflicting values at stake, to make explicit which

stakeholders and values are addressed throughout my analysis. (For a more general discussion of this method, see Chapter 2).

6.3.3. Philosophical method

After the presentation of findings, I develop an analytic argument while examining and applying theory to the findings of law and to my initial and exploratory data analysis. This methodology carries over into Chapter 8, where I develop my broader normative arguments based on the case presented in this Chapter as well as the other two cases presented in Chapters 5 and 7. For more specifics on my application of this methodology, see my expanded discussion in Chapter 2.

6.4. The law and civilian video

In about a dozen U.S. states, wiretapping (or eavesdropping) statutes prohibit civilians from making audio or audio-visual recordings of conversations without getting consent from all parties to the recorded conversations (e.g. California Penal Code § 632; Connecticut General Statutes § 53a-189 (all-party consent required for telephonic recording; only one-party consent required for in-person conversations); Delaware Code Title 11 § 1335(a)(4) (although a person may record his own phone calls without getting consent of the other party (United States v. Vespe, 1975, p. 1372; State v. Dorn, 1993, p. *3)); Florida Statutes § 934.03(2)(d); 720 Illinois Compiled Statutes § 5/14-2; Maryland Code, Courts and Judicial Process §10-402; Massachusetts General Laws, Ch. 272 § 99; Michigan Compiled Laws § 750.539c-d (although this may be limited to situations when interception occurs (Sullivan v. Gray, 1982)); Montana Code § 45-8-213 (includes exception for recording public officials on duty); Nevada Revised Statutes § 200.650 (all-party consent required for telephonic recording; only one-party consent required for in-person conversations); New Hampshire Revised Statutes § 570-A:2; Pennsylvania Consolidated Statutes, Title 18 §§ 5702, 5704(4); Revised Code of Washington § 9.73.030).

These state laws vary in their scope, but have been used frequently in recent years to arrest, detain, and harass photographers, including civilians and members of the credentialed press. Officers may at times invoke these statutes to stop civilians from recording encounters with police officers to restrict subsequent disclosure of information that might subject an officer to possible censure. Appeals to privacy in public encounters under current law are unlikely to result in success, and because some of the statutes cover activity in public as well as private spaces (see e.g. 720 Illinois Compiled Statutes § 5/14-2), their reach is much broader than needed to protect against invasions of privacy. Some of these laws may have made recordings of conversations between civilians and police officers, like those described above, illegal (at least as far as conversations or speech were part of the recordings). In the United Kingdom, an anti-terrorism law similarly used by police officers to detain and question photographers has recently been held to be in violation of the European Convention for Human Rights and Fundamental Freedoms (Gillan and Quinton v. The United Kingdom, 2010).

6.4.1. Federal and state court law in cases outside Washington

In a landmark case in 2011, the First Circuit held that the First Amendment clearly gave citizens the right to record police officers and other public officials while they were performing their official duties in public spaces as long as the citizens did not interfere with the police officer's legitimate work and made the recordings overtly (not secretly) (Glik v. Cunniffe, 2011). In that case, Glik v. Cunniffe (2011), a Boston attorney named Simon Glik was walking through the Boston Common when he saw officers using what he thought was unnecessary force to affect an arrest (Glik v. Cunniffe, 2011, pp. 79-80). As a consequence, Glik pulled out his smartphone and made a video recording of the incident (Glik v. Cunniffe, 2011, p. 80). When one of the officers approached him, asking whether he was taking photographs, Glik indicated that he was actually recording video and audio of the events (Glik v. Cunniffe, 2011, p. 80). Subsequently, the officers arrested Glik and charged him with a number of crimes, including violation of the Massachusetts state wiretapping statute (Glik v. Cunniffe, 2011, p. 80). After the public prosecutor dropped the charges against him, Glik filed a civil rights lawsuit against the city, officers, and the police department (Glik v. Cunniffe, 2011, p. 80). The court found that the right of individuals to film public officials in public spaces was a "fundamental and virtually self-evident" right under the First Amendment (Glik v. Cunniffe, 2011, p. 85). According to the court,

> ...though not unqualified, a citizen's right to film government officials, including law enforcement officers, in the discharge of their duties in a public space is a basic, vital, and well established liberty safeguarded by the First Amendment (Glik v. Cunniffe, 2011, p. 85).

After the Glik decision, the City of Boston paid Simon Glik a $170,000 settlement to close his case (ACLUM, 2012).

A year after *Glik*, the Seventh Circuit enjoined the Cook County State's Attorney from using the Illinois wiretapping law to arrest members of the ACLU from recording police officers as part of a police accountability program (ACLU of Illinois v. Alvarez, 2012, p. 583). The Illinois statute prohibits audio recordings even where officers do not maintain any expectation of privacy in their conversations, and carries steep criminal penalties as a class 1 felony—equivalent to sexual offenses such as rape (Illinois Compiled Statutes § 5/14-2). In that case, ACLU of Illinois v. Alvarez (2012), the court held that the statute, as written and applied to the facts of the case, "likely violates the First Amendment's free-speech and free-press guarantees" and remanded the case to the district court (pp. 586-587).

In another case, the City of Baltimore agreed to a $250,000 settlement[36] with a man named Christopher Sharp after the police seized and deleted the video from his phone before giving it back to him after he filmed officers arresting one of his friends (Broadwater, 2014). Prior to the

[36] The settlement is available at http://www.aclu-md.org/uploaded_files/0000/0486/sharp_v._bpd_final_signed_agreement.pdf.

settlement in that case, the U.S. Department of Justice (DOJ) had filed a Statement of Interest with the trial court, in which the DOJ stated that,

> [t]he right to record police officers while performing duties in a public place, as well as the right to be protected from the warrantless seizure and destruction of those recordings, are not only required by the Constitution. They are consistent with our fundamental notions of liberty, promote the accountability of our governmental officers, and instill public confidence in the police officers who serve us daily (Sharp v. Baltimore City Police et al., 2012).

The DOJ also wrote a letter to the Baltimore Police Department in advance of a settlement conference in which it reiterated its position in favor of the First Amendment right to record police conduct (Smith, 2012) and the Baltimore Police Department instituted a formal policy recognizing the First Amendment right of citizens to:

> record, photograph, and/or audio record [Baltimore Police Department] Members while [Baltimore Police Department] Members are conducting official business or while acting in an official capacity in any public space, unless such recordings interfere with police activity (Baltimore Police Department, "Policy"; see also Broadwater, 2014).

A few other court decisions in other parts of the country also protect the public's right to record officers in public (see e.g. Gericke v. Begin, 2014; ACLU of Illinois v. Alvarez, 2012; Glik v. Cunniffe, 2011; Smith v. City of Cumming, 2000, p. 1333; Fordyce v. City of Seattle, 1995, pp. 438-439; State v. Flora, 1995; see also Kramer, 2011, pp. 367, 369; Bowens v. Superintendent of Miami South Beach Police Dept., 2014, p. 863), but reports of officers arresting photographers on eavesdropping charges continue to proliferate around the country (see Gurnon, 2013; Kopan, 2013; ACLU-PA, 2013; 2012)—in some cases, even in jurisdictions where police department orders have expressly stated that officers should not arrest civilians for recording (Fenton, 2013). And in one case, a civilian recorded a conversation with an official while making a public records request and when the civilian brought the recording to the department's attention, claiming the recording showed that his request was inappropriately handled, the police department arrested him for violating the eavesdropping law (Kohn, 2010). Civilians have also frequently been arrested for filming their encounters with police during traffic stops or while witnessing arrests in a variety of situations (see CBS News, 2009).

Prior to the Glik and Alvarez decisions, a number of courts had previously come to similar conclusions. For example, In Smith v. City of Cumming (2000), the plaintiffs filed suit against the city and police chief in Cumming, Georgia, claiming that, "Smith had been prevented from videotaping police actions in violation of Smith's First Amendment rights" (p. 1332). The 11th Circuit affirmed the lower court's holding that the First Amendment protects the right to "photograph or videotape police conduct," but that this right was "subject to reasonable time, manner and place restrictions" (Smith v. City of Cumming, 2000, p. 1333). The court found it persuasive that a number of other decisions around the country had previously upheld First Amendment rights to film public meetings (see Blackston v. Alabama, 1994, p. 120; Iacobucci v.

Boulter, 1997; Thompson v. City of Clio, 1991, pp. 1070-1071), to film matters of public interest (Fordyce v. City of Seattle, 1995, p. 439), as well as decisions holding that the press generally should not have any greater right to document or access information than members of the general public (United States v. Hastings, 1983, p. 1281; Lambert v. Polk County, 1989, p. 133).

However, some courts have also come to contrary conclusions about whether the right to film officers while they are on duty is a clearly established First Amendment right, finding officers entitled to qualified immunity for arresting or detaining civilians for recording or confiscating cameras. Within the Third Circuit, a few cases stand out. First, in Kelly v. Borough of Carlisle (2010), the Third Circuit held that "even insofar as it is clearly established, the right to record matters of public concern is not absolute; it is subject to reasonable time, place, and manner restrictions" and that, on the facts in that case, there was,

> insufficient case law establishing a right to videotape police officers during a traffic stop to put a reasonably competent officer on "fair notice" that seizing a camera or arresting an individual for videotaping police during the stop would violate the First Amendment (p. 262).

The *Kelly* court put significant weight on the fact that "traffic stops especially fraught with danger to police officers" (Kelly v. Borough of Carlisle, 2010, pp. 262-263, citing Arizona v. Johnson, 2009).[37] This allowed the *Kelly* court to distinguish its case from that in the Eleventh Circuit decision in Smith v. City of Cumming (2000) and a prior district court decision in the Third Circuit (Robinson v. Fetterman, 2005). In Robinson, the district court had held that the plaintiff had a First Amendment right to film state troopers when his filming did not interfere with the officers' truck inspections on a public roadway and when he filmed from private property and at least 20 feet away from the officers at all times (p. 541). The Third Circuit had also previously upheld a ban on recording public meetings (Whiteland Woods, L.P. v. Township of West Whiteland, 1999). More recently, in Fleck v. Trustees of University of Pennsylvania (2014), a district court in Pennsylvania held that an officer was entitled to qualified immunity when she seized a preacher's camera after he refused to move the camera away from her face[38] as she questioned him as he was "impeding the flow of congregants into [a] mosque" while preaching loudly about how Islam was a "destructive religion" (Fleck v. Trustees of University of Pennsylvania, 2014, pp. 397-398). The court held that the officer's actions were justified because the plaintiff had "ignored repeated police requests to move from the mosque doorway" and because the court found that "there was then no clearly-established First Amendment right in our Circuit to film police activity where, as here, the plaintiffs actively impeded efforts to restore public order" (Fleck v. Trustees of University of Pennsylvania, 2014, p. 408). However, the court did state, in a footnote, that subsequently issued Philadelphia Police Department guidelines affirming the right to record might have made that issue

---

[37] But see Lichtenberg and Smith (2001), finding evidence that "police homicides and assaults were found to be very infrequent occurrences during traffic encounters" (p. 419), casting "doubt… on the United States Supreme Court's reliance on an assumption of danger during the routine police–citizen traffic encounter" (p. 426).

[38] The bystander's action in this case is fairly aggressive, more so than in many of the other examples given here.

"ripe for reconsideration in [the Third] Circuit" (Fleck v. Trustees of University of Pennsylvania, 2014, p. 407 fn. 13).

In other jurisdictions, courts have also limited the rights of civilians to record in various settings; for example, finding no First Amendment right to record courtroom proceedings (McKay v. Federspell, 2014) or security officials in airports (Mocek, 2014, pp. 1074-1076; Mocek v. City of Albuquerque, 2013, pp. 38-40). Courts have also found officers immune from prosecution in a variety of situations; for example where it was not "clearly established" under prior case law that filming officers during a "tense active arrest situation with crowd control concerns would not be viewed as subject to some reasonable restrictions" (King v. City of Indianapolis, 2013, p. 1092).

6.4.2. Washington state law and civilian video

In Washington State, RCW 9.73.030 makes it unlawful for any individual to record any *private conversation* "without first obtaining the consent of all the participants in the communication" (RCW § 9.73.030(1)(a)), as discussed in some detail in section 4.3.2 of Chapter 4, *supra*. This analysis requires us to define what the law means by the terms "private conversation," what it requires in terms of "consent," and to determine whether any other relevant exceptions exist. Additionally, the Supreme Court of Washington has held that the Privacy Act only applies to interception, and RCW 9.73.030 does not provide a remedy for violation of privacy based on *divulging* the contents of personal communications (Kearney v. Kearney, 1999, pp. 411-412) (which, presumably, might protected by other sources of law—e.g. the common law privacy torts—in certain circumstances).

6.4.2.1. Private conversation

Washington courts have looked to a variety of factors to determine whether a recorded conversation was private or not for purposes of the eavesdropping law, with three primary inquiries: location (e.g. on a public roadway versus inside a private residence), whether or not third parties are present, and the nature of the conversation itself (e.g. between a civilian and police officer or between private parties). In State v. Flora (1992), the Washington Court of Appeals held that an arrestee's covert recording of a conversation between the arrestee and "public officers performing an official function on a public thoroughfare in the presence of a third party and within the sight and hearing of passersby" was not restricted by the statute because, in such a situation, the police officers could not "enjoy a privacy interest which they may assert under the statute" (p. 806). In that case, Flora had covertly recorded his encounter with and arrest by police officers using a tape recorder hidden inside a pile of papers (State v. Flora, 1992, pp. 804-805). The court concluded, in line with prior state court decisions, that "private" under RCW 9.73.030 means:

> secret... intended only for the persons involved (a conversation) ... holding a confidential relationship to something... a secret message: a private communication... secretly; not open or in public (State v. Flora, 1992, p. 806, citing State v. Slemmer , 1987, p. 52; State v. Forrester, 1978, p. 861; and State v. Bonilla, 1979, p. 872).

In conclusion, the *Flora* court held that,

> Because the exchange was not private, its recording could not violate RCW 9.73.030 which applies to private conversations only. We decline the State's invitation to transform the privacy act into a sword available for use against individuals by public officers acting in their official capacity (State v. Flora, 1992, p. 808).

In a series of later cases, Washington courts and federal courts deciding cases arising under Washington law have repeatedly maintained this interpretation of the Privacy Act (see e.g. State v. Roden, 2014, pp. 899-900; Johnson v. Hawe, 2004).

Washington courts have held that "[d]etermining whether a particular conversation is private is a question of fact," but that "where the pertinent facts are undisputed and reasonable minds could not differ on the subject, the issue of whether a particular conversation is private may be determined as a matter of law" (State v. D.J.W., 1994, p. 140; Kadoranian v. Bellingham Police Department, 1992, p. 190; State v. Flora, 1992, p. 806; Johnson v. Hawe, 2004, p. 683). The Supreme Court of Washington has recently elaborated on the appropriate test for determining a private conversation:

> In determining whether a communication is private, we consider the subjective intention of the parties and may also consider other factors that bear on the reasonableness of the participants' expectations, such as the duration and subject matter of the communication, the location of the communication, and the presence of potential third parties. We will generally presume that conversations between two parties are intended to be private (State v. Roden, 2014, p. 900 (internal citations omitted); see also State v. Kipp, 2014, p. 729).

However, conversations held in public spaces (and especially if held in front of third parties) will generally not be considered private (Fordyce v. City of Seattle, 1995; State v. Clark, 1996).

Subsequently to the *Flora* case, a number of additional decisions have affirmed the general holding in that case. For example, in Alford v. Haner (2003), the Ninth Circuit held that it was clearly established in Washington law, based on the decision in *Flora*, that "[t]ape recording officers conducting a traffic stop is not a crime in Washington" (p. 976). Alford had originally been pulled over for possibly impersonating a police officer (he was driving with headlights that flashed alternatively and had assisted motorists with a flat tire), but was arrested for recording his traffic stop (Alford v. Haner, 2003, p. 974-975). Because the right to record the traffic stop was clearly established, the court held that the subsequent arrest on the eavesdropping charge was objectively unreasonable and that officers could not benefit from qualified immunity based on a subjective mistake of law (Alford v. Haner, 2003, pp. 978-979).

Likewise in Johnson v. Hawe (2004), the Ninth Circuit held that police radio communications audible outside an officer's vehicle were not private because the officer had "'knowingly expose[d]' them to the public" by virtue of having been listening to his radio with his vehicle

windows down near a public skate park (Johnson v. Hawe, 2004, p. 683-684). The court stated that,

> With his window rolled down in a public parking lot, Chief Nelson's police radio communications were 'within the ... hearing of passersby' such as Johnson and other members of the public, and thus could not be private under the Act (Johnson v. Hawe, 2004, p. 684).

The *Johnson* court also cited an Attorney General Opinion from 1988 (Eikenberry and Day, 1988) that extended the definition of public (or not-private) to conversations that are of a purely business nature:

> … even where a conversation is not 'public' in that it is not monitored or heard by the public, it may be 'public' in that the subject of the conversation is strictly of a public business nature. We assume that virtually all conversations between 911 Central Dispatch and public officers are official, public business conversations (Eikenberry and Day, 1988, pp. *2-3).

Similarly, a recent Opinion by Washington Attorney General Ferguson (2014) argues that all conversations between on-duty police officers and members of the public are 'public' conversations, not subject to limitation by RCW 9.73.030 (pp. *1-2).

6.4.2.2. Consent

Under the state Privacy Act's eavesdropping provisions in RCW 9.73.030, consent may be either explicit (State v. D.J.W., 1994, p. 138 ("there is no… expectation of privacy in a conversation where, as here, one party consents to the recording of the conversation")) or implied. In terms of implied consent, "[a] party to a conversation is deemed to have consented to having his or her communication recorded when the person knows that the recording is taking place" (State v. Modica, 2006, p. 449; see also State v. Townsend, 2006, p. 675; In re Marriage of Farr, 1997, p. 184). The relevant provision of the Privacy Act states:

> Where consent by all parties is needed pursuant to this chapter, consent shall be considered obtained whenever one party has announced to all other parties engaged in the communication or conversation, in any reasonably effective manner, that such communication or conversation is about to be recorded or transmitted: PROVIDED, That if the conversation is to be recorded that said announcement shall also be recorded (RCW § 9.73.030(3)).

Courts have upheld this sort of implied-consent-by-virtue-of-knowledge conclusion in cases where a party has intercepted telephone conversations (State v. Modica, 2006; State v. Pejsa, 1994), emails (State v. Townsend, 2006), and voicemail messages (In re Marriage of Farr, 1997) where the complaining party had reason to know the communications were being intercepted.

Additionally, employees of a "regularly published newspaper, magazine, wire service, radio station, or television station" engaged in "bona fide news gathering" (RCW § 9.73.030(4)) must meet a low threshold for consent purposes; specifically, journalist exception requires only that, if

consent is not explicitly given, that "the recording or transmitting device" used by the journalist "is readily apparent or obvious to the speakers" (RCW § 9.73.030(4)).

6.4.2.3. Other exceptions

The provisions of RCW 9.73.030 prohibiting interception of private communications have been held to not apply to conversations between police officers and individuals pulled over on suspicion of driving while under the influence of alcohol (and in all other traffic stops, for that matter) (see Lewis v. State Dept. of Licensing, 2006, pp. 465-466). However, despite this lack of any expectation of privacy, RCW 9.73.090(1)(c) does require police officers to issue verbal notification of audio recording when the recording is tied to the use of a dashboard-mounted camera in a patrol vehicle (Lewis v. State Dept. of Licensing, 2006, pp. 464-466).

In other cases, recordings have been held admissible when the conversations at issue contain requests to commit murder (State v. Caliguri, 1983), "conveyed threats of extortion, blackmail, bodily harm," or other unlawful requests or demands (State v. Williams, 1980; RCW § 9.73.030(2)(b)). In these cases, only the consent of one party is required. Single-party consent is also required to record emergency calls to police and fire stations (State v. Bonilla, 1979; RCW § 9.73.030(2)(a)), "which occur anonymously or repeatedly or at an extremely inconvenient hour" (RCW § 9.73.030)(2)(c), and communications related to hostage takers or barricaded persons (State v. Pejsa, 1994; RCW § 9.73.030(2)(d)).

6.5. Value Sensitive Design

In contrast to the other two cases presented in this dissertation, civilian video does not directly involve public access to government records. However, the right to record on-duty police officers while they carry out their work still hinges on the right of citizens to document government conduct (and, likewise, enables a form of antipower and the ability to check state action). The publication of civilian recordings to the internet or through other media channels, just like the publication of police ALPR or BWC records, still functions as a form of secondary visibility of police officers and of civilians alike. The public disclosure of these videos (or audio recordings) offers the potential for similar privacy harms. However, in this case, the primary subjects of the original recordings are the police, rather than civilians. In the following paragraphs, I discuss how I bound direct and indirect stakeholder groups, and then develop three value scenarios to help surface the relevant tensions raised by the recording and making public of civilian video recordings. As in the previous chapter, I focus on elaborating narratives with relevance to the "five key elements" that ought to be addressed in the application of value scenarios under the VSD framework to "develop provocative sketches of the future: stakeholders, pervasiveness, time, systemic effects, and value implications" (Nathan, Klasnja, and Friedman, 2007, p. 2587). None of these scenarios directly deal with the benefits of civilians creating records of police misconduct (the primary purpose of civilian video as I have defined it in this Chapter), but rather with other, perhaps less obvious, implications.

In the subsections that follow, I conduct a stakeholder analysis, outline a fictional, yet possible future, and then present three value scenarios based on that hypothetical future.

6.5.1. Direct and indirect stakeholders

In regards to civilian video, there are potentially a vast number of stakeholders who directly interact with the technologies in question, as these include essentially any number of now ubiquitous audio-visual recording device such as cell phones, digital cameras, tablets, and other computing devices. As in prior VSD research (Miller, et al., 2007, pp. 283-284), I identify direct stakeholders by the role they play in connection to the system under examination—in this case, by interactions including 1) recording police action, 2) using video as evidence of alleged police misconduct, and 3) posting civilian video of police officer conduct to the internet. For purposes of this project, I define *direct stakeholders* as those individuals who actually engage in the recording (role 1), submitting for use in evidence (role 2), and/or uploading and posting (role 3) civilian video footage of police officer conduct to publicly accessible websites, such as YouTube, Facebook, blogs, or police accountability-related websites (e.g. CopWatch or ACLU). In many cases, single individuals will take on both of these roles, but it is conceivable that they might be separate in some cases, for example when groups—such as CopWatch organizations or ACLU police accountability teams—engage in coordinated efforts to record and then publicize their recordings at an organizational level. *Indirect stakeholders* (those who do not directly interact with, but who are affected by the output), on the other hand, may also include a vast number of individuals or other entities, including police officers, bystanders and anyone else caught on tape, companies whose property is captured on video, and internet service providers who host, index, or link to the associated user-generated content and who may have to react to requests for removal (e.g. on the basis of privacy violations) or de-linking under European laws such as the right to be forgotten or the right to erasure (see European Commission, 2014; Tsesis, 2014; Google Spain SL v. Agencia Espanola de Proteccion de Datos, 2013). In this project, I am limiting my discussion of indirect stakeholders to those individual persons (police or civilian actors or bystanders) who are identifiably captured on civilian video and, as a consequence of that identifiability, whose privacy rights may be implicated by subsequent disclosure of the footage.

6.5.2. Value Scenarios: Overview of a possible future

More now than ever, mobile recording devices have become a ubiquitous aspect of modern life. These devices have become increasingly wearable, networked, and integrated into daily activities. Long past are the days when stationary CCTV cameras were relied on as the primary visual evidence available for law enforcement information gathering after a crime had occurred. Now, geo-tagged and time-stamped civilian video has proliferated on the web—and is searchable by a variety of biometric indicators, including face, gait, and voice recognition, at the push of a button—and law enforcement have the ability, almost in real time due to new automated subpoena processes, to automatically source media files from all wireless devices that recorded audio, images, or video within geographic "bubbles" of space at or around the time a crime or accident occurs. The ubiquity and interconnectedness of these mobile surveillance devices has made

possible the world imagined by James Stacey Taylor (2005) when he argued that "the State should place all of its citizens under surveillance at all times and in all places, including their offices, classrooms, shops—and even their bedrooms" (p. 227), although many of the devices in this mesh are those owned and used by ordinary civilians and not the state itself. On the other hand, this same pervasive mesh of surveillance has also enabled hyper-vigilant civilian oversight of police misconduct. As a result, police violence and use of force have disappeared almost completely within the past decade as virtually all incidents of misconduct have been thoroughly documented and prosecuted.

6.5.3. Value Scenario 1: Civilian video and crowd-sourced evidence

Scenario. On his way home from work one evening in July, Robert crosses a lightly populated park a few blocks away from his bus stop. The park contains a number of students playing Frisbee and taking photographs as well as a few families with small children feeding ducks by a pond. As he walks down the gravel path around the pond, two men approach him and ask for money. Robert tells them he doesn't have any, and attempts to walk around the men. However, they block his exit and one of them pulls out a knife. Scared for his life, Robert gives the men his wallet and they quickly run down the path and out of sight. Robert calls 911 on his phone and is told an officer is nearby. While Robert tells the dispatcher what had happened, the police submit an automated request to all the major cellular service providers to access photographs and video captured by phones within a quarter-mile radius of the mugging. Within minutes the patrol officer at the park contacts Robert and shows him the media collected from nearby devices. Robert identifies the men from a video taken by the father of one of the nearby children at the pond, and the officer quickly takes off in pursuit while sending the video of the assailants back to the department so it can be used to match against a wider net of images and video captured by devices in the direction the two men had fled. Forty minutes later, as Robert steps off his bus two blocks from his house, the police officer call him and tells him they have retrieved his wallet.

Discussion. This scenario, in some respects, is similar to the investigatory techniques employed by investigators after the Boston Marathon bombing (Stroud, 2013; Madrigal, 2013) and the 2011 Stanley Cup riots (Vancouver Police Department, 2011; 2013). In each of these cases, police sourced large amounts of video and photographs from nearby CCTV cameras, civilians' cellphones, and nearby cell towers. However, the twist in the scenario above rests in the idea that the process of law enforcement sourcing media from privately owned devices can be automated, regardless of whether the individuals consent to having their devices accessed. This scenario raises a number of important issues outside the scope of this project, but it also implicates domination. Allowing the state to access private devices and pull information and files remotely from these devices for investigatory purposes could obviously lead to abuse and, in any respect, could also give the state the power to intrude into the private lives of its citizens. This sort of process would potentially violate both the *access* and *use* provisions of the definition of the right to privacy I employ in this project, suggesting that such activity would not be warranted. Additionally, even if

we disregard that conclusion, without significant safeguards this scenario could grant the state dominating power.

On the other hand, this scenario can easily be modified to demonstrate the power of civilian video to document and hold police officers visible (and sometimes accountable (see e.g. Goodman and Baker, 2014)) like in the cases mentioned earlier in this Chapter involving the pepper spray incident during the Occupy Protests on the UC Davis campus in 2011 (see Federated Univ. Police Officers Ass'n v. Superior Court, 2013; Chander and Sunder, 2012, p. 1605; Lautt, 2012, pp. 376-377), the shooting of Oscar Grant on a San Francisco subway platform (Antony and Thomas, 2010, pp. 1280-1281), and the death of Ian Tomlinson during the London Riots in 2011 (Greer and McLaughlin, 2010, p. 1049). Indeed, existing smartphone apps designed to record police-civilian encounters and automatically upload forensically intact recordings to local chapters of the ACLU already provide a glimpse of the potential power of civilian video in such cases. These videos could be readily flagged and sourced during protests, for example, and civil liberties organizations could proactively publish evidence of police officer conduct during these events, even as the events are still unfolding.

6.5.4. Value Scenario 2: Civilian video and discrimination

Scenario. Jackie has been down on her luck for a number of years. As a decade-long member of the local homeless population, she has long relied on the charity of strangers and the safety, warmth, and dryness of public spaces like the local library. However, a few months ago, while staying dry inside the library during a string of cold and rainy days, she noticed that a number of library patrons would frequently record her loitering in the library lobby or trying to sleep in a soft chair in a reading nook. These patrons complained to the library staff and shared their footage with the library security force (off-duty officers on loan from the local police department), who asked her to leave if she was only going to use the facilities for loitering or sleeping. The next day, Jackie was woken abruptly as she was sleeping near the front entrance to the library and contested the security officer's request that she leave the premises. When Jackie started to leave (albeit somewhat slowly), the officer restrained her forcefully, knocking her to the sidewalk and injuring her face and shoulder. The incident was captured on bystander video and at least one clip was later uploaded to YouTube.

A couple of weeks later while Jackie was again waiting in the library for the rain to stop, she was trespassed by the library staff and her biometric information was added to the library database for unwanted persons. Now, whenever she tries to enter the front doors, the surveillance system, comprising stationary cameras, body-cameras on library security staff, and the smartphone cameras of other patrons connected to the library WiFi, automatically detects her presence, identifies her, and sends a warning to the security guards posted just inside the door. On some occasions, she hasn't even made it to the front doors, as patrons taking photographs on the sidewalk outside the library have detected her presence and have sent signals to other nearby devices, as well as the library staff, even before she entered the view of the library CCTV cameras. As a consequence, Jackie has not been able to enter the library for weeks and has found it particularly

difficult to find a safe and dry place to spend her time. However, after she eventually finds the video of the incident online, she is able to file a complaint against the officer and demonstrate that she was, in fact, not refusing to follow the officer's instructions. Armed with this evidence, Jackie is able to regain her right to enter the library and the officer is ultimately reprimanded.

Discussion. As also demonstrated in the modified version of the previous case, as well as in the numerous legal decisions discussed above, the fact that a bystander filmed the incident and posted it online makes it possible for the un-empowered citizen to ensure that their side of a story can also be told. Publication or dissemination of the video is ultimately an essential element to making civilian video useful for oversight in these cases. This scenario also exemplifies the concept of surveillance as "social sorting" (Lyon, 2003) and is supported by evidence that surveillance of public spaces has produced discriminatory effects on marginalized groups (see Sætnan, Lomell, and Wiecek, 2004). As civilian video adds itself to the milieu of surveillance, its impact on individual visibility may be changed dramatically when biometric identification (e.g. face recognition) technology becomes more accurate and accessible—to the general population and as a standard feature in all of the most popular social media sites. Stakeholders engaged in uploading footage to the cloud may do so for a variety of reasons, from the benign to the malignant, but the result may be that subjects and bystanders are more easily subject to observation and identification.

6.6. Other questions raised by overbroad restrictions on civilian video

In 2009, during protests following the G20 in London, England, a short video filmed by a bystander found its way into the popular press and online media by way of the Guardian newspaper (Lewis, 2009). The video depicted an officer purposefully knocking Ian Tomlinson, who was not directly involved in the protests, to the ground with his baton without any apparent provocation. Tomlinson died at the scene shortly thereafter. This example of citizen journalism (in concert with promotion by the established press) dramatically changed the way the mass media reported the riots and policing tactics employed by the local police (Greer and McLaughlin, 2010, p. 1049), and it has now been viewed over a million times on the popular video-sharing website, YouTube.com (The Guardian, 2009). The release of the video also resulted in a number of official investigations of the incident and the eventual firing of the officer for gross misconduct, although he was acquitted of manslaughter (Walker, 2012). In the cases of *Glik*, the Oscar Grant shooting, and the choking death of Eric Garner, discussed previously, civilians made the recordings while walking through the area or standing nearby. Out of concern for what they observed, these individuals began to film the arrests with their smartphones from a safe distance. And, in Simon Glik's case, this also led to his arrest for filming the incident in violation of the Massachusetts state wiretap statute (Glik v. Cunniffe, 2011). Indeed, civilians recording video or taking photographs may also implicate a variety of additional legal considerations, such as property-based restrictions on image capture (when they are in private or quasi-private spaces), and the subsequent publication or dissemination of their recordings may also raise intellectual property or national security concerns (Newell, 2011).

Imagine the position of the civilian wielding a camera in either of these cases. A number of "obvious" questions (see Nussbaum, 2000) appear in sequence. First, suppose the camera is not already recording when the civilian sees what she feels is abuse or unlawful use of force by a police officer (the case in the *Glik* example). Within a jurisdiction that requires all-party consent before recording, pulling out the camera and pressing record (without gaining the officer's consent) might very well violate state eavesdropping law. However, failing to act might allow the abusive conduct to go unverified and potentially unnoticed by those in a position to remedy wrongs or provide justice to the abused. A number of legal and ethical conflicts also further complicate this situation, such as the conflict between the potential First Amendment right to record and the state law prohibition, the privacy rights of the various subjects of the recordings (including innocent bystanders), the property rights of the camera owners, and the context of a public space.

Alternatively, let us imagine that the camera was recording prior to the noticed abuse (or alleged abuse) by the officer, and the initial officer conduct was unintentionally captured (such as in the Tomlinson case). The camera-wielding civilian must now decide whether to continue recording (in potential violation of state law), move the camera so as to avoid capturing any more of the incident, or turn the camera off (with similar consequences as noted above in the first example). Admittedly, it is not clear that violating the law in this example is immoral (unlike unjustified homicide, for example) or that the decision does in fact have moral import. However, the potentially adverse consequences to the civilian—arrest and punishment—would be substantial. Additionally, if we entertain Nussbaum's (2000) approach to moral reasoning, the law's denial of the citizen's First Amendment rights would create a tragic situation, making the government's role in restricting the citizen's basic entitlements morally significant.

In either of these two cases, if the recording captures any of the alleged abuse, the civilian must also decide what to do with the footage. She could turn it over to the police department to use for internal investigation (although, in real-life, this option has actually resulted in the civilian being charged with a crime and the footage used as the evidence of the unlawful recording at issue for prosecution of the eavesdropping offense) (Kohn, 2010), keep the footage to herself, or she could destroy the footage. Alternatively, she could also post the video to the Internet, although the reality here is that any expectation of anonymity would unlikely be justified, and this option could very well subject her to the same risk of prosecution as turning the footage over to the department. Destruction in this case could be considered unlawful destruction of evidence and obstruction of justice, should the abuse be prosecuted by local authorities, and keeping the evidence hidden could mean, again, that the offense would go unpunished at the expense of justice.

It seems evident that these scenarios suggest that the "obvious" question does not always have an obvious answer, regardless of whether the situation is necessarily "tragic"—that is, that none of the available actions would actually be morally blameless. However, as Nussbaum (2000, p. 1009) notes, the obvious question must be addressed. It cannot be escaped, since inaction itself is an answer. Additionally, it is important to also determine the answer to the tragic question, since doing so allows us, as a society, to work toward addressing and fixing the situation our laws and

policies have created. The possibility does exist, however, that each of the various ethical traditions (consequentialist, deontological, Aristotelian) would lead us to the same conclusion about which available action would be most appropriate—and presumably also morally blameless (aside from whether the action ought or ought not to be done). Presumably, the documentation of the abuse of government power—even in violation of state law—could be seen as morally permissible under both consequentialist and deontological accounts of normative ethical theory. If we accept Nussbaum's claim that certain costs—based on violations of basic human entitlements as set forth in our Constitution—are distinctively bad such that "no citizen should have to bear them" (Nussbaum, 2000, p. 1036), then we can begin to see how policy choices that restrict civilian video through the application of law have created situations fraught with tensions among transparency, privacy, and accountability, and that such policies therefore have some moral import because they involve the violation of basic rights and entitlements.

Secondly, if we set up our legal frameworks to restrict the rights of citizens to engage in civilian video of police conduct, we force civilians to make moral choices between obedience to law and engaging in democratic oversight of state action. In the first situation described previously, the initial set of alternatives consists of choosing to begin recording or to refrain from documenting the incident. At first glance, choosing to record would not necessarily appear to involve morally blameworthy conduct, except that such action would potentially be in violation of state criminal law—something our intuitions might tell us is generally morally suspicious. To commit a crime, we might say, is morally blameworthy. But what of the (un)justness of the law itself, or our actual moral obligation to obey the law (whether perceived as just or unjust), or the potential that the state law is potentially in violation of a higher law, the U.S. Constitution and First Amendment of the Bill of Rights?

On the other hand, choosing not to record, as we have said, might allow the abusive conduct to go unverified and potentially unnoticed by those in a position to remedy wrongs or provide justice to the abused. Audio-visual and photographic materials are, after all, important and very powerful sources of evidence. Allowing an act of injustice to go unpunished (or at least failing to act to prevent such an outcome when one could have done differently), can also be seen as a violation of our moral obligations to the abused or society generally. Morally significant questions might also be raised should such a choice violate our own deeply held moral convictions, affecting our autonomy and integrity. We might also say that, as citizens, we have some obligation to prevent and report unlawful and abusive conduct on the part of our government, or to hold our government accountable for its wrongs and violation of its citizens' rights. In some cases, the situation is compounded by the additional question about what to do with footage already obtained (whether purposefully or unwittingly). The considerations are similar, however, and not necessarily any easier to answer. Obstruction of justice and destruction of evidence of serious wrongdoing can easily be seen, intuitively, as morally suspicious actions.

It is in some sense tragic that we (as a society) have designed some of our laws and policies in a way that subject civilians to situations where they must struggle with these questions in the first

place (regardless of their strictly moral import). The fact that portions of our society subject their citizens to having to struggle with these difficult questions on a regular basis (decisions that must also be made without time for reflection and deliberation), is itself a very undesirable reality. Considering whether, and when, violation of law might be morally justified and acceptable appears fraught with difficulty and competing considerations of significant import, despite the importance of that endeavor (which is generally outside the scope of this dissertation.[39] Additionally, when police surveillance—in the form of wearable cameras, etc.—is broadly allowed by the law, based on the idea that civilians have no reasonable expectation of privacy in public spaces, any legal restraints (e.g. eavesdropping statutes) on civilians looking back and conducting reciprocal surveillance in these same public spaces becomes very problematic as, potentially, a form of codified state domination that strikes at the core values of the First Amendment.

6.7. Conclusion

In conclusion, it is important to reiterate that the aim of this Chapter has not been to conclusively resolve the moral questions confronting citizen journalists in the field. Rather, the conflict between First Amendment ideals—as announced by the First Circuit in Glik v. Cunniffe (2011) and Seventh Circuit in ACLU v. Alvarez (2012)—and the enforcement of eavesdropping laws against civilians filming officers carrying out official duties in public spaces is untenable. When considered against state use of mobile, officer-mounted, video cameras, the need to limit the unbalanced possibility of domination made possible by increased state information collection and analysis is pronounced.

Generally, enforcing certain time, place, and manner restrictions on the right to record may be justified; in particular those that are narrowly targeted to ensure officer safety and that do not interfere with legitimate police work. Additionally, private-party restrictions on recording in private or semi-private spaces would obviously not implicate First Amendment concerns, and may be justified. However, the right to record should not hinge on whether recording is conducted overtly or covertly as long as the recordings are made in public places or where police and bystanders do not have substantial expectations of privacy.

In the end, persons (including police officers and bystanders) ought to enjoy certain rights to privacy in public spaces. The right to control how our personal information is accessed and used (for example, through aggregation from multiple sources into large databases) is vitally important if we are to care about personal privacy at all. Entering a public space may necessarily imply a waiver of certain types of information related to our presence in that space, but such a waiver need not encompass all future uses, analysis, and aggregation of such information over time (especially by government agents). This right to control ought also to place affirmative obligations on state action to preserve civilian obscurity by limiting visibility (qua aggregation, retention, and analysis), just as in the case of ALPR and the mosaic theory of the Fourth Amendment, when antipower would be increased through such action. However, in this particular case (civilian video), police privacy interests will generally have to give sway to transparency as the speech at

[39] See Newell, 2014a, for additional analysis or the moral questions raised by citizen video.

issue is directly connected to democratic governance and state accountability. In some sense, because of the public interest in ensuring political liberty and in conducting effective civilian oversight of state action—through exercising First Amendment rights to gather and access information—points to the conclusion that police officers and other public officials have, by virtue of their public roles, effectively waived certain of their rights to privacy while carrying out their official duties in public spaces. As such, the right to conduct reciprocal surveillance of state agents conducting their official duties in public spaces (a form of 'smartphone journalism') is an important aspect of reducing domination and preserving individual liberty.

7. Policing and body-worn cameras

7.1. Introduction

September 2014. I sit against the wall in an overcrowded police department training room as about two-dozen police officers pull small black cameras out of square white boxes. Most of them appear eager to see what's inside, and they begin to talk excitedly amongst themselves as they try to figure out how to attach the cameras to their uniforms. A representative from TASER,[40] whose logo is printed on each box, is explaining to the officers what to expect from their new body-worn cameras. As the trainer explains how to activate and deactivate the cameras, electronic beeps fill the room as a number of the officers initiate their first recordings. All of the officers, except two who have just been hired by the department and have been required to begin using a camera, have volunteered to wear the cameras as part of the initial pilot program. They have a variety of reasons for volunteering, but many claim they want to be able to document evidence and counter unfounded claims of misconduct. As they watch example videos of officers using TASER weapons to subdue uncooperative suspects, they express excitement about the video they see on the screen, and ask how they should mount their own cameras to get a similar perspective. As they try out various mounts, one officer turns to another and, as he struggles to get the camera situated on his uniform, says, "don't look at me like I'm a monkey, I'm just bad with technology." Another officer turns to his neighbor and says, "I guess I won't say anything stupid, I'm sure at least one person in the room is recording right now." The good humor in the room is evident as the officer's play with the cameras for another few minutes. Eventually, one officer asks jokingly, "Where's the direct-to-YouTube button?" The subsequent commentary makes it obvious that some of the officers feel that they should have the ability to post videos of citizens to YouTube, just as citizens have been doing for years. "If citizens can do it," another officer tells me after the training, "why can't we also benefit from the ability to record in public places?"

Less than two months later, all of the test videos created by the officers during this training meeting will be uploaded to YouTube along with many of the additional videos filmed by the officers in the succeeding weeks as they interact with civilians during their shifts. Just days after this initial training meeting, the department (and others across the state) received a blanket request, under the state public disclosure law, for all video footage generated by BWCs or dashboard cameras mounted in patrol vehicles (see Figure 8, below). Armed with legal advice that almost all of the footage must be disclosed without any form of redaction, the department struggles to process hundreds of hours of early footage, a process that is taking three times longer than the video itself. As it is being released, the disclosed footage is channeled directly to the YouTube channel[41] of the (then) anonymous requester. Within weeks, it becomes clear that the Washington State Public Records Act is functioning—in this case—as a legally sanctioned direct-to-YouTube alternative

[40] References herein to TASERs refer to the non-lethal electronic control device (weapon) manufactured by TASER International. TASER also sells a product line of body cameras, but these cameras will be referred to as BWCs.

[41] https://www.youtube.com/user/policevideorequests.

for police body camera footage, albeit pushed online by private actors and not the police officers themselves.

> This is a public records request for the police department.
>
> I'm requesting all dash and body camera videos not involved in pending litigation.
>
> I would like the requested videos to be uploaded to Youtube by the department at https://www.youtube.com/user/[redacted] or another channel. If the department doesn't want to upload them to its own Youtube account then I would like it to consider uploading it to Youtube via an account I create and maintain. If uninterested in doing that I would like it to consider uploading the videos to a website, FTP server or cloud storage system like Dropbox or Google Drive.
>
> I would like the videos uploaded in installments beginning with the oldest.

Figure 8. Text of a public records request received by a number of police departments in Washington State in September 2014. Videos disclosed to this requestor have been posted to an anonymous YouTube channel at https://www.youtube.com/user/policevideorequests.

After the initial disclosures hit YouTube, the commentary offered by officers at the outset of my subsequent ride-alongs changes dramatically. During my very earliest rides, officers were generally quite vocal about the benefits they expected to see from the cameras (e.g. they would capture evidence of criminal wrongdoing by civilians and have an increased ability to counter false claims of misconduct). In one case, captured on an officer's body camera, a man is caught on camera arguing with an officer prior to leading the officer on a lengthy foot chase. After the man originally pleaded not guilty for crimes captured on tape, the department provided his defense attorney a copy of the footage, resulting in a speedy change of plea. Some of the officers see these events as strong evidence that the cameras will capture important evidence and improve their work. However, after the blanket request for all footage becomes common knowledge, the dominant refrain I hear at the outset of rides over the next few months is the officers' dismay that all of their footage is likely bound to be visible to anyone on the internet. Their frustration is targeted at what they perceive as a significant violation of privacy; however, it is not always their own privacy they feel is violated, but the privacy of those whom they encounter during their shifts. One officer who recorded a lengthy interview with a young woman detained during a prostitution sting on his body camera, explained how he spent time after the video was posted to YouTube trying to figure out how, and whether, he could request the video be taken down for privacy reasons. He couldn't believe that such a sensitive interview could be disclosed and published without being redacted to protect the young woman's privacy. The interview, which remains on the internet, includes the woman stating her name, talking about her boyfriend and family, as well as the events and activities that led to her arrest for prostitution.

A couple of months later, while sitting around a table eating lunch with a group of five or six officers from another police department in a different part of the state, one of the officers has loaded a video that his camera recorded a few weeks earlier. He stands and places the laptop on

the table in front of me and says, emphatically, "Here, tell me this should be on YouTube." On the screen, I see the view from the officer's chest as he quickly exits his vehicle and runs across a lawn and through the open front door of a private home. As he enters the house, I hear multiple people screaming and a woman wailing loudly. Quite a few people are crowded into the small living room. Suddenly, I see the officer turn and take a small infant (who I later learn was two-months old) from the wailing woman. The infant's head and arms hang limply as the officer carefully transfers the baby's body to the floor and begins to attempt to resuscitate it, unsuccessfully. In the background, I see a couple of additional small children, held back by another adult, before I turn away from the screen in shock at what I've just seen.

A day or two later, I stand inside a couple's living room with two officers as the couple tries to explain why the wife had called 911 and accused the husband of threatening violence. The husband is drunk—and drinking more while he talks to an officer who is wielding a camera on his chest—and tells a rambling story about how much trouble his wife has caused him over the years. Perhaps he should leave her and move on. Perhaps he loves her. On the other hand, she's caused him nothing but grief and makes his life miserable. Accepting the officer's "if you think that's what needs to be done, then what are you going to do about it?" as an affirmation of his tentative plan to leave his wife, the man says, "now, don't try to force me into anything… I see what you are trying to do here." Moments later he says "maybe what I really should do is stop drinking," as he takes another sip from his can. Turning to me, he asks, "who are you?" He stares at me intently for a few moments. "He's with us," the officer says, "he's evaluating how we work while wearing these cameras." "Oh, that's good," the man replies. Even if he were sober, he probably wouldn't realize that this conversation was likely bound for YouTube and virtually unlimited visibility. If he did, would he or his wife (who was talking to a second officer in the far corner of the small living room) have let the police into their house in the first place? Would the wife have even called to report her husband's threats? These questions relate to interactional aspects of technology—meaning that the introduction of a technology into society can actually alter the existing social structure and change individual behavior and expectations over time. Although BWCs may have been initially perceived as a response to officer-involved violence and a need to capture evidence of officer misconduct—or deter such conduct in the first place—they may end up significantly impacting the nature of police-civilian interactions in ways not intended or even envisioned at the time the technology was deployed.

7.2. Prior research on body-worn cameras

Generally, the perceived benefits of body-worn cameras include increased transparency and accountability, improved citizen perceptions of police, more civil police-citizen interactions, evidentiary benefits in criminal prosecutions or for countering claims of misconduct, and improving police officer training (White, 2014, pp. 6-7). On the other hand, oft-cited potential problems include the invasion of citizen and/or police officer privacy, health and safety concerns due to wearing head-mounted cameras over long periods of time, and the need for significant investment in training, policy development, and technical infrastructure (White, 2014, pp. 7-9).

Earlier research investigating the effects of in-car cameras claimed substantial value to law enforcement, including enhancing officer safety, improving agency accountability, reducing agency liability, simplifying incident review, enhancing new recruit and in-service training (post-incident use of videos), improving community/media perceptions, strengthening police leadership, advancing prosecution/case resolution, enhancing officer performance and professionalism, increasing homeland security, and upgrading technology policies and procedures (IACP, 2005; see also IACP, 2004; 2003).

A growing number of studies have been conducted to examine various implications of police use of body-worn cameras, and studies are currently ongoing in multiple states, including Florida, Arizona, Nevada, New York, California, and Washington (as well as additional projects in the UK, Brazil (Willis, et al., 2013), South Africa (Bruce and Tait, 2015), and Kenya (Igarapé Institute, "Smart Policing"). Generally, these studies have been designed to test hypotheses through the application of quantitative methodologies, from randomized control trials to the administration of survey questionnaires. Qualitative approaches to these questions have, to this point, been rather rare, and if they have been employed, have been used only to supplement quantitative analyses. Corporate evaluation firms or police department personnel have managed many of these studies, but a few have also been designed and run by independent academic researchers (and others by think tanks, such as the Igarapé Institute in collaboration with Google Ideas). Despite the emergence of some new studies in recent years, at least one prominent researcher in this space has concluded that we still have "little evidence to support or refute many of the claims" of either the proponents or critics of body-camera adoption because there are still so many "outstanding questions regarding the impact and consequences of body-worn cameras" (White, 2014, p. 6).

In the United Kingdom, body-worn cameras have been utilized and studied for a number of years. In 2007, the Home Office's Police and Crime Standards Directorate published a report entitled, "Guidance for the Police Use of Body-Worn Video Devices" (Goodall, 2007) in which the directorate summarized internal research conducted during the Plymouth Basic Command Unit's (BCU) Head Camera Project. In their foreward to the report, Ministers McNulty and Scotland outline a glowingly positive vision for the future of body-worn video, focusing on the potential for the footage to provide evidence and to prevent crime. They claim that because "A picture paints a thousand words," the resulting video recordings of police-citizen interactions:

> will capture compelling evidence of the activities of suspects and will enable the raw emotion and action from the scene to be replayed in the courts in a manner that could never be captured in written statements. The courts can see and hear the incident through the eyes and ears of the officer at the scene, thereby gaining a real understanding of the actions of the accused and the challenges that face the Police Service today (McNulty and Scotland, 2007).

The BCU's initial testing began in 2005, with a single head-mounted camera used by a police Sergeant in the Devon and Cornwall Constabulary (Goodall, 2007, pp. 6, 30). In early 2006, another head-mounted camera was used as part of a domestic violence enforcement initiative that led to international media attention after footage was used as part of a successful prosecution in

March of that year (Goodall, 2007, p. 30). Another five cameras were deployed shortly thereafter (Goodall, 2007, p. 30). Initial findings from these early deployments included a significant increase the in the quality of evidence gathered at incidents (Goodall, 2007, p. 6). These early positive findings led to a number of additional body-camera pilots around the country, and the BCU began an extended trial in October of 2006 that included the use of 50 additional head-mounted cameras (Goodall, 2007, pp. 6, 30). Following a Home Office evaluation of the extended trial, the directorate found that body-worn video had provided more accurate evidence, served as a valuable training tool, saved time in a variety of situations (e.g. by reducing the need for elaborate written reports, increasing guilty pleas, and deterring complaints), provided important context surrounding the use of deadly or non-lethal force by officers, caused reluctant witnesses to testify in domestic violence cases and strengthened the ability of prosecutors to prosecute these cases, and decreased anti-social behavior by those subject to the recordings (Goodall, 2007, pp. 7-8, 32-33). Potential drawbacks reported were minimal, largely limited to the needed technical infrastructure (i.e. data storage capabilities) and related personnel requirements (Goodall, 2007, p. 8), or other technical problems (Goodall, p. 33).

In another report published in 2011, a consulting group evaluated body-worn camera programs by police in Aberdeen and Renfrewshire, Scotland (ODS Consulting, 2011). In Renfrewshire, the Strathclyde Police had begun using three head-mounted cameras in 2006, expanding to 38 in 2009 (ODS Consulting, 2011, p. 1). In Aberdeen, 18 cameras were initially deployed by the Grampian Police in 2010, quickly expanding to 39 (ODS Consulting, 2011, p. 5). The evaluation indicated a decrease in incidents of crime in the areas most saturated with cameras compared to the previous year and in comparison to the larger area as a whole, though these results cannot be considered a causal outcome of the body-worn camera pilot due to the non-experimental nature of the study (ODS Consulting, 2011, pp. 7-8). As in the earlier Home Officer study (Goodall, 2007), ODS Consulting also reported anecdotal evidence that the use of the cameras contributed to an increase in guilty pleas by defendants in criminal prosecutions (ODS Consulting, 2011, p. 9), as well as some evidence that the video was useful to counter complaints of misconduct (ODS Consulting, 2011, pp. 11-12).

In 2014, the College of Policing (UK) conducted a four-month randomized controlled trial (RCT) of body-camera adoption on domestic abuse outcomes in the criminal justice system in Essex, UK (Owens, Mann, and Mckenna, 2014). In the RCT, 70 officers wore cameras as part of the treatment group, and another 238 were assigned to the control (no camera) group (Owens, Mann, and Mckenna, 2014, p. 1). The researchers found some evidence that BWC use in domestic abuse incidents increased the number of criminal charges filed, but cautioned that officers reported not always turning on their cameras during these incidents as well as technical problems (Owens, Mann, and Mckenna, 2014, pp. 1-2, 14-18). In that study, officers also reported that having BWCs increased their confidence in their ability to get convictions, improved evidence gathering, and increased officer accountability (Owens, Mann, and Mckenna, 201, pp. 2, 5). Officers also reported that the existence of BWC footage of an initial domestic abuse incident made victims and

witnesses more confident and more likely to stay in the criminal justice process (Owens, Mann, and Mckenna, 2014, pp. 5, 17).

In another example, the Igarapé Institute's Smart Policing project has outfitted officers in Brazil, South Africa, and Kenya, with body-camera systems consisting of smartphones and open-source recording, streaming, and management software (Bruce and Tait, 2015, p. 12; see also Willis, et al., 2013; Igarapé Institute, "Smart Policing")—called "CopCast"[42]. The system allows for passive, on-device, recording as well as live streaming via WiFi or 3G/4G connections (Bruce and Tait, 2015, p. 28). In the South African context, an initial review of the CopCast pilot found that officers reported that "suspects tend to be more respectful and calm during routine traffic checks" when they realize officers are wearing a camera, and that officers also feel more confident and safer knowing that an incident will be recorded (Bruce and Tait, 2015, p. 17). Reportedly, officers were generally enthusiastic about the cameras, primarily for reasons related to obtaining cooperation from civilians and collecting evidence to support arrest and prosecution (Bruce and Tait, 2015, p. 24). Bruce and Tait (2015) also heard from officers that they have changed behavior to ensure encounters are recorded (see pp. 17-18). One officer stated mentioned that during traffic stops:

> I tell the motorist that my supervisor is watching the entire process via live video streaming. People seldom feel the need to negotiate when they know they are being watched (Bruce and Tait, 2015, p. 18).

Bruce and Tait (2015) also discuss privacy concerns raised by the use of BWCs and the potential for public access to BWC footage, finding good reasons to "protect members of the public against gratuitous embarrassment" (pp. 20-21). Officer privacy was also raised as a potential roadblock to successful adoption, especially when officers might have reasons to resist or subvert the requirement to wear a camera (Bruce and Tait, 2015, p. 30).

In the United States, both academic and commercial studies of body-camera adoption have been conducted over the past few years. In perhaps the most widely cited study to date within the U.S., researchers from Cambridge University partnered with the Police Chief at the Rialto (California) Police Department to conduct a randomized controlled trial (RCT) of that department's body-camera program, beginning in 2012 (Ariel, Farrar, and Sutherland, 2014; Ariel and Farrar, 2013). The most prominent findings from that study, namely significant decreases in officer use of force as well as the number of formal citizen complaints, were initially published in a report (Ariel and Farrar, 2013) on the Police Foundation's website in early 2013. Coming just months prior to the police-involved killing of Michael Brown in Ferguson, Missouri, and a federal district court judgment in New York requiring the NYPD to begin piloting cameras (Floyd v. City of New York, 959 F.Supp.2d 549 at 563; Floyd v. City of New York, 959 F.Supp.2d 668 at 685), these findings

[42] The open-source code for the CopCast project is available at https://github.com/igarape/copcast-android (Android client) and https://github.com/igarape/copcast-admin (administrative components). The CopCast project also involves collaboration from Google Ideas in New York City and a number of local partners in Brazil, South Africa, and Kenya.

have been cited routinely in media reports and by advocacy groups in support of requiring officers to wear body cameras.

In the Rialto Study, the researchers randomly assigned police shifts to either experimental (treatment) or control conditions, during which officers were required to wear (during the experimental shifts) or not wear body-cameras (Ariel, Farrar, and Sutherland, 2014). The experimental design involved all front-line patrol officers in the department (n = 54), and was primarily aimed at determining the effect of body-worn camera usage on use of force and citizen complaint numbers (Ariel, Farrar, and Sutherland, 2014). Interestingly, the researchers found that officers used force roughly half as often during shifts assigned to the treatment condition than they did on shifts when they were not wearing cameras (Ariel, Farrar, and Sutherland, 2014). There was also a significant reduction in overall uses of force across conditions, ranging from a 64.3%-58.3% decrease compared to the previous three years (25 instances during the 12 month study period, compared to 70, 65, and 67 in each of the preceding years, respectively) (Ariel, Farrar, and Sutherland, 2014).

In terms of citizen complaints, the reported between-groups treatment effect was not statistically significant, largely due to the low number of total complaints filed during the study period (n = 3; two during treatment, one during control conditions) (Ariel, Farrar, and Sutherland, 2014). However, the decrease in total complaints compared with the previous three years was significant, dropping between 88-94%, or from "0.7 complaints per 1,000 [total citizen] contacts to 0.07 per 1,000 contacts" (Ariel, Farrar, and Sutherland, 2014). Despite generally proposing that body-worn cameras present largely positive results, the researchers also caution that additional research is needed to determine whether the presence of a camera reduces the likelihood of victims reporting crimes, as well as questions about victims' rights (Ariel, Farrar, and Sutherland, 2014).

In a second study, completed between October 2012 and September 2013, The Mesa (Arizona) Police Department deployed 50 TASER Axon Flex (head-mounted) cameras, primarily to study "the system's impact on reducing civil liability, addressing departmental complaints and enhancing criminal prosecution" (White, 2014, p. 17; Rankin, 2013, p.1). The study design required 50 officers to wear cameras (nearly half volunteered, and the rest were assigned), and compared these officers with another set of "demographically similar" officers in the same department (White, 2014, p. 18) (presumably, all of these officers had chosen not to volunteer). In a final report compiled by the police department (Rankin, 2013), the research found that those officers who had volunteered were 60.5% more likely to activate and use the body cameras than the officers who had been assigned (Rankin, 2013, p. 1). Additionally, after the department modified its body-camera policy to allow officers greater discretion about when to record (from "when practical, officers will make every effort to activate the on-officer body camera when responding to a call or have any contact with the public" to activating the cameras when the officers "deem it appropriate"), the rate of use dropped by 42% (Rankin, 2013, p. 1). Officers wearing the cameras also received fewer departmental complaints (40% decrease) and use of force complaints

(75% decrease) during the study period, compared to the prior twelve months (Rankin, 2013, p. 1).

Interestingly, at the outset of the study, the Mesa Police Department evaluation team identified the single biggest challenge to body-camera adoption as integrating the footage into the public disclosure process under Arizona state law (Rankin, 2013, p. 5). In particular, the department's records supervisors insisted that "they are unable to complete the review of on-officer video," primarily because "the process is extremely time consuming and they do not have the personnel to absorb the increased workload" (Rankin, 2013, p. 12). As a consequence, the individual officers who filmed the video in the first place are sent the footage and are required to "review the video in its entirety" and identify elements of the video that need to be redacted, including "NCIC/ACJIS information, personal biographical information, juvenile faces, undercover officers, informants, nudity and other sensitive information as determined by the staff attorney" (Rankin, 2013, p. 12). The patrol officers are required to provide descriptions of materials to be redacted as well as timestamp information before redaction can take place (Rankin, 2013, p. 12). During the study period, the department reported receiving an average of three to four requests for body-camera footage per month (Rankin, 2013, p. 12). Of these 36-48 requests (the exact total is not reported) over the 12 month period, only three videos were forwarded by officers to the department's video unit for redaction, amounting to less than 6 hours of total footage requiring some redaction (Rankin, 2013, pp. 12-13). However, the total time to complete the redaction of these three clips took department personnel approximately 30.5 hours (Rankin, 2013, p. 13), more than five times the total running length of the videos.

An initial survey of officers participating in the body-camera program conducted by the department in conjunction with researchers at Arizona State University revealed that over 80% of officers felt the cameras would produce better evidence; over 76% felt the footage would be helpful to prosecute domestic violence cases where victims were unwilling to testify; 45% felt citizens would act more respectfully towards officers wearing cameras; almost 77% felt the cameras would make them act more professionally; 81% indicated the cameras would make them more cautious when making decisions; and fewer than half of the respondents believed their fellow officers would be receptive to having a camera on scene (Rankin, 2013, p. 11). However, only 23.5% indicated that the department should adopt body cameras (Rankin, 2013, p. 11).

In 2013, the Police Executive Research Forum (PERF) conducted a large-scale survey of police department use of BWCs with support from the U.S. Department of Justice's Office of Community Oriented Policing Services (COPS) (Miller and Toliver, 2014). PERF sent surveys to 500 police departments—receiving responses from 254 agencies for a 51% response rate—finding that, as of July 2013, over 75% of reporting agencies did not use BWCs, and nearly one-third of agencies that did use cameras did not have any written policy (Miller and Toliver, 2014, p. 2). The PERF research team also interviewed 40 police executives and convened a conference for more than 200 police agency representatives (Miller and Toliver, 2014, p. 2). Police administrators generally cited greater accountability and transparency as positive outcomes from BWC deployment,

including fewer complaints against officers—both through civilizing police-civilian encounters at the outset and by decreasing formal complaints by showing footage to civilians who come to the department seeking to file a complaint, resulting in civilians "literally turn[ing] and walk[ing] back out" (Miller and Toliver, 2014, pp. 5-6).

PERF also reported that BWC footage can be used as a useful training tool, allowing easier identification and correction of internal problems (Miller and Toliver, 2014, pp. 7-8), and as a useful tool for collecting better evidence for use in investigations and court proceedings (Miller and Toliver, 2014, p. 9). The PERF report discusses a number of privacy implications raised by BWC use, including their ability to enter private homes, to gather up-close surveillance footage that could be incorporated into facial recognition programs, or to enable voyeurism (e.g. a "person [might] be able to obtain video that was recorded inside a neighbor's home") through liberal public disclosure or posting to online repositories (Miller and Toliver, 2014, p. 11)[43], and the privacy intrusions possibly generated by certain data storage, retention, and disclosure policies (Miller and Toliver, 2014, pp. 15-16). In addition to these privacy-based concerns, PERF recommends against "always-on" recording policies:

> …requiring officers to record every encounter with the public would sometimes undermine community members' privacy rights and damage important police-community relationships. There are certain situations, such as interviews with crime victims and witnesses and informal, non-law enforcement interactions with members of the community, that call for affording officers some measure of discretion in determining whether to activate their cameras. There are situations in which not recording is a reasonable decision. An agency's body-worn camera policy should expressly describe these situations and provide solid guidance for officers when they exercise discretion not to record (Miller and Toliver, 2014, p. 12).

In its research, PERF found that most agencies with formal policies did not require officers to have their cameras always recording (Miller and Toliver, 2014, p. 13). Most commonly, agency policies allowed for some level of officer discretion, and directed officers to record encounters during "calls for service and during law enforcement-related encounters and activities, such as traffic stops, arrests, searches, interrogations, and pursuits" (Miller and Toliver, 2014, p. 13). PERF also reported that at least one state has changed its all-party consent requirement for officers wearing BWCs and that a number of agencies are requiring officers to announce that they are recording—although in others, such as Kansas, police only tell civilians the cameras are recording if they are asked (Miller and Toliver, 2014, p. 14).

In another on-going BWC study, Jennings, Fridell, and Lynch (2014) have reported findings from an initial survey of Orlando (Florida) Police Department officers. In their study, Jennings, Fridell, and Lynch (2014), received 91 responses to a survey (voluntary response, out of 95 officers who

[43] It appears that a neighbor could request this sort of footage in at least a couple of states (Washington and New Mexico, for example) (see Miller and Toliver, 2014, p. 15).

volunteered to participate in the research, and almost 400 eligible officers) of patrol officers in the Phoenix Police Department designed to examine officer perceptions about BWCs (p. 550). The survey was distributed *before* officers began using cameras in the field, to serve as a baseline for further research (Jennings, Fridell, and Lynch, 2014, p. 550). Officers were asked to respond to questions measuring their level of agreement with various statements on a Likert scale, from 1 to 5 (general, "strongly disagree" to "strongly agree") (Jennings, Fridell, and Lynch, 2014, p. 551). Responses indicated that 62.7% of officers agreed or strongly agreed that their department ought to adopt BWCs, 77% said they would feel comfortable wearing BWCs, and 18.7% agreed that BWCs would increase officer safety (Jennings, Fridell, and Lynch, 2014, p. 551). Fewer than half (40.7%) of the officers felt that BWCs would "improve citizen behavior," and only 19.8% felt BWCs "would improve their own behavior"—though 29.7% felt it would promote their own "by-the-book" behavior, and 42.9% felt it would promote "'by-the-book' behavior of other officers" (Jennings, Fridell, and Lynch, 2014, p. 551). Most (84.4%) believed BWCs would not decrease "their likelihood of responding to calls for service" (Jennings, Fridell, and Lynch, 2014, p. 551). In terms of use of force, few officers (3.3%) believed that BWCs would decrease "their own use of force," though more felt they would decrease external (30.8%) and internal (27.5%) complaints against officers (Jennings, Fridell, and Lynch, 2014, p. 551).[44]

Other studies of various sorts are ongoing with the Phoenix (Arizona) Police Department (White, 2014, p. 18; Katz and Kurtenbach, 2014; Jennings, Fridell, and Lynch, 2014, p. 550), Las Vegas (Nevada) Metropolitan Police Department (Lochhead, 2014), Los Angeles (California) Police Departments (National Institute of Justice, "Body-Worn Cameras"), New York Police Department (personal communication with researcher), and London's Metropolitan Police Service (College of Policing, 2015). In preliminary results from the Phoenix research, in which researchers equipped half of the 100 patrol officers in Phoenix Police Department's Maryvale Precinct with BWCs, officers reported concerns about the "potential negative impact" that the cameras might have for officers, including internal "fishing expeditions" and internal investigations of misconduct not generated by citizens (Katz and Kurtenbach, 2014). Katz and Kurtenbach (2014) also reported increased productivity (daily arrests per officer with BWC increased by 16%) and decreased complaints against officers wearing BWCs (44%).

7.3. Methodology

In this chapter, I primarily draw upon legal research, analytic argumentation, and the development of value scenarios and stakeholder analysis (Value Sensitive Design). I also draw briefly on some of my experiences observing the use of BWCs by officers in two police departments between September 2014 and February 2015 during on-going fieldwork with those two departments. This

[44] The Jennings, Fridell, and Lynch (2014) research paper also addresses a number of additional questions not summarized here, and performs analysis on differences by demographic variables (see Jennings, Fridell, and Lynch, 2014, pp. 551-552).

empirical data collection is presented here only to give context to the overarching questions about BWCs, privacy, and public access to BWC footage.

7.3.1. Legal research

In developing this chapter, I conducted legal research into the regulation of the use of BWC technologies by law enforcement agencies in Washington State, including state constitutional law, statutory law, decisions by Washington State courts, and federal case law related to the Fourth Amendment to the United States Constitution. To this end, I searched Washington law using Westlaw® Classic, and I also conducted general Google and Google Scholar (case law) searches to identify other relevant issues. For comparison, I also conducted searches of Westlaw's legal database and referred to various state legislature websites and news sources to determine whether legislatures in other states had proposed or adopted statutory laws regulating BWC use (or public access to footage) in their jurisdictions. In Westlaw, I searched for statutes and cases using the following search string: *"body worn camera!*" *OR* "*body worn video" OR "body camera!" OR "on-officer camera!" OR "on-officer video"*. I also conducted searches for potentially relevant Fourth Amendment search and seizure cases decided by the United States Supreme Court. (For a more general discussion of this method, see Chapter 2).

7.3.2. Value Sensitive Design

I utilize value scenarios, the value tensions framework, and conduct a stakeholder analysis. Value scenarios are used, not to predict the future, but as an analytic tool to help me anticipate what is at stake with various policy and regulatory options and as a communicative tool to help make the issues more readily comprehendible by placing them into narrative form. The value tensions perspective of VSD fits quite well into the larger framing of this dissertation, and helps me to remain grounded in the reality that the values at stake are complicatedly intertwined and—in some sense—need to be brought into balance (or at least alignment). Identifying stakeholders impacted by BWC use (privacy and spatial considerations related to data collection by BWC technologies), retention/sharing, and public access to BWC footage also helps to surface the conflicting values at stake, to make explicit which stakeholders and values are addressed throughout my analysis. (For a more general discussion of this method, see Chapter 2).

7.3.3. Empirical data collection and analyses

As stated earlier, my reliance on empirical research is utilized herein solely as a useful tool to help frame and guide my conceptual analysis. In this chapter (and especially in the introduction), I draw upon some of the findings from my own on-going empirical project, including fieldwork conducted with police officers in the Spokane Police Department and the Bellingham Police Department. The initial findings presented herein are sourced from ride-alongs, observation, and informal interviews with officers wearing BWCs in each of these departments.

7.3.1. Philosophical method

After the presentation of findings, I develop an analytic argument while examining and applying theory to the findings of law and to my initial and exploratory data analysis. This methodology carries over into Chapter 8, where I develop my broader normative arguments based on this Chapter as well as the other two cases presented in Chapters 5 and 6. For more specifics on my application of this methodology, see my expanded discussion in Chapter 2.

7.4. The legal implications of on-officer wearable cameras

The use of BWCs implicates a number of privacy concerns, despite potentially providing significant evidence for oversight and police accountability purposes. These privacy concerns can be divided into two main areas: 1) privacy violations stemming from the surveillance activities of the state, including the collection of evidence via BWC recordings and the nature of consent or notice required for such recording to occur in the first place, and 2) privacy violations occurring as a consequence of the public disclosure of BWC footage. The following two subsections (s. 1.4.1 and s. 1.4.2) address how pending legislation in Washington State has addressed these concerns, followed by a broader discussion (in subsections 1.4.3 to 1.4.5) of the privacy implications raised by the use of BWCs in Washington State.

As of March 2015, only two states appear to have enacted legislation directly applicable, and in response to, the possibility (or reality) of BWC adoption. In 2014, Pennsylvania enacted legislation that explicitly allows officers enforcing fish and game laws to wear body cameras, and exempts officers enforcing these laws from the state's all-party consent requirements (Pennsylvania Consolidated Statutes, Title 34 § 901(b.1); Pennsylvania Consolidated Statutes, Title 30 § 901(c)). Additionally, in Vermont, the legislature has enacted a law requiring the state's Law Enforcement Advisory Board to "study and make recommendations as to whether officers authorized to carry electronic control devices [e.g. TASERS] should be required to wear body cameras" (Vermont Statutes, Title 20 § 2367).

On the other hand, quite a few states have recently proposed legislation to regulate the use of BWCs or exempt BWC footage from public disclosure and judicial decisions are also beginning to note the presence of BWCs, or deal with the issues raised by BWC use, in cases brought to court.[45] In 2015, two bills were introduced into the Washington State Legislature that would regulate the use of BWCs; both would limit public access to BWC footage (see Washington House Bill 1917, 2015; Washington House Bill 1917 (Substituted), 2015; Washington House Bill 1910, 2015; Washington Senate Bill 5732, 2015).

[45] It should be noted that body cameras have been used by police in cases beginning in the late 1990s. For the earliest cases discussing body camera use, see Smith v. State, 229 Ga.App. 570 (1997) and United States v. Davis, 326 F.3d 361 (2003).

7.4.1. Body worn camera legislation addressing public disclosure in Washington

House Bill 1910 and identical Senate Bill 5732, which appear to have died in committee, would exempt most audio and video captured by BWCs and dashboard cameras[46] from public disclosure (see Washington House Bill 1910, 2015, s. 3(5); Washington Senate Bill 5732, 2015, s. 3(5)). According to the bills, audio and video recordings generated by these devices "is for the exclusive use of investigations of potential law enforcement misconduct" and may only be used for internal investigations or court proceedings if "the action or proceeding relates to or arises as a result of law enforcement misconduct" (Washington House Bill 1910, 2015, s. 3(5)). However, the bill makes exceptions for public access in cases where footage is "flagged"[47] as useful for oversight purposes (Washington House Bill 1910, 2015, s. 6(1)(a)). Footage is "flagged" when it is:

> (1) …related to an incident involving the use of force, or for which a complaint, formal or informal, is registered;…
> (2) …when requested by a subject of the recording;…
> (3) …when requested by any other person only if:
> (a) The recording was not made inside a private residence; and
> (b) The requester presents specific, articulable facts to support a reasonable belief that law enforcement misconduct occurred during the incident related to the recording (Washington House Bill 1910, 2015, s. 4(1)-(3)).

House Bill 1910 would further regulate disclosure to third parties (those not the subjects of the recording(s) at issue) by requiring "consent of the subject of the recording" and, if a recording contains multiple subjects, redaction of the video, "if feasible, to obscure the identity of all subjects who have not consented to disclosure" (Washington House Bill 1910, 2015, s. 6(1)(b)). Any unflagged recordings could only be disclosed when "all subjects of the recording" consent, or when redaction of all non-consenting subjects has occurred (Washington House Bill 1910, 2015, s. 6(1)(c)). Under the bill, unflagged recordings would be kept for between 60 and 75 days, and flagged recordings must be retained for at least three years (longer if subject to pending resolution in any on-going misconduct investigation).

In comparison to House Bill 1910, House Bill 1917 would also limit public disclosure of BWC footage. This bill has been amended and, as of March 28, 2015, has been consolidated into a substituted version (Washington House Bill 1917 (Substitute), 2015) by the House Committee on Judiciary, and is currently before the House Rules Committee for its second reading. Substitute House Bill 1917, in its preamble, states that while individuals maintain no expectation of privacy when "interacting with law enforcement or corrections officers carrying out their official duties…

---

[46] The bills describe BWCs and dashboard cameras as "law enforcement oversight recorders" and limit the use of resulting video solely to law enforcement oversight and the prosecution of police misconduct.

[47] Section 2, subsection 1 of the proposed bill defines "Flag" as meaning: "to identify a recording as potentially containing evidence that is useful for purposes of oversight of law enforcement conduct in a manner consistent with section 4 of this act" (Washington House Bill 1910, 2015, s. 2(1)).

those individuals do not surrender their right to privacy as it relates to the public records act" (Washington House Bill 1917 (Substitute), 2015, s. 1).

> The legislature intends to promote transparency and accountability by permitting individuals who interact with law enforcement or corrections officers to access the video and/or sound recordings of these interactions while preserving the public's reasonable expectation that the recordings of these interactions will not be publicly disclosed to enable voyeurism or exploitation (Washington House Bill 1917 (Substitute), 2015, s. 1).

To those ends, the bill further states that recordings "made by uniformed law enforcement or corrections officers while in the course of their official duties" may not be made available to the public, unless the requestor specifies 1) the name(s) of the person(s) "involved in the incident and the case number" or 2) "the date, time, and location of the incident" (Washington House Bill 1917 (Substitute), 2015, ss. 1(c)(i)(A)(I)-(II)). Such requests may be made by "a person directly involved in the [recorded] incident" or their attorney, and must be accompanied by a "certification under penalty of perjury… that the person requesting disclosure does not intend to use the recording to intimidate, threaten, abuse, or harass any individual on the recording" (Washington House Bill 1917 (Substitute), 2015, s. 1(c)(i)(B)(I)). All other persons seeking disclosure of BWC recordings would be required to obtain:

> …a court order finding, by clear and convincing evidence, that: The public interest in the disclosure of the video and/or sound recording significantly outweighs the privacy interests of the person or persons whose image or sound is contained in the recording (Washington House Bill 1917 (Substitute), 2015, s. 1(c)(i)(B)(II)).

This same provision would also place the burden on the requester to prove, as part of the process to obtain the aforementioned court order, that the requestor had identified each non-law enforcement officer appearing in the recording(s) and had notified them of the requested disclosure "in the best manner practicable under the circumstances, including individual notice to every person who can be identified through reasonable effort" (Washington House Bill 1917 (Substitute), 2015, s. 1(c)(i)(B)(II)).[48] Additionally, each of these notified persons must have had a reasonable opportunity to seek and obtain a court order, if they so chose, to enjoin the disclosure of the requested recordings (Washington House Bill 1917 (Substitute), 2015, s. 1(c)(i)(B)(II)).

Substitute Bill 1917 would also allow law enforcement agencies to require requestors to identify themselves—a change, as currently the Public Records Act allows anonymous requests—and to pay the costs incurred to redact the audio and/or video requested (Washington House Bill 1917 (Substitute), 2015, ss. 1(c)(ii)-(iii)). Also, in contrast to House Bill 1910/Senate Bill 5732, Substitute Bill 1917 would allow agencies to use footage for accountability, evidentiary, and any other lawful purposes (Washington House Bill 1917 (Substitute), 2015, s. 1(c)(iii)).

---

[48] Note, however, that the bill would require law enforcement agencies to "provide information [to the requestor] sufficient to enable the giving of notice, where available, so long as that would not interfere with ongoing investigations" (Washington House Bill 1917 (Substitute), 2015, s. 1(c)(i)(B)(II)).

7.4.2. Body worn camera legislation addressing other privacy concerns in Washington

In the preambulatory section of House Bill 1910, the bill's authors note the tensions between BWCs as an effective oversight tool and the potential for this new tool of surveillance to invade personal privacy "and subject members of the public to unwarranted public attention" (Washington House Bill 1910, 2015, s. 1). The bill would require that BWCs and dashboard cameras be operated "continuously… while law enforcement officers are on duty"—which would not include time periods when officers were using the restroom or taking a "scheduled or routine break" (Washington House Bill 1910, 2015, ss. 3(1)-(2)(b)). Officers would be required to inform members of the public when they are recording (and such statement must be captured on the recording itself), except in exigent circumstances (Washington House Bill 1910, 2015, s. 3(3)). The bill would also extend the current exemption from the Privacy Act's all-party consent requirement for dashboard cameras to BWCs as well (Washington House Bill 1910, 2015, s. 9(1)(c)).

Substitute House Bill 1917, on the other hand, would also extend the dashboard camera exemption from the Privacy Act to BWCs, and it also extends this exemption to corrections officers as well (Washington House Bill 1917 (Substitute), 2015, s. 2(1)). The bill would also require law enforcement agencies using BWCs to establish policies that address when officers must (or must not) record, how to deal with circumstances where individuals refuse to speak to an officer while the officer is recording, and how officers should document when and why they deactivated their BWC during an interaction with a member of the public (Washington House Bill 1917 (Substitute), 2015, ss. 5(1)-(3)).

7.4.3. Privacy, space, and collecting evidence

In public spaces, the use of BWC systems poses fewer problems than when used by police within homes, businesses, or other non-public spaces, but important problems still remain. Even when these cameras are worn and activated during the execution of search or arrest warrants within a person's home or other non-public place, for example, serious privacy implications arise when the recordings may capture individuals, activities, or information that would otherwise not be relevant to the investigation at hand. This reality could potentially open up the plain view exception[49] and allow subsequent searches and seizures based not only on an officer's actual—real-time—observation, but on ex-post review of footage. For the sake of argument, I will assume that the benefits of having a record of police conduct to serve oversight goals may override the individual privacy interests at stake in some circumstances—at least insofar as the initial capture of the

[49] In regards to digital evidence and the plain view exception, Orin Kerr has argued that, "Although uncertainty about the direction of technological change counsels caution, the best option ultimately may be to reconfigure the plain view doctrine for digital searches. Computer hard drives store a tremendous amount of private information that can be exposed even in a targeted search. If everything comes into plain view, the plain view exception threatens to swallow the rule. Narrowing or even eliminating the plain view exception may eventually be needed to ensure that warrants to search computers do not become the functional equivalent of general warrants" (Kerr, 2005, p. 566).

recording is concerned. However, if subsequent access to and use of the recordings extends beyond these purposes, or is even available to any member of the public upon filing a public disclosure request, such use poses a serious invasion of personal privacy.

Additionally, the increasing effectiveness of facial recognition software, even in consumer products like Facebook, means that simply recording an image of a person (in a private or public space) can lead to further identification (either in real time or post hoc). These realities implicate an increased ability of state surveillance to gather, collect, combine, and analyze personal information—and this reality suggests the state is capable of exercising a greater amount of power over the individual. Officer-mounted wearable cameras, paired with facial recognition, could easily become much like the current crop of automated license readers, constantly reading thousands of faces (license plates), interpreting identity (plate number), and cross checking this information against national and local crime databases in real-time. Officers could then respond to information instantly pushed to a heads-up display (e.g. Google Glass-like glasses, visor, or other augmented reality heads-up display[50]) and react appropriately by detaining, questioning, or arresting the unsuspecting individual. This power itself is not necessarily inimical to individual liberty (e.g. the public may have, with proper informed consideration and deliberative democratic action, approved the surveillance), but it should be treated with suspicion when it makes domination possible.

Under current Washington law, recording a private conversation without the consent of all parties would violate the state Privacy Act (RCW § 9.73.030), as discussed *supra* in sections 4.3.2 and 6.4.2. However, this prohibition may only limit police use of BWCs in very limited circumstances. As discussed in Chapter 6, conversations between a police officer and a civilian in a public place (or within the hearing of passersby) would not constitute a private conversation for purposes of the Privacy Act.[51] Additionally, in Washington State law, whatever a person has "voluntarily exposed to the general public and [that is] observable without the use of enhancement devices from an unprotected area is not considered part of a person's private affairs" (State v. Creegan, 2004, p. 722, quoting State v. Jackson, 2002, p. 683, quoting State v. Young, 1994, p 182). To reiterate, the Washington State Supreme Court's test for determining whether a conversation is private, has recently been restated in State v. Roden (2014):

> In determining whether a communication is private, we consider the subjective intention of the parties and may also consider other factors that bear on the reasonableness of the participants' expectations, such as the duration and subject matter of the communication, the location of the communication, and the presence of potential third parties. We will generally presume that conversations between

[50] For a very brief introduction to some of the legal and technological issues at play with these sorts of augmented reality systems, see Roesner, et al. 2014.

[51] In State v Flora (1992), a Washington court came to this conclusion when the conversation was conducted "on a public thoroughfare in the presence of a third party and within the sight and hearing of passersby" (p. 806).

two parties are intended to be private (State v. Roden, 2014, p. 900 (internal citations omitted); see also State v. Kipp, 2014, p. 729).

The Washington State Attorney General has also recently issued an opinion stating that all "conversations between police officers and members of the public, when the officers are performing their official duties and are known to the other speakers to be performing their official duties, are not private conversations" (Ferguson, 2014, p. *4, citing State v. Kipp, 2014, p. 732, Lewis v. State Dept. of Licensing, 2006, p. 460, and Johnson v. Hawe, 2004, pp. 682-83). Under this interpretation, even BWC recordings made by uniformed officers inside private residences would not be subject to the Privacy Act, as the conversations would not be considered a *private conversation*.[52] Additionally, because police can obtain implied consent by merely announcing that they are making a recording before engaging in conversation or entering a private space (RCW 9.73.030(3)), they can ensure their compliance with law fairly easily (even though it is likely the announcement is not legally required in the first place).

Video surveillance can constitute a search for Fourth Amendment or state constitutional purposes. However, when the police have a lawful right to be inside a private home, it is somewhat unclear how a recording would violate those constitutional interests—at least as long as the recordings were made for purposes related to the police officers' legitimate presence in the home.[53] However, there are a few situations that would appear to strain current doctrine or, at least, raise seemingly unanswered questions. First, all of the cases holding that conversations with police officers are not private have been decided in the context of officer-citizen conversations; none have considered the possibility of the recordings capturing peripheral conversations between other persons inside the home (see Ferguson, 2014, p. *6). One Washington Supreme Court decision has indicated that, "a conversation between two other parties is not private where they know a police officer is present" (Furguson, 2014, p. *6, citing Lewis v. State Dept. of Licensing, 2006, p. 465).[54] Absent this knowledge of the police officer's presence, a court would need to examine the context of the

---

[52] In State v. Kipp (2014), the Washington Supreme Court found that a conversation recorded by an accused person's brother-in-law in a private kitchen violated the Privacy Act because the accused had a legitimate expectation that a conversation (even a confession to a crime) between two private individuals would not be recorded absent his consent. However, the court also noted that the result might have been different had the recording been made by a police officer (during a conversation with the officer) rather than by the brother-in-law (see State v. Kipp, 2014, p. 732). This decision, and the AG Opinion (Furguson, 2014), seem to have clarified earlier questions about the applicability of the Privacy Act to BWCs. In an earlier memo within the Seattle Police Department, concerns had been raised that recording would expose "police to potential civil suits. State law does allow an exception for dashboard-mounted cameras in police cars but not body cameras on police officers.… The city law department has informed the police department that 'it would be unwise to implement a body camera program without first obtaining a legislative exception to the Washington Privacy Act'" (Rosenberg, 2011).

[53] However, any use of the recordings beyond the legitimate scope of the officer's presence could possibly constitute a Fourth Amendment violation (see Wilson v. Layne, 1999, p. 613; Ferguson, 2014, p. *7).

[54] In Lewis, the court stated that, "the same factors that indicate that a driver does not have a reasonable expectation of privacy with an officer during a traffic stop conversation also indicate there is no reasonable expectation of privacy in other conversations that same driver might have in the presence of the officer during a traffic stop, such as with his passenger or with another party over a cellular phone" (Lewis v. State Dept. of Licensing, 2006, p. 465).

conversation, as indicated in State v. Roden (2014) and State v. Kipp (2014), including analyzing whether the *subject matter* of the conversation was potentially incriminating (making a finding of an expectation of privacy more likely) (Furguson, 2014, p. *6).

Second, whether sustained or systematic observation of a home can rise to a constitutional violation may be an open question—though it is not instantly clear how frequent or common this use of BWCs might be in practice, as opposed to fixed-pole-mounted camera surveillance. The U.S. Supreme Court has repeatedly authorized single (non-recurring) instances of surveillance of private residences (see California v. Ciraolo, 1986; Dow Chemical Co. v. United States, 1986; Florida v. Riley, 1989). However, in an on-going federal criminal case based in Washington State, Senior Judge Edward Shea of the Eastern District of Washington ordered the suppression of six weeks of video evidence obtained by police from a camera mounted on a utility pole outside the defendant's house. Judge Shea found that,

> The American people have a reasonable expectation of privacy in the activities occurring in and around the front yard of their homes particularly where the home is located in a very rural, isolated setting. This reasonable expectation of privacy prohibits the warrantless, continuous, and covert recording of Mr. Vargas' front yard for six weeks (United States v. Vargas, 2014, p. 2).

Thus, it appears likely that no significant state or constitutional privacy laws would restrain officers from recording in the basic scenario of a BWC-wearing police officer entering a private residence by consent (or while executing a warrant) and, in some cases, stating that s/he was recording.

7.4.4. Public disclosure of body worn camera footage in Washington

As discussed in Chapter 4, Washington State has a very broad and inclusive public disclosure law (RCW § 42.56.001 et seq.). BWC footage is subject to disclosure under the Washington Public Records Act (PRA) (see Sullivan, 2014a; Lucia, 2014). Requests for BWC footage, like that discussed above in the introduction to this Chapter, have caused quite a stir amongst Washington police agencies, including causing some departments to halt BWC deployment (Lucia, 2014) or consider shelving cameras (personal communication) and leading the Seattle Police Department to collaborate with local technologists in its first-ever Hackathon to work towards a software-based mechanism to automatically redact footage prior to disclosure (Sullivan, 2014b). The Seattle Police Department subsequently started proactively posting over-redacted footage[55] to a public YouTube channel (Seattle Police Department, 2015).[56] Additionally, the liberal disclosure of BWC footage is further motivated by the fact that the PRA defaults to a position that records should be disclosed, and places the burden on government agencies to articulate why redaction or denials are appropriate under one of the applicable exemptions (Fisher Broadcasting-Seattle TV

[55] The SPD has applied a few different types of redaction to this footage. Generally, however, their "over-redaction" has consisted of applying a Gaussian blur to the whole frame of video and removing the audio stream entirely.

[56] The channel is accessible at https://www.youtube.com/channel/UCcdSPRNt1HmzkTL9aSDfKuA.

LLC v. City of Seattle, 2014, pp. 521-522; In re Request of Rosier, 1986, p. 609), as well as that the law penalizes overbroad secrecy but not generally over-disclosure.[57]

In Fisher Broadcasting-Seattle TV LLC v. City of Seattle (2014), the Washington Supreme Court held that dash camera videos were subject to the PRA, and that the Seattle Police Department had violated the law when it refused to disclose videos to a reporter who had requested them under the PRA (Fisher Broadcasting-Seattle TV LLC v. City of Seattle, 2014, p. 529). In that case, the police department argued that privacy provisions of the state Privacy Act, specifically RCW 9.73.030(1)(c), limited their ability to produce the requested dash camera videos (Fisher Broadcasting-Seattle TV LLC v. City of Seattle, 2014, p. 525). The police department argued that the Privacy Act operated as an "other statute" under the PRA (RCW § 42.56.070(1))—which would have effectively made it a legitimate basis for an exemption to disclosure. However, the majority of the court concluded that RCW 9.73.090(1)(c) "is a limited exception to immediate disclosure under the PRA, but it is one that applies only where there is actual, pending litigation" (Fisher Broadcasting-Seattle TV LLC v. City of Seattle, 2014, p. 528). This decision effectively confirms that all police footage is publicly disclosable absent explicit statutory exemptions, and that the Privacy Act cannot bar such disclosure except when criminal or civil litigation related to the footage has been filed and is actually on-going. Indeed, there is no general privacy exemption to the PRA in Washington law, and the privacy provisions of the PRA itself (RCW § 42.56.050) cannot be claimed as a stand-alone exemption (Washington Administrative Code § 44-14-06002(2)). That provision reads:

> A person's "right to privacy," "right of privacy," "privacy," or "personal privacy," as these terms are used in this chapter, is invaded or violated only if disclosure of information about the person: (1) Would be highly offensive to a reasonable person, and (2) is not of legitimate concern to the public. The provisions of this chapter dealing with the right to privacy in certain public records do not create any right of privacy beyond those rights that are specified in this chapter as express exemptions from the public's right to inspect, examine, or copy public records (RCW § 42.56.050).

As such, any explicitly stated exemption from disclosure on privacy grounds would be limited to the extent the above criteria is also met; that is, that the purportedly exempt information—based on the express provisions in another section of the act or another law—must also be "highly offensive to a reasonable person" and "not of legitimate concern to the public" (RCW § 42.56.050). If not, it must be disclosed.

While footage itself may be disclosable under the PRA, certain additional exemptions do apply that would require redaction. For example, the federal Driver Privacy Protection Act (18 USC §§

[57] Indeed, the PRA explicitly absolves agencies of liability for harm caused by disclosure as long as they acted in "good faith." RCW § 42.56.060 ("No public agency, public official, public employee, or custodian shall be liable, nor shall a cause of action exist, for any loss or damage based upon the release of a public record if the public agency, public official, public employee, or custodian acted in good faith in attempting to comply with the provisions of this chapter").

2721-2725) makes it unlawful for state agencies to disclose personal information connected to a motor vehicle record (including drivers licenses). Under Washington law, it is also unlawful for agencies to disclose (among others, many of which are not directly applicable to BWC footage (see RCW § 42.56.240 for others):

> Information revealing the identity of persons who are witnesses to or victims of crime or who file complaints with investigative, law enforcement, or penology agencies, other than the commission, if disclosure would endanger any person's life, physical safety, or property (RCW § 42.56.240(2)).

Victims, witnesses, or complainants may also indicate "a desire for disclosure or nondisclosure," and their stated desire should govern decisions about disclosure (RCW § 42.56.240(2)). However, even a stated desire for nondisclosure may be subject to the test enumerated in RCW 42.56.050 requiring the disclosure to be highly offensive and not of public concern (see Martin v. Riverside School Dist. No. 416, 2014, p. 35).

State law also exempts certain investigative records compiled by law enforcement agencies when nondisclosure "is essential to effective law enforcement or for the protection of any person's right to privacy" (RCW § 42.56.240(1)). However, the Washington Supreme Court has held that this provision should be construed narrowly (like all exemptions) and did not always constitute a categorical exemption (Sargent v. Seattle Police Department, 2013, pp. 386-387). A categorical exemption might apply to BWC footage when the footage is an integral part of an investigative file in an unsolved and on-going criminal investigation where charges had not yet been filed (see Sargent v. Seattle Police Department, 2013, p. 387, citing Newman v. King County, 1997, pp. 574-575). However, in cases where defendants have been identified and charges have been filed, "nondisclosure is not categorical and automatic" and legitimate reasons for nondisclosure must be proved by the agency "on a document-by-document basis" (Sargent v. Seattle Police Department, 2013, p. 388-389, *citing* Cowles Pub. Co. v. Spokane Police Department, 1999, pp. 479-480). Because, presumably, most BWC footage will not be essential to criminal investigations, this exemption may only apply to a small subset of all recorded videos.

Additionally, RCW 42.56.230 exempts certain personal information from disclosure, including information about "students in public schools, patients or clients of public institutions or public health agencies, or welfare recipients" (RCW § 42.56.230(1)), children enrolled in early care or certain youth programs (RCW § 42.56.230(2)), personnel files for "employees, appointees, or elected officials" of public agencies (RCW § 42.56.230(3)), certain information related to tax preparation (RCW § 42.56.230(4)), certain financial information (RCW §§ 42.56.230(5)-(6)), records "used to prove identity, age, residential address, social security number, or other personal information required to apply for a driver's license or identicard… that indicates that an applicant declined to register with the selective service system" and other records "pertaining to a vehicle license plate, driver's license, or identicard" or vessel registration (RCW § 42.56.230(7)), and

"information related to individual claims resolution structured settlement agreements submitted to the board of industrial insurance appeals" (RCW § 42.56.230(8)).[58]

Many of the exemptions to the PRA are unlikely to apply to BWC footage on a routine basis, but individuals responsible for public disclosure are required to review both video and the audio of recorded BWC footage prior to disclosure, and this process takes a tremendous amount of time and agency resources (see Rankin, 2013, pp. 5, 12).

7.5. Value Sensitive Design

Police use of BWCs implicates privacy interests both by recording police interactions with civilians and by the subsequent use and/or public disclosure of the resulting footage, which raises sharp tensions between these privacy interests and access to government information for oversight purposes. In the case of BWCs, despite the public-facing rationale for adopting the cameras as police oversight tools, the primary subjects of the original recordings are actually the civilians—officers generally acting off screen, behind the cameras mounted on their bodies. The publication of BWC recordings to the internet or through other media channels by police agencies or civilians functions—just like the publication of ALPR data or civilian video—as a form of secondary visibility of police officers and of civilians alike. The public disclosure of these videos offers the potential for privacy harms similar to those discussed in the previous two chapters. In the following paragraphs, I conduct a stakeholder analysis, outline a fictional, yet possible future, and then present two value scenarios based on that hypothetical future. As in the previous chapters, I focus on elaborating narratives with relevance to the "five key elements" addressed in the application of value scenarios under the VSD framework; that is, to "develop provocative sketches of the future: stakeholders, pervasiveness, time, systemic effects, and value implications" (Nathan, Klasnja, and Friedman, 2007, p. 2587).

7.5.1. Direct and indirect stakeholders

As in Chapter 6, there are potentially a large number of stakeholders who directly interact with the technologies in question (BWCs), including the police officers who wear the cameras, civilians subject to being recorded, public disclosure personnel, and requestors under the PRA. As in prior VSD research (Miller, et al., 2007, pp. 283-284) and in the prior chapter, I identify direct stakeholders in this case by the role the stakeholder plays in connection to the system under

[58] Other exemptions apply to information related to employment and licensing (RCW § 42.56.250), real estate appraisals (RCW § 42.56.260), other financial and commercial information (RCW § 42.56.270), preliminary drafts, notes, and intra-agency memorandums (RCW § 42.56.280), locations of archaeological sites (RCW § 42.56.300), library patron records (RCW § 42.56.310), educational information (RCW § 42.56.320), certain public utility information (RCW § 42.56.330), and health care information (RCW § 42.56.360) and some personal information about health care professionals (RCW § 42.56.350), client records of domestic violence or sexual assault recovery programs (RCW § 42.56.370), certain information about agricultural and livestock operations (RCW § 42.56.380), persons in emergency or transitional housing (RCW § 42.56.390), certain information held by insurance and financial institutions (RCW § 42.56.400), and a variety of other reasons.

examination—in this case, by interactions with the process of recording, disclosing, and posting BWC video. For purposes of this project, I define *direct stakeholders* as those individuals—generally police department or city employees or members of the public—who actually engage in the recording (role 1), public disclosure/redaction processes (role 2), and/or requesting and uploading (role 3) of BWC video to publicly accessible websites, such as YouTube, Facebook, blogs, or police accountability-related websites (e.g. CopWatch). Unlike in the case of civilian video, the roles here will presumably be more separated, as different individuals will likely take part in the different roles.[59] *Indirect stakeholders* (those who do not directly interact with, but who are affected by the output), on the other hand, may also include a vast number of individuals or other entities, including police officers, bystanders and anyone else caught on tape (i.e. not primary subjects of the recordings), companies whose property is captured on video, and internet service providers who host, index, or link to the BWC-generated content and who may have to react to requests for removal (e.g. on the basis of privacy violations) or de-linking under European laws such as the right to be forgotten or the right to erasure (see European Commission, 2014; Tsesis, 2014; Google Spain SL v. Agencia Espanola de Proteccion de Datos, 2013). Court personnel, police executives, taxpayers, and the general public who may change behavior based on perceptions about the use of the technology or the possible disclosure of footage are all also indirect stakeholders in this analysis—though any of these people who also engage more directly with the technology would be direct stakeholders. As in Chapter 6, I am limiting my discussion of indirect stakeholders to those individual persons (police or civilian actors or bystanders) who are identifiably captured on BWC video and, as a consequence of that identifiability, whose privacy rights may be implicated by subsequent disclosure of the footage.

7.5.2. BWC value scenarios: Overview of a possible future

In the past few years, BWCs have become enmeshed into society and citizens now expect (by default) that any encounter with a police officer will be recorded. Most BWCs are now interconnected within urban wireless mesh networks and contain a variety of sensors besides mere video and audio recording capabilities. As real-time biometric capabilities have improved, facial recognition, gait detection, and voice analysis software have become integrated into these systems, and the deployed technology now includes heads-up, augmented reality, displays that alert officers of potentially risky surroundings or the presence of wanted individuals by providing real-time information about individuals identified by the biometrics to the lenses of officers' glasses or the screens on their oversized—and wirelessly connected—wrist watches. More and more officers are being assigned to walking or bicycle patrols in urban areas, as the new technologies have become remarkably good at identifying wanted persons when worn in close proximity by officers on foot.

[59] Although, Rankin (2013) reported that the same police officers who recorded videos requested under Arizona's public records act were brought into the public disclosure process due to resource constraints at the Mesa Police Department's public records office.

7.5.3. Value scenario 1: Recording in private homes and the nosey neighbor

Scenario. Charles is a middle-aged construction worker who lives on his own in an apartment on a busy street in the downtown area of a large urban city. Some of his neighbors are college students, and others include other singles and families with small children. The complex is also quite racially and ethnically diverse. At times, the apartment complex receives quite a lot of police activity, especially at two apartments: 1) the apartment of 4 young female college students who frequently host late-night parties, and 2) the apartment of a couple with three small children who have frequently had the police show up to diffuse domestic violence or child welfare situations. Curious about what was happening, Charles has been requesting the BWC footage captured by officers responding to calls for service at these apartments for the past six months. At first, his requests were simply out of basic curiosity, but as time progressed he began to become addicted to watching the videos and started requesting videos for all of the people living on the street. His collection quickly included video showing neighbors during domestic disputes, children in various states of cleanliness and undress, police interactions with the local transient community, as well as footage of his college-aged neighbors intoxicated and in scantily clad attire. Recently, Charles started an anonymous blog where he posts particularly juicy videos and comments at length about "real life behind the doors" in his neighborhood, including detailed commentary responding to events depicted in the videos. While watching his last round of requested videos, Charles discovers that one of the videos appears to him to show the aftermath of a child abuse incident in which police barely saved the life of a six-year old child (who's very badly beaten face and body is depicted on screen). He immediately posts this video and his summary of events to his website, which gets numerous hits in the first few days. As it turns out, the child simply fell down the stairs and was not abused at all, but police had at first suspected abuse and the darkish video and chaotic audio did not clearly capture the resolution to that line of questioning.

Discussion. This scenario is actually based on discussions of possible scenarios I've had with police officers during my on-going fieldwork, as well as actual observation of BWC use during ride-alongs with officers. Some of the officers I have talked to have actually recorded footage that depicts dead children, domestic disputes, and a variety of other very sensitive (and disturbing) content. Some have shown me the footage their cameras have captured (if I wasn't present) during conversations about what should or should not be subject to public disclosure. The current state of the law in Washington would allow the disclosure of some of this sensitive material. However, public disclosure only becomes a problem when there is something to disclose. Before discussing the appropriateness of disclosing this sort of footage, this scenario begs questions about whether the footage ought to be recorded inside private residences or in certain circumstances in the first place. And, even if we didn't limit all recording inside homes, perhaps we should allow those present to determine whether they consent to the recording as well as to public disclosure if the recording is made. The information contained on the footage may include things not relevant to the police-civilian encounter or call for service or that were not noticed by the officers at the time the recording was made. The mere documentation and retention of this information by the state—with all the possibilities inherent in subsequent analysis—implicates domination. And because

one of the overarching pillars of neorepublican theory is the normative claim that states should not function in ways that dominate their citizenry, this collection is suspect absent consent or other reasonable grounds for the officers' to record these encounters.[60] On the other hand, if footage is recorded, the public disclosure of this sensitive information could empower other private individuals—in this case, Charles—to acquire dominating power over the subjects of the videos. And this disclosure would effectively function as a license to cast visibility on private information that would otherwise be objectionable under civil tort theories of privacy, such as the tort of intrusion. In the scenario above, we might question whether we want Charles—or any other random citizen—entrusted with the task of uncovering and publicizing situations like child or spousal abuse, rather than the police. The information Charles would access would already be in the hands of the police (from whom he received it), and the ability of the camera to function as an objective observer capturing all relevant facts is probably somewhat spurious. In any case, it would appear that the presence of BWCs and the risk of increased visibility vis-à-vis public disclosure could easily function to make people think twice about calling the police or letting them into their homes, even in times of emergencies.

7.5.4. Value scenario 2: Proactive disclosure but limited public access

Scenario. In attempts to protect civilian privacy, the state has exempted public disclosure of BWC footage but has allowed agencies to proactively post videos that don't intrude on protected privacy interests. Because of the deterrent effects of the disclosure of BWC video, the local police department has maintained a liberal policy in regards to releasing videos made in public spaces, and even posts many proactively to its own website. However, because not all videos are accessible, the press and public cannot ensure that all video of potential misconduct is noted and made part of the public record. Tami is a local reporter covering city hall and the police department. She has recently been investigating a few cases of alleged police misconduct brought to her attention by a group of local public defense attorneys whose clients claim police officers mistreated them. The police have repeatedly denied her requests for footage of these arrests, while claiming that internal investigations have shown that officer conduct has been warranted and not excessive.

Discussion. Most legislative proposals that have been addressing the disclosure of BWC footage have tilted in favor of largely exempting footage, which follows the trend identified in Chapter 5 in regards to the exemption of ALPR databases by state legislatures around the country. Some limits are undoubtedly warranted (and needed), however, swinging the pendulum too far in the other direction towards nondisclosure would seriously undermine the ability of these tools to serve their intended oversight purposes. Should review of footage for potential misconduct be restricted to inside the doors of police departments, we lose public accountability and BWCs become simply

[60] These might include situations where the need to document events is heightened when, for example, officers have a reasoned and articulable basis for assuming their efforts will be resisted or when the use of force or an arrest is likely, or in other emergencies that would give rise to an exception to the Fourth Amendment.

another form of invasive state surveillance. However, we have other options that can serve the purposes of providing obscurity and limiting the collateral visibility of private individuals as well as allowing for oversight and disclosure. Option 1: agencies could provide the public with the identified videos in over-redacted form, such as that piloted by the Seattle Police Department (Seattle Police Department, 2015)—however, this option does potentially open up the possibility that re-identification could occur, either through another form of biometric identification such as gait detection that might be useable even after faces have been blurred or if algorithms are developed to reverse blurring processes, for instance. Option 2: we limit public disclosure on privacy grounds (as mentioned above) but we allow for court orders to require the more limited disclosure to wronged parties (or even the media) when there is a reason to do so—and this might also include in-camera review by judges to limit fishing expeditions by defense attorneys who might use footage to troll for potential clients.[61] Option 3: we establish an independent oversight body that bears responsibility of reviewing otherwise exempt footage in these circumstances prior to making determinations about whether broader release or use in litigation is appropriate.

7.6. Discussion

The use of BWC systems does have the obvious effect of documenting more encounters, which can then serve as evidence for or against officer or citizen misconduct. However, too much reliance on audio-visual evidence could also decontextualize events and also, possibly, diminish the recognition given by the public and courts to the realities that confront police officers on the ground. In short, it may lead to judgments about the wrongness/rightness of police action based on small windows of reality that ignore some relevant context. This may also affect policing by further diminishing the amount of discretion available to officers. Indeed, as Bittner (1990) found, police have historically kept few records of procedures that do not involve making arrests (p. 32) and the nature of their work has unavoidably led to officers having a great deal of discretionary freedom (p. 48). These facts, combined with the reality that police work has long been divided into both law enforcement and peace keeping activities (which involves officer discretion and action outside the domain of making arrests) (Bittner, 1990, pp. 31-32), suggests that always-on wearable cameras might begin to document wide swaths of police conduct that have heretofore been largely left to the officers themselves. Thus, in the context of skid row policing investigated by Bittner (1990), the fact that officers use force to effectuate arrests on the basis of risk (considered in the aggregate for the area) and personal knowledge, rather than mere individual culpability, may be antithetical to the wider public's notions about legitimate police work.

Bittner (1990) has stated:

> When arrests are made, there exist, at least in the ideal, certain criteria by reference to which the arrest can be judged as having been made more or less properly, and there are some persons who, in the natural course of events, actually judge the

[61] I have been told by officers during ride alongs that defense attorneys have already begun requesting footage from departments for this purpose.

> performance. But for actions not resulting in arrest there are no such criteria and no such judges" (p. 37).

However, with the rise in the number of cameras present in public, and the advent of the officer-mounted wearable camera, these non-arrest situations are becoming increasingly documented and, as a consequence, there are potentially numerous judges (police administrators, elected officials, or the public) and a variety of criteria against which individual officer conduct may begin to be judged. These realities are exacerbated by the ease of uploading footage to the internet and the availability of police records under public disclosure and freedom of information laws.

The resultant footage could be viewed, searched, and analyzed by superiors, and if accessible to the public under state disclosure laws, could provide very broad ranging access to records of such police work. This reality also suggests that what it means to do a good job "keeping the peace" could be defined more by outside forces than by the officers themselves. This will likely create tensions between the officers' self-perception as separate and distinct "skilled practitioners" and the public's preferred perception of police as subservient to society (see Bittner, 1990, p. 33; Herbert, 2006b).[62] Some argue that wearable cameras promise to document police abuse and also preserve evidence to exonerate officers falsely accused of improper conduct (see e.g. Franklin, 2013). A transparent monitoring system, this argument suggests, would encourage proper behavior on both sides and would restore trust in policing. Others, argue that police would only behave more appropriately under surveillance if they know someone is actually going to watch what their cameras record (i.e. active monitoring/oversight) and that wearable cameras shouldn't replace written reports, including legal justifications for officer actions (see e.g. La Vigne, 2013).

Relatedly, preserving the rights of citizens to conduct reciprocal surveillance is also an important aspect of this overall question (see e.g. Sellars, 2013; see also Newell, 2014a; 2014b). Significant questions also remain about whether (and to what extent) these cameras could also be used to intimidate or chill legitimate speech and other protected activities or even whether individuals will be less likely to report crime or call the police for assistance because of the additional, collateral, visibility that would be foisted upon them due to the liberal public disclosure regime. Additionally, long-term storage and archiving of police footage could pose a threat to privacy interests of innocent citizens, as the release of such footage under state disclosure laws threatens to "embarrass" innocent bystanders caught on tape or individuals who ask police for help in sensitive circumstances (while also serving the ends of citizen oversight as a form of reciprocal surveillance). Despite these concerns, the ACLU originally claimed that wearable police cameras are a "win-win" situation, stating that,

---

[62] Additionally, whether officers engage in forms of resistance (see e.g. Marx, 2003; Grenville, 2010; Haggarty and Ericson, 2006; Monahan, 2006; Shay, Conti and Hartzog, 2013; Wilson and Serisier, 2010), to mandated surveillance or citizen-initiated surveillance (e.g. by selectively recording interactions with citizens, confiscating cameras/cellphones, and/or destroying footage) also poses some fascinating, and important, empirical research questions that bear heavily on any attempts to normatively define proper policies, laws, or regulations.

> Although we [the ACLU] generally take a dim view of the proliferation of surveillance cameras in American life, police on-body cameras are different because of their potential to serve as a check against the abuse of power by police officers (Stanley, 2013).

This is not a claim that should be made lightly without a deeper empirical understanding of the effect of these systems in society (and the forms of police officer resistance to the surveillance attendant in BWC deployment that may become clear from such research).

Research has indicated that the use of officer-mounted wearable cameras has reduced instances of officers using force and the number of citizen complaints (Ariel, Farrar, and Sutherland, 2014; Ariel and Farrar, 2013; Rankin, 2013; see also Jennings, Fridell, and Lynch, 2014). Many of the proposed benefits, as well as significant causes for concern, are tied to the concept of police visibility (with its potential to change the dynamics of police-citizen encounters, to either exonerate or implicate officers in wrongdoing, or to provide evidence of citizen misconduct). As stated earlier (in Chapter 3) police departments have "a clear interest in *how* their personnel and activities become visible to others and in *what* is revealed as a result to outsiders" (Goldsmith, 2010, p. 915, *citing* Mawby, 2002, *and* Adut, 2008). Left to their own devices, a move towards secrecy is obviously a strong possibility—a possibility that is limited by robust access laws. This reality points towards the importance of understanding police conduct (and possible reactions to BWC deployment) through the lenses outlined in Chapter 3, namely Goldsmith's (2010) articulation of "policing's new visibility" and his argument that any value to the police of increased visibility was contingent "upon maintaining 'normal appearances' and delivering 'proper performances'" (p. 915, *citing* Goffman, 1971; 1990); Herbert's theory about how subservience, separateness, and generativity affect and are interwoven into police officer conduct; and a recognition of how BWCs and increased visibility might impact officer discretion during what Bittner (1990) called the "peace keeping" aspects of policing—potentially restricting officers' ability to "act alternatively" to diffuse situations without issuing citations or making arrests (see Bittner, 1990, p. 36).

The deployment of BWCs may only serve to support citizen oversight and law enforcement accountability when 1) the cameras are either always on (that is, officers have no discretion as to when/whether the cameras are recording) or 2) officers adhere to strict guidelines requiring activation during every citizen encounter (unlikely without strict policies, active oversight, and engaged supervision), and 3) citizens are provided adequate *ex post* access to recorded footage to dispute charges or challenge officer conduct, 4) access to recorded footage is strictly regulated to information relevant to active (or potential) official investigations or prosecutions (of police OR civilian misconduct) and to proper personnel, and 5) footage is consistently and routinely destroyed in a manner that respects the above requirements.

In the aftermath of police-involved killings in Ferguson, Missouri and New York, in 2014, the adoption of BWC technologies by police departments around the country has come under much greater scrutiny. The racial tensions between non-white communities and their local law

enforcement agencies around the country were exacerbated by the deaths of Michael Brown, Eric Garner, and Walter Scott at the hands of white police officers. Violent protests followed, and calls for mandatory camera adoption started to become a common occurrence in the media. Post-Ferguson, civil liberties organizations, communities, and a variety of commentators came out publicly in favor of outfitting officers with body-worn cameras.

Footage from a body-camera may well have provided better evidence of what transpired between Michael Brown and Officer Darren Wilson than what was actually available from conflicting eyewitness testimony and after-the-fact civilian video. However, the potential for police body cameras to increase transparency and accountability needs to be considered side-by-side with a consideration of the privacy risks inherent in the use of such technologies, as well as the inherent limitations of the technology itself to stand in as a neutral observer (which is questionable). It is also important that little or no research has yet addressed many of the questions that surround the adoption of BWCs (see White, 2014, p. 6), including the impact of access to information law on police department administration, personal privacy, and other civil liberties. When technologies touted as tools to make law enforcement officers more visible in cases where alleged misconduct occurs also lead to drastic increases in civilian visibility, we need to think critically about how to regulate the use of these systems of surveillance. We cannot ignore the unintended consequences—such as the *collateral visibility* and horizontal surveillance of and between civilians enabled by public disclosure—that make our lives more transparent; not just to government agents, but also to our neighbors and the world at large. If not, we may find that the walls of our homes become transparent to the world anytime we invite a police officer though the front door.

If policing is a means to an end—a means to create social order through the application of power (see e.g. Bittner, 1990, pp. 94-97)—then the addition of wearable cameras to the officer's toolkit must be examined for its potential to quell or instigate various forms of violence. Information, seen as some "thing" that facilitates knowledge (Buckland, 1991) and grants power to its holder over the information subject (see Forcese and Freeman, 2004, pp. 481-84), can enable power of some over others. Through vertical surveillance, police gain evidentiary information (as "knowledge" (Buckland, 1991, p. 351)—and possibly investigatory information through subsequent analysis, if allowed—about civilians. And through public disclosure of footage in which other civilians are the primary subjects, citizens can engage in increasingly revealing forms of horizontal surveillance, potentially generating shifts in power relationships among ordinary people.

The use of wearable cameras also has the potential to alter or disrupt the nature of non-reported, so-called "peace keeping," aspects of policing and the attendant discretion that officers have historically had for their activities not resulting in arrests. Wearable cameras may serve to exacerbate the compromised position of the patrol officer, who is often under the "dual pressure[s] to 'be right' and to 'do something,'" even in stressful or dangerous situations) (Bittner, 1990, p. 97). The use of BWCs can be a two edged sword. It promises some benefits, but also poses important problems. The use of such systems is not necessarily inimical to freedom (and its

attendant privacy and speech concerns), but significant checks need to be employed to ensure against the possibility of arbitrary interference and the improper use of power generated through the accumulation of information and potential intimidation implicit in these surveillance practices. In a modern society where surveillance has become a stable and accepted element of everyday life, it is appropriate to consider the role of research "to make surveillance strange again, and therefore open to rigorous examination and possibly change" (Wood and Webster, 2009, p. 260).

7.7. Conclusion

Despite decades of increasingly safer streets and fewer instances of serious police-citizen violence in America (US DOJ, 2003), the police continue to hold a highly criticized role in society (this is not a new phenomenon; *see* Bittner, 1990, pp. 89-102). Indeed, most recent press about police use of new technologies has focused on the negative implications that these developments have on citizen privacy—which is an important concern—but less attention has been given to balancing these privacy interests with the important societal interest in promoting effective and efficient police work. The tensions between these competing—and legitimate—aims is substantial and, in the context of police use of wearable camera systems, limiting the scope of law enforcement data collection and retention to protect citizen privacy might also protect the privacy of the police officers using these systems, as disclosure of the resultant footage to the public under freedom of information (FOI) laws can allow citizens to track the historical policing patterns of individual officers and scrutinize officer conduct, especially if the systems are always on. Thus, wearable cameras become a useful means of watching the officers themselves. In this context, the more recognizable tensions between protecting privacy and ensuring efficacious policing are compounded by a direct tension between privacy interests and freedom of information as citizen oversight—as an important form of freedom-preserving reciprocal surveillance. This form of checking government power resists the reification of potential domination. One possible response, limiting public access to footage, protects the privacy of innocent individuals and police officers, but it also limits the ability of the public to conduct oversight. Such oversight, with its attendant right to access information about government action, also serves important First Amendment interests in facilitating informed speech and enhancing democratic governance.

There are a few variables that must be accounted for to properly determine whether footage should be publicly accessible through FOI mechanisms. Each of these recommendations seeks to limit the potential for domination as well as the risks of collateral visibility by balancing oversight interests with the obscurity of personal information not necessary to that oversight. First, access should always be granted to the individual(s) depicted in the footage, especially the subjects of the police-citizen interactions depicted. Without this rule, BWCs would play the part of state surveillance with no corresponding oversight function—eviscerating the very possibility of oversight by those directly harmed by the police. This rule allows those charged with crimes or claiming police misconduct to bring evidence to light that may (or not) help prove their case and it also respects the rights of individuals to be informed about what information the state's surveillance has captured about them so that they can exercise their right to control subsequent use

of such information. Because the personal information of bystanders, victims, witnesses, and even suspects, are not likely to be needed to demonstrate police misconduct, blurring or otherwise obscuring or redacting identifiable information about these individuals prior to disclosure should be built into public disclosure laws and agency policies.

Second, excluding wider public access to the recorded footage may sometimes restrict the ability of the public and news media to serve important functions as watchdog. This limit to citizen oversight, as a basic level, reduces the effective antipower available to society and risks reifying dominating structures within government and law enforcement agencies. When the footage is recorded in public spaces, because of the claim that presence in public may involve a waiver of the right to access such information, the public's interest in access to footage may outweigh the full denial of requests for that footage, but this concern can be accommodated by requiring the anonymization of the faces of those individuals whose identities are not key to the oversight purposes of such access (e.g. innocent bystanders).[63]

Third, footage captured within a person's home (or other private area) should, by default, be protected more stringently than footage captured in public or outside locations. I do not discuss the notion of property much at all in this dissertation, but I believe property rights, like speech and privacy, also serve important liberty interests. Property rights also (rightly) encapsulate privacy interests—and in this case, spatial property rights should protect informational privacy interests in footage filmed in non-public spaces, and particularly inside private homes. These limits protect individuals from interference and domination by states or private agents, as well as from the prying eyes of neighbors and the voyeuristic tendencies of strangers. Likewise, because of the enhanced claim to privacy in a person's home as opposed to in a public space (e.g. a park or public sidewalk), public access to such footage under FOI laws should only be allowed when the person whose property and privacy interests are at issue consents to such disclosure.

[63] I recognize that this undoubtedly places significant pressure and administrative burden on agencies subject to disclosure laws, but I believe decisions about adopting BWCs should be made with these requirements in mind.

8. Conclusions: A theory of information policy

8.1. Outlining a theory of information policy

It is clear that democracy (and political liberty) should be predicated on the presumption that the public is sufficiently informed (or has the effective ability to become informed) and able to intelligently participate in political life (including having the capability to engage in oversight of government action), regardless of whether a preferred political theory claims civic virtue is inherently or instrumentally valuable. And, "[w]ithout access to adequate and appropriate information related to governance, such informed participation and deliberation are impossible" (Jaeger, 2007, p. 843; see also Cohen, 2012; 2013; Newell, 2014c; 2014d). However, promoting broad access to government information does raise concerns about information reliability, comprehensibility, completeness, privacy of data subjects, and a host of other problems (Dawes, 2010, p. 378). Access to information itself can also effect direct violations of privacy when personal information is disclosed as part of government records (Solove, 2002). Thus, as we seek to balance liberty with security—with public access and government secrecy for certain purposes—we need to critically and thoughtfully evaluate the broader ramifications of our information policies.

Much current liberal privacy theory fails to adequately protect privacy in an age of ubiquitous vertical and horizontal surveillance. The phenomena encapsulated within the concept of "new visibility"—and discussed above in Chapters 5, 6, and 7— provide both the potential for enhanced civilian oversight as well as a host of new privacy intrusions. Modern surveillance capabilities, including increasingly sophisticated forms of *vision*, the aggregation of personal information across time and disparate systems—related to various concepts (e.g. what Solove (2001; 2002) calls the "database problem," what Haggarty and Ericson (2000; 2006) call the "surveillant assemblage," and what legal commentators have called the "mosaic" (Slobogin, 2012; Kerr, 2012))—and the permanence of digital memory, all point to a need to rethink how we structure privacy rights, from both a moral and legal perspective. In contemporary society, we also see the struggle to balance the proper functioning of government with the interests and rights of the people to access and document information about government activity. This conflict is characterized by increasing technological prowess on both sides as well as more institutional resort to information seeking, data mining, and monitoring of public (and private) spaces—both offline and on the internet—and by a focus on the security enhancing aspects of contemporary surveillance hailed by communitarians (see e.g. Etzioni, 2014).

Additionally, liberal conceptions of liberty and privacy based on restricting actual negative interference fail to coherently explain how covert surveillance that never results in actual interference with a person's life can constitute a privacy violation. However, viewing privacy and freedom through the lens of republican theory, we can explain the harm caused by these forms of surveillance by reference to the concept of *domination*. A republican conceptualization of privacy "grounded on the idea of freedom as non-domination can explain a loss of privacy where there is

no subsequent interference in terms of negative freedom" (Roberts, 2014, p. 10). As Roberts (2014), has clearly stated:

> … at the root of our anxieties about loss of privacy, is concern about what republicans will recognize as domination. While liberals can explain how a loss of privacy that does not lead to any interference might affect the individual's autonomy, where she is unaware of the loss, they will have difficulty in explaining the value of privacy (pp. 2-3).

When an individual's personal information is captured—in identifiable form and without their knowledge—by a passing police officer's body camera, or when their license plate is scanned by an ALPR system while their car is parked on a public street, and this information is subsequently stored in a police database but not actually accessed or used in any way, no actual (negative) interference has occurred. Negative liberal theories of privacy have difficulty explaining how privacy is violated, in this case, prior to any subsequent access to or use of this information by the state. Moore's (2010) control definition of privacy—which I have incorporated into my broader theory—does provide an argument that such information collection would violate a person's right to control access to that information—especially when our presence in public spaces cannot necessarily be considered entirely consensual. However, this limit on access to publicly visible information—without deeper justification—seems overly broad precisely because it would effectively limit all surveillance in public spaces absent particularized justifications from the police. In effect, it would prohibit all forms of persistent surveillance, including the use of CCTV cameras, ALPR cameras, body-cameras, etc. except in cases where police had acquired, for example, a warrant or some other form of particularized justification. The republican account, however, opens the way for such collection to occur, in the first instance, but only when citizens are sufficiently empowered to conduct oversight (i.e. when sufficient antipower exists) and when other limitations have been put into place to prevent the arbitrary use of the information against individuals.

Additionally, the potential violation of privacy in these scenarios cannot be explained by either of Calo's (2011) categories of privacy harm. The subjective category only extends to *actual subjective perception* of surveillance, and the objective category requires some actual "use of information about a person against that person" (Calo, 2011, p. 1143). On the other hand, republican theory can explain the violation in these cases by reference to domination—the existence of state of affairs where one entity *could interfere*, should it choose to, with another person's agency. This sort of covert collection generates the potential for arbitrary interference by the state into the lives of innocent citizens, and ought to be limited by requiring the institutionalization—into legal doctrine, technology design, and institutional practice—of elements of semantic discontinuity (Cohen, 2013; 2012) as a means to increase obscurity and empower democratic deliberation and a state of "play in everyday practice" (Cohen, 2012, p. 6). Only then can a theory satisfactorily account for conflicts between personal information privacy rights, government surveillance, and government disclosure of personally identifiable information contained in public records under access to information laws.

The current situation in Washington State provides a rich context in which to study the relationships and tensions among societal interests in effective, efficient, and fair law enforcement and criminal justice processes, personal privacy, and citizen oversight and state transparency. It is vitally important that we engage in interdisciplinary and multi-method socio-legal approaches to understanding how these instances of law and technology fit into a broader social context. This dissertation provides a largely conceptual account of the issues implicated by civilian video, police-worn body cameras, and automated license plate detection, but—given my commitment to socio-legal empirical inquiry of the sort espoused by new legal realism—much empirical inquiry is still needed. Some of this analysis is being completed in my own currently on-going research in which I am continuing to explore and analyze ALPR databases and the deployment of BWCs in local police agencies, but additional empirical questions remain unanswered.

Security, privacy, and liberty are all important aspects of a modern society. Security protects us from threats to our very lives—from crime and terrorism—and can provide the opportunities that we need to actually enjoy our privacy and liberty. Privacy allows us to develop personally, nurture relationships, gather information, engage in intellectual pursuits, and maintain dignity. Liberty allows us to be free from unnecessary interference and potential domination by others, including government. If we determine that all three of these values are of significant importance, then we must determine how to properly balance them—both generally and, if appropriate, in particular circumstances that demand certain (temporary) concessions. Whether to make concessions in our privacy and individual liberty for the promise of greater collective security is a choice that citizens often face, especially in times of national crisis, war, and threat from those who would do us harm (see generally Moore, 2011; Posner & Vermeule, 2003; Rosenfeld, 2006; Waldron, 2005).

In modern society, governments are conducting enormous amounts of surveillance—both online and offline—and are amassing huge databases of information about citizens within the scope of their searches. The enormity, and attendant reality, of this information gathering has been recently granted greater visibility as a consequence of The Guardian's recent publication of a classified court order granting the U.S. government on-going, daily, access to information about all calls (whether domestic or international) made over Verizon's systems, and top secret documents indicating that the U.S. government has had a high level of access to user data held by a number of large U.S.-based internet companies, including Google, Apple, and Facebook (the so called "PRISM" program) (Greenwald, 2013; Greenwald & MacAskill, 2013; Roberts & Ackerman, 2013). The public disclosure of ALPR databases and BWC footage by agencies in Washington State (and elsewhere) has also made what is collected more transparent.

Police departments and other government agencies are installing and utilizing video surveillance cameras in urban and commercial areas (or are accessing video footage filmed by privately-owned cameras); adopting body-worn cameras; utilizing automated license plate recognition systems to track and locate vehicles; data-mining information available online (including information from online social networks and personal data aggregation enterprises); employing facial recognition

systems to identify individuals; and using unmanned aerial vehicles (otherwise known as "drones") equipped with cameras, weapons, communications receivers and cellphone tower imitators.

8.2. An argument balancing access to information and privacy

As an initial matter, we must determine whether (and how) each of these scenarios limiting public access to government surveillance information implicates subjugation and domination. In the first two cases presented above, the government (or government agents) clearly have the actual capacity (rather than merely "virtual" or unrealized capacity) to exercise arbitrary power over the dominated person(s) because of their control of collected information (and of the modalities in which such information was obtained), whether by coercion, arrest (or threat of arrest or punishment), or limiting or refusing to release information. It is also clear that restricting (chilling) a person's free expression, their first amendment right to gather information (implicated by all three scenarios), or their right to acquire information about government activity, causes harm and affects a person's choices. This is especially apparent when, under Pettit's account of freedom, a subjugating interference with a person's choices may be limited to certain choices of varying centrality or importance, and need not totally remove all choices available to that person. Such interference by police officers or law enforcement (and the policy or law-making processes behind the enforcement) also clearly equates to "an intentional attempt to worsen an agent's situation of choice" (Pettit, 1996, p. 578) because it represents an intentional act that eliminates certain information that might be relevant to that decision-making process of that agent in that situation.

Since the Fourth Amendment generally does not protect against the government's collection of information and surveillance in public spaces, many forms of surveillance (e.g. use of body cameras, drones, cameras, license plate readers, and mining personal information on the internet) may not be subject to any real scrutiny through democratic processes or legal proceedings in courts of law. The legal and practical restrictions on citizens wanting to document or access information about government conduct, combined with the power of government to watch its citizens, represents an imbalanced situation where citizens lack the antipower they might otherwise command. As a result, we should question whether this is a situation in which:

> The powerless are not going to be able to look the powerful in the eye, conscious as each will be – and conscious as each will be of the other's consciousness – of this asymmetry. Both will share an awareness that the powerless can do nothing except by the leave of the powerful: that the powerless are at the mercy of the powerful and not on equal terms. The master–slave scenario will materialize, and the asymmetry between the two sides will be a communicative as well as an objective reality (Pettit, 1996, p. 584).

Perhaps this overstates the case somewhat. However, when the people do not have access to all of the information that supposedly supports the government's need to conduct various types of electronic surveillance, they do not have full access to information about what the government has done with the powers it has been given. This is inherently problematic, especially under the neorepublican position that governments should protect their peoples' freedoms and ensure that the state does not come to dominate its people in any arbitrary fashion. Without some form of

effective democratic check in place—some way for the public to make informed, deliberative choices based on real information—abuse (and domination) is always a real possibility.

Perhaps it is best—even essential—that citizens grant their governments some power to restrict public access to information for various purposes like criminal investigation or national security (though this seems less vital for crime control at the local state or municipal level), but this does not mean that citizens should not have the right to insist on safeguards, and the right to ensure the government complies with constitutional requirements in the exercise of its power. If that were so, the exercise of power would cease to be arbitrary, and the action would not be subjugating. The people would retain antipower.

Because the people are sovereign and should retain antipower *vis-à-vis* their government, there should be a presumption that the people retain the right to access government information and to document information about how the government discharges its duties. However, a presumption, by definition, may be overcome in appropriate circumstances, and a more robust description and explication of the appropriate threshold is in order. In some instances, it might be appropriate for a state to withhold information from its people—potentially an act of domination if the people have not granted such power—, acting unilaterally or on its own, for the protection of the people and national security, as long as certain safeguards are put in place to properly respect the sovereignty of the people. Thus, building on this argument, we can see that the state, absent powers granted by its citizens, may not generally withhold information about its activities from its people or deny them the right to access information about government activity, because such actions are acts of domination. However, as stated above, this theory does have room to entertain the idea that certain state interests, such as national security, may sometimes justify the state in withholding information from its citizens, despite the possibility that such withholding may infringe the people's antipower, thus overcoming the initial presumption.

Importantly, there appears to be a significant difference (in terms of the threat to antipower) between government decisions re secrecy (and the related risks to law enforcement or national security) of 1) the substantive information collected by the government (i.e. the actual information or metadata collected through mechanisms of surveillance), and 2) the procedural information about how the government conducts its activities (surveillance activities or otherwise) or the legal processes that authorize such conduct. This division rests on the idea that the Constitution protects the people from certain inappropriate actions of government (e.g. the Fourth Amendment prohibition on unreasonable and unjustified searches or seizures).

Domination is also more clearly implicated in terms of government conduct (or the potentiality of arbitrary conduct) that interferes with a person's situation of choice than it is with the nature of the underlying information.[64] Thus, the following distinctions need to be made: First, there is a greater

[64] Although this can also be constitutionally significant, for example, in the distinction between content and non-content information about a citizen's communications under the Fourth Amendment, but this distinction is often secondary to the procedural question about whether the information was obtained lawfully in the first place.

abrogation of the peoples' antipower when the state withholds information about the methods and procedures used by the state to collect the information and to approve information gathering activities of the state than when the state withholds substantive information collected by the state about its citizens or other targets.

Second, if the state collects information about its citizens, but denies its citizens the right to know what information has been collected about them, the state has acted in a dominating manner unless the people themselves have authorized the government to withhold such information and sufficient constitutional safeguards are put in place to ensure civil liberties are not violated. In no case, however, shall the people relinquish their right to sovereignty by allowing the government to act without censure in ways that may violate the Constitution (for example, by relinquishing their right and ability to access information about the methods and procedures used by government to carry out and justify its surveillance activities). Thus, if the state exercises its surveillance powers, but denies its citizens the right to know or document how this information was collected, and what procedural requirements were met to authorize such information gathering, then the state has acted in a dominating way by eliminating the citizens' antipower, and has come to impermissibly dominate its citizens because it has eliminated the sovereign right of its people to ensure that their government protects their freedom and Constitutional rights. Likewise, a government acts in a dominating fashion when it engages in the initial collection of its citizens' personal information without their knowledge and informed consent.

The preceding argument leads to the conclusion that, because the people are sovereign, they should presumptively retain the right to access and document information about how their government conducts the activities and duties entrusted to it by the people. This presumptive right of access encompasses information about how government agents conduct surveillance and what information is gathered through such surveillance activities, subject only to determinations by the people themselves that certain information be kept secret (for example, for national security purposes). In any case, however, the state may not withhold information about the methods and procedures used to gather the information or the procedural requirements used to authorize such information gathering.

However, at least one additional problem needs to be addressed at this point. The allowance just made for government secrecy must be tempered. If it is not, the peoples' antipower has been severely limited and the state retains much of the power the argument presented in this paper has sought to limit. The allowance was predicated on the assumption that sometimes certain information ought to be secret to protect the peoples' interests in security and protection by the state from outside evils. But such secrecy does not necessarily need to persist for lengthy periods of time, and certainly not in perpetuity. Sunlight provisions, or enforceable and mandatory declassification provisions, would provide a balance between law enforcement and national security interests (when those interests are present and legitimate) and the peoples' right to sovereignty and liberty by providing a form of retroactive accountability. This idea, despite its

simplicity, is an incredibly important core issue, and is vital to a proper balancing of the security and liberty interests at stake.

Thus, we may concede that substantive information collected by governments about its citizens or other targets may sometimes be withheld from the people, because release would compromise legitimate national security interests, without eliminating the usefulness or force of our neorepublican conception of freedom. But, as just stated, withholding this information in perpetuity always impermissibly infringes the people's antipower, unless the people effectively retain the right to override the State's ability to classify the information in perpetuity. Thus, when government surveillance information is withheld from the people for national security purposes, it should only be temporarily withheld, mandatory sunlight provisions should be specified clearly in the law, and the people should retain the power to ensure information is released consistent with the relevant sunlight provision(s). Importantly, such provisions might also contain clauses that allow the people to hold state actors accountable for violations of their rights after the information is lawfully declassified, should violations of constitutional or legal rights be identified.

This argument provides justification—based on republican concerns for liberty and a robust opportunity for citizen oversight of state action—for broad access to information laws. However, much of this dissertation has been premised on the claim that such broad access to surveillance information that references personally identifiable persons may violate individual privacy. Indeed, Jaeger's (2007) concept of "information politics," meaning "the manipulation of information access for political gain" (p. 851), suggests that much of the problems attributable to information access are related to personal information privacy. Governments and citizens both potentially have much greater access to information about the activities of the other than they have in the past—and this information has the potential to produce and influence power on both sides (see Forcese & Freeman, 2005, pp. 481–84). Information can equal power, and if rights to personal privacy are not respected by the state, the imbalance indicates a potential for subjugation. And, when personal information that could create dominating power when controlled by the state is released to the public under the guide of state transparency, we have a situation where individual visibility becomes the collateral damage of our transparency regime—what I refer to herein as *collateral visibility*.

Thus, we also need to account for the personal privacy concerns raised by the discussion presented in the preceding chapters. Because of the direct tensions between privacy and speech—including, but not limited to access to information—and the nature of constitutional law, we must also account for First Amendment considerations. Democratic theories of free speech—like those announced by Meiklejohn (1961; 1960; 1948) and Post (1997; 1995; 1993)— that focus on prioritizing speech that enables democratic participation provide one way to claim that personal privacy interests should be overridden by speech only when the speech furthers the democratic project and pertains to self-governance. As stated by Meiklejohn (1961), "the First Amendment does not protect a "freedom to speak," rather, "it protects the freedom of those activities of thought and

communication by which we 'govern'" (p. 255). I return to the powerful statement by Justice Brandeis in Whitney v. California (1927):

> Those who won our independence believed that the final end of the State was to make men free to develop their faculties, and that, in its government, the deliberative forces should prevail over the arbitrary. They valued liberty both as an end, and as a means… that, without free speech and assembly, discussion would be futile; that, with them, discussion affords ordinarily adequate protection against the dissemination of noxious doctrine; that the greatest menace to freedom is an inert people; that public discussion is a political duty, and that this should be a fundamental principle of the American government" (Whitney v. California, 1927, p. 375).

As Jack Balkin (2009) also argues, the First Amendment's free speech principle may be about more than just democracy—at least defined narrowly, e.g. voting. It may include some aspects for what Balkin (2009) calls "democratic culture," meaning, "a culture in which ordinary people can participate, both collectively and individually, in the creation and elaboration of cultural meanings that constitute them as individuals" (p. 438). As stated earlier, I read this claim as related to (and potentially consistent with) Meiklejohn's (1961, p. 263) extension of free speech rights to the creation of novels, dramas, paintings, and poems—which Meiklejohn believes are necessary to educated and informed voting and political participation. According to Balkin (2009), democratic culture is "about individual liberty as well as collective self-governance" (p. 3). These claims also resonate with Cohen's (2013; 2013) emphasis on achieving a state of human flourishing (liberty) through making space for individuals to "play" in their process of self-development.

Thus, in my view, the First Amendment (and the aspects of freedom of information laws that are related to free speech concerns), is inextricably tied up in notions of self-government, truth discovery (at least when restricted to matters related to governing or, if not, those that do not invade another person's privacy), checking potential government abuse or domination, and, to some extent, allowing individuals to participate in the creation of culture and meaning within society. That said, we should recognize robust rights to gather information, the ability to withdraw and contemplate or discuss openly and debate ideas in public, to think and believe as each sees fit, and to assemble for these purposes, insofar as such activity does not violate another person's rights (including the right to privacy). However, speech that does not promote, facilitate, or relate to self-government may need to give way to privacy rights.

Information privacy (defined as the right to control access to and uses of personal information) can be squared with the First Amendment rights of speech, association, and belief in a couple of primary ways (see Moore, 2013; 2010). First, the First Amendment itself protects certain privacy interests, including the right to speak anonymously (McIntyre v. Ohio Elections Commission, 1995; Solove, et al., 2006), the freedom of assembly (National Association for the Advancement of Colored People v. Alabama, 1958; Solove, et al., 2006), freedom of thought (Richards, 2008; Blitz, 2009; Palko v. Connecticut, 1937) and, to some extent, the right to gather information (First Nat'l Bank v. Bellotti, 1978; Glik v. Cunniffe, 2011). All of these First Amendment protected

activities implicate privacy in various ways, and also help to limit the potential for domination of individual citizens or groups by states or other actors.

Second, conceptualizing free speech as primarily protecting communication that promotes or impacts democratic self-governance allows for stronger personal privacy rights to control personal information than, say, Volokh's (2000) prioritization of speech would permit. For example, if the government is restricted from regulating or prohibiting strictly private speech (e.g. if it cannot limit the right to publish intimate personal details about another person, even when this information is not connected to self-governance), protecting a robust right to control access to and use of our own personal information becomes much more difficult. It would essentially equate privacy with absolute secrecy. However, under a democratic theory of free speech, such as that provided by Meiklejohn (1961; 1960; 1948) Sunstein (1992; 1993), Baker (1978; 1989), or Post (1997; 1995; 1993), the government could legitimately provide legal avenues of redress for such invasions of privacy.[65] Additionally, establishing the boundaries of privacy and free speech as largely driven by collective social choices enables citizens to control the level of privacy they prefer as a society—against a baseline minimum that may be required to ensure against domination.[66]

In my view, privacy and free speech should both be protected for two reasons: they limit the possibility of arbitrary interference by another with an individual's choices and they promote the ability of the people to engage in open (or closed) democratic deliberation and active civic participation. When privacy and free speech are not in conflict, they both promote these ends and are not in significant tension. In some cases, government records might contain both information relevant to self-governance and purely personal information about individuals. When these pieces of information can be teased apart, we ought to require disclosure *after* redaction to protect the personal information from disclosure. However, when these values conflict—that is, when the personal information is inextricably tied to, or is itself, related to issues of state accountability or other aspects of self-governance—, we must determine how to balance or bound these competing interests. When the information at issue is not related to self-governance, even when used in a context that Balkin (2009) might consider supportive of "democratic culture," privacy rights ought to prevail. In my mind, the making of cultural artifacts and the idea of supporting democratic culture is also a valuable aspect of free speech, but not one that ought to trump privacy interests in most cases, given the potentially serious ramifications of collateral visibility.

Generally, I believe each of these rights should be protected vigorously as far as they don't interfere with the rights of another person or group. The right to free speech—or to access government information—should trump the right to privacy when the speech at issue concerns information relevant to self-governance (a difficult question, admittedly) but, when speech is not related to self-governance and another's privacy interests are implicated, privacy should prevail.

---

[65] E.g. Prosser's (1960) tort of publication of private facts.

[66] Of course, in practice, this enterprise would only be truly successful if paired with a strong right to access information related to state surveillance, national security, and other countervailing interests might otherwise be chosen over privacy, so as to ensure informed deliberation and decision-making.

When government records contain both sensitive personal information and information about government surveillance, for instance, partial disclosure and redaction is entirely appropriate as a means to separate the two types of information as much as possible. Speech in the public interest (defined narrowly to include speech relevant to governance and deliberation about social issues), then, may prevail over privacy rights in some cases, but ought to do so only when public access to the personal information is *necessary for informed choices about proper governance* (e.g. the public should be able to talk candidly about a public official involved in a scandal or illegal activities). Again, speech and access to information concerns should only trump individual privacy rights when use of the personal information itself is needed to properly inform the public of a matter of general public interest (this is the phrasing used in the ECtHR's decisions, though "public interest" as used here ought to be defined in terms of its relevance to self-government). Thus, if omitting another's personal information can satisfy the democratic aims of speech, such redactions are appropriate and should be required.

As stated above, I believe the right to free speech should trump the right to privacy when the speech at issue concerns information relevant to self-governance. In this case, we have a compelling reason to prioritize speech.[67] For example, when a journalist reveals private information about a politician—say that s/he has been receiving political donations from certain special interest groups related to pending legislation—the journalist's right to publish should outweigh the politician's right to control the journalist's access to and use of that information. In this scenario, active democratic deliberation and civic participation is served by prioritizing free speech. Prioritizing privacy in this case would subvert the purposes of protecting these rights in the first place. It may also be the case that this balancing promotes and preserves the privacy of lay individuals, and that disclosure about public officials or government agents (e.g. police officers) is generally more permissible—as long as the information disclosed is necessary for the citizenry to make informed political decisions. In fact, I believe this outcome is the desired end. Body-camera footage filmed inside a person's home during a domestic violence response should not become part of the public record unless, and until, an officer is charged with an allegation of misconduct. Even in this scenario, redaction of personal information not relevant to the misconduct allegation should be required.

On the other hand, when speech concerns information that is not relevant to self-governance and both parties are private individuals—e.g. a spurned lover publishing an expose on the intimate details of a sexual relationship—, such speech should not necessarily outweigh the privacy interests at stake. Prioritizing the free speech rights, at the expense of the other person's privacy, would similarly violate their interest in avoiding interference with their own personal choice to keep the information private, unless we hold that sharing this information with the other person—

[67] Of course, determining whether information is relevant to such ends is not easy, but I would argue 1) that it is possible as a practical legal matter, and 2) that the ECtHR has struck a better balance than many American courts on this issue and could serve as a guidepost: *cf.* Von Hannover v. Germany (2004) *with* Time, Inc. v. Hill (1967), New York Times v. Sullivan (1964), *and* DeGregorio v. CBS (1984).

the speaker—constituted some form of implied waiver of privacy in that information. Such a waiver would apply only to the use of the information by the individual it was originally shared with, and would not apply to surreptitiously intercepted information. In this case, however, the speech is not relevant to self-government (though I suppose we could cook a case where it was), and there are pressing reasons to prioritize the privacy interests at stake. Because the speech implicates some important interests, but not the most core interests in promoting democratic governance, it may generally give way to another person's claim of personal privacy. In another example, discussed by Moore (2013) and based on an actual legal case (Cape Publications v. Bridges, 1982), a rape victim was photographed leaving the scene of her attack and the photograph and other personal information were published in the media accounts of the incident. In this case, as Moore (2013) notes, there is no compelling reason to reveal the personal information of the victim—in fact, doing so does not further democratic aims but merely violates her right to control access to and the subsequent dissemination of personal information about herself. Her name and address—and her face—are irrelevant to democratic self-governance. Thus, privacy ought to trump speech in this and similar cases. Importantly, however, individuals and the press ought to maintain the right to speak, write, and publish information about the case that does not invade the victim's privacy. However, these situations concerning private parties are much more difficult than those implicated by state-citizen interactions. My focus in this project is directly focused on access to information held by government agencies (specifically, information collected by police departments through the use of ALPR and body-camera surveillance technologies) and broader questions about citizen access to information about (or their right to document) how the government conducts its business, not directly on the proper limits on speech between private parties.

8.3. Conclusion

In conclusion, it is important to note the potential objection of the dominant liberal view that freedom (of the negative kind) is really noninterference. The attraction of this view is clear. Can we really say that a person is less free when no one ever actually interferes with his or her speech or ability to access information (despite the possibility, however vague and unlikely) than when no one can interfere? This view makes great intuitive sense, but it also creates some potential problems. For example, it problematizes forms of non-arbitrary, democratically decided, and appealable acts of interference, such as the application of law itself. On this view, any application of law is an abrogation of freedom, regardless of whether the enforcer acted on clear constitutional grounds and without impunity. The noninterference view of freedom was embraced by some, like Hobbes, Paley, and Bentham, to argue that all law and every form of government restricted liberty, whether enacted by democratic authority or despotic rulers, American revolutionaries or the British parliament (Lovett & Pettit, 2009, pp. 13–15; Pettit, 1996, pp. 598–600). Clearly, noninterference is an aspect of freedom, but why should all interference negate freedom per se?

Viewing freedom as antipower—as the absence of domination by another—allows us to respect the importance of noninterference, but also to recognize that some forms of interference (those

that are not arbitrary or without recourse) do not necessarily restrict our freedoms, but may only condition it (Pettit, 1997, pp. 26, 56, 76, 83, 94, 104; Pettit, 2002, p. 342). On this view, we can see that proper application of the nonvoluntaristic rule of law (with opportunities for effective appeal and democratic participation) actually protects and preserves our freedoms, rather than restricting them as a means to some other end. A person living under a friendly despot is not in the same position—in terms of freedom—as the person living in a properly constituted constitutional democracy with limits on domination. Fully realizing a situation of more equalized reciprocal surveillance and rights to access information about government activities (with temporary exceptions as may be needed to protect important state interests, as described above) would give citizens greater ability to ensure their government was not overreaching and abusing its authority, to hold the state and state actors accountable for rights violations, and to maintain government as an entity that protects it citizens' freedoms without coming to subjugate them to arbitrary exercises of power. However, the public disclosure of personal information held in state surveillance databases should be weighed against its implications for personal privacy and its use relevance to democratic self-governance, and redaction may be an important tool to help balance the tensions at play between privacy and access.

Consequently, the version of neorepublican theory developed in this paper and applied to information policy, with its core concept of freedom as nondomination, provides valuable insights into how one-sided surveillance powers and control of information vested in states can limit individual freedom. Applying neorepublican political theory in this context represents an important and novel application of these valuable ideas with the capacity to inform future information policy research and the development of better laws and policies related to surveillance, secrecy, and access to information. However, maintaining too narrow a focus on nondomination alone may obscure the continuing importance of restricting actual unjustified interference. Actual interference is, importantly, a more serious problem for freedom than is the mere possibility that such interference could take place in the future. As a consequence, we might be suspect of republican or liberal approaches that prioritize positive freedoms at the expense of limiting our focus on the importance of limiting actual interference, especially when such interference is—or might be—arbitrarily exercised by one agent over another. Ultimately, however, the differences between the version of neorepublicanism espoused here and more traditional liberal theories of negative freedom may not be as incommensurate as some prior work suggests.

At the end of the day, the primary point of this argument is not that we eliminate or unduly restrict the ability of government and law enforcement to conduct surveillance (or to restrict access to certain information in some cases), but rather that we recognize the bargain we have struck, in our representative democratic society, that the government assume some surveillance powers—and thus encroach on our individual negative freedoms to some degree—because they have the ability (and the responsibility) to use these powers for the public good; namely, public safety and national security. Our contract, and our consent, does not negate the possibility of domination or the relevance of freedom (Pettit, 1996, p. 585). The neorepublican concept of non-domination allows us to address, understand, and accept this reality. However, this power cannot be granted without

strings attached, and privacy ought to be safeguarded to preserve the individual right to control access to and uses of our personal information.

Fundamentally, I agree with Westin (1967) that, "the achievement of privacy for individuals, families, and groups in modern society has become a matter of freedom rather than the product of necessity" (pp. 21-22). Like Cohen (2013), I also argue that "freedom from surveillance, whether public or private, is foundational to the practice of informed and reflective citizenship" and that "privacy… is an indispensable structural feature of liberal democratic political systems" (p. 1905; see also Roberts, 2014). Viewed through the lens of republican political theory, privacy is also broadly valuable because it allows us to conceptualize how individual privacy can be violated in situations involving direct interference by another entity (the typical case addressed in many liberal theories), as well as when an individual is "aware that he has suffered a loss of privacy, but suffers no subsequent interference," and when the person "is unaware that he has suffered any loss of privacy, and suffers no subsequent interference" (Roberts, 2014, p. 1). This broad conceptualization of privacy as both inherently valuable in itself and instrumental to democratic self-governance and generating antipower, would provide robust privacy rights in an age of ubiquitous vertical (panoptic) and horizontal (omnioptic) electronic surveillance, even when such surveillance is conducted covertly and results in harms not always detectable by reference to identifiable interference.[68]

[68] For a discussion of republican theory and privacy applied to covert mass surveillance by the National Security Agency and in other contexts, see Newell, 2014d; 2014c.

References

1987 Session Laws of the State of Washington, regular session, fiftieth legislature, volume 2, available online at http://leg.wa.gov/CodeReviser/documents/sessionlaw/1987pam2.pdf.

Ackerman, Spencer. 2013. "Data for the Boston Marathon Investigation Will Be Crowdsourced." *Wired* (Apr. 16, 2013, 1:18 PM), http://www.wired.com/dangerroom/2013/04/boston-crowdsourced/.

ACLU of Illinois v. Alvarez, 679 F.3d 583, 586 (7th Cir. 2012), *cert. denied*, 133 S. Ct. 651 (2012).

ACLU-PA [American Civil Liberties Union-Pennsylvania]. 2012. Press Release: "ACLU-PA, ACLU Files Suit On Behalf of Fayette County Man Arrested for Recording Police Officer." American Civil Liberties Union-Pennsylvania, July 19, 2012, http://www.aclupa.org/news/2012/07/19/aclu-files-suit-behalf-fayette-county-man-arrested-recording-police-officer.

ACLU-PA [American Civil Liberties Union-Pennsylvania]. 2013. Press Release: "ACLU-PA, ACLU-PA Files First in Series of Lawsuits Over Illegal Arrests for Observing and Recording Philadelphia Police." American Civil Liberties Union-Pennsylvania, Jan. 16, 2013, http://www.aclupa.org/news-/2013/01/16/aclupa-files-first-series-lawsuits-over-illegal-arrests-for-observing-and-recording-philly-police;

ACLUM [American Civil Liberties Union of Massachusetts]. 2012. Press release: "City of Boston pays $170,000 to settle landmark case involving man arrested for recording police with cell phone." American Civil Liberties Union of Massachusetts, March 27, 2012, https://www.aclum.org/news_3.27.12.

Adams v. King County, 164 Wash. 2d 640 (Wash. 2008).

Adut, Ari. 2008. *On Scandal: Moral Disturbances in Society, Politics, and Art.* Cambridge: Cambridge University Press.

Alford v. Haner, 333 F.3d 972 (9th Cir. 2003).

Allen, Anita L. 2011. *Privacy Law and Society*. West Academic Publishing.

Antony, Mary Grace, and Ryan J. Thomas. 2010. "This is citizen journalism at its finest": YouTube and the public sphere in the Oscar Grant shooting incident. *New Media & Society, 12*, 1280–1296.

Ariel, Barak, and Tony Farrar. 2013. Self-Awareness to Being Watched and Socially-Desirable Behavior: A Field Experiment on the Effect of Body-Worn Cameras on Police Use-of-Force. Washington D.C.: Police Foundation. Accessed February 20, 2015, http://www.policefoundation.org/content/body-worn-camera.

Ariel, Barak, Tony Farrar, and Alex Sutherland. 2014. The Effect of Police Body-Worn Cameras on Use of Force and Citizens' Complaints against the Police: A Randomized Controlled Trial. *Journal of Quantitative Criminology*. Prepublished November 19, 2014, DOI: 10.1007/s10940-014-9236-3.

Arizona Revised Statutes § 28-7751 (West, 2015).

Arizona v. Johnson, 555 U.S. 323 (2009).

Arkansas Code § 12-12-1801, et seq. (West, 2015).

Baile, Noam. 2008. Report: "Expert Findings on Surveillance Cameras: What Criminologists and Others Studying Cameras Have Found." American Civil Liberties Union, ACLU Technology and Liberty Program.

Baker, C. Edwin. (1978). The Scope of First Amendment Freedom of Speech. *UCLA Law Review, 25*, 964-1040.

Baker, C. Edwin. 1989. *Human Liberty and Freedom of Speech*. Oxford Univ. Press.

Balkin, Jack M. 2004. Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society. *New York University Law Review*, 79, 1-__.

Balkin, Jack M. 2009. The Future of Free Expression in a Digital Age. *Pepperdine Law Review, 36*, 707.

Balkin, Jack M. 2012. Room for Maneuver: Julie Cohen's Theory of Freedom in the Information State. *Jerusalem Review of Legal Studies, 6*(1), 79–95.

Balkin, Jack M. 2013. The First Amendment is an Information Policy. *Hofstra Law Review, 41*, 101-130.

Ball, Kirstie. 2003. Categorizing the Workers: Electronic Surveillance and Social Ordering in the Call Center. In David Lyon (ed.), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, 201-225. London; New York: Routledge.

Baltimore Police Department. Policy. http://www.aclu-md.org/uploaded_files/0000/0487/bpd_policy.pdf.

Bannister, Frank. 2005. The Panoptic State: Privacy, Surveillance and the Balance of Risk. *Information Polity, 10*, 65-78.

Bellevue John Does 1-11 v. Bellevue School Dist. #405, 164 Wash.2d 199 (Wash. 2008).

Benkler, Yochai. 1998. "The commons as a neglected factor of information policy." Paper presented at the 26th Annual Telecommunications Research Conference, Arlington, VA. Available at http://www.benkler.org/commons.pdf.

Bennett, Colin, Charles Raab, and Priscilla Regan. 2003. People and Place: Patterns of Individual Identification within Intelligent Transportation Systems. In David Lyon (ed.), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, 153-175. London; New York: Routledge.

Berger v. United States, 388 U.S. 41 (1967).

Berlin, Isaiah. 1969. Two Concepts of Liberty. In Henry Hardy (ed.), *Isaiah Berlin: Liberty: Incorporating Four Essays on Liberty*. Oxford: Oxford University Press, 2002.

Bernhard v. City of Ontario, 270 Fed.Appx. 518 (9th Cir. 2008) (unpublished).

Bibring, Peter, Yaman Salahi, and Jennifer Lynch. 2013. "Verified Petition for Peremptory Writ of Mandate," May 6, 2013, Sup. Ct of Cal. Los Angeles, in American Civil Liberties Union of Southern California, et al, v. Los Angeles Police Department, et al., available at https://www.eff.org/files/filenode/pet.sup_.verified_petition_for_writ_050613.pdf.

Bittner, Egon. 1990. *Aspects of Police Work*. Boston: Northeastern University Press.

Blackston v. Alabama, 30 F.3d 117 (11th Cir. 1994).

Blanton, Tom. 2011. A Humble Forward. In David Cuillier and Charles N. Davis, *The Art of Access: Strategies for Acquiring Public Records*. Washington D.C.: CQ Press).

Blasi, Vincent. 1977. The Checking Value in First Amendment Theory. *Law & Social Inquiry, 2(3)*, 521-649.

Blitz, Marc J. 2009. *The Where and Why of Intellectual Privacy. Texas Law Review, 87,* 15-23.

Blumenthal, Jeremy A., Meera Adya, and Jacqueline Mogle. 2009. The Multiple Dimensions of Privacy: Testing Lay 'Expectations of Privacy'. *University of Pennsylvania Journal of Constitutional Law, 11*, 311-374.

Bowens v. Superintendant of Miami South Beach Police Dept., 557 Fed.Appx. 857 (11th Cir. 2014).

Boyd v. United States, 116 U.S. 616 (1886).

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

Braman, Sandra. 2011. Defining Information Policy. *Journal of Information Policy*, *1*(1), 1-5.

Brannum v. Overton County School Board, 516 F.2d 489 (6th Cir. 2008).

Brin, David. 1998. *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* New York: Perseus Books.

Brink v. Griffith, 65 Wash. 2d 253 (Wash. 1964).

Broadwater, Luke. 2014. "New city police policy says public has right to film officers." The Baltimore Sun, March 12, 2014. http://articles.baltimoresun.com/2014-03-12/news/bs-md-ci-aclu-recording-settlement-20140312_1_police-officers-police-actions-christopher-sharp.

Bruce, David, and Sean Tait. 2015. "A 'Third Umpire' for Policing in South Africa: Applying Body Cameras in the Western Cape." Strategic Paper 14 (March 2015). Igarapé Institute.

Buckland, Michael. 1991. Information as Thing. *Journal of the American Society of Information Science, 42*(5), 351-60.

Building Industry Ass'n of Washington v. State Dept. of Labor & Industries, 123 Wash.App. 656 (2004).

California Penal Code § 632 (West, 2015).

California v. Ciraolo, 476 U.S. 207 (1986).

California Vehicle Code § 2413 (West, 2015).

Calo, M. Ryan. 2011. The Boundaries of Privacy Harm. *Indiana Law Journal, 86,* 1131-1162.

Calo, M. Ryan. 2012. Against Notice Skepticism in Privacy (and Elsewhere). *Notre Dame Law Review, 87,* 1027-1072.

Cape Publications, Inc. v. Bridges, 423 So. 2d 426 (Fla. Dist. Ct. App. 1982).

Carson, Bryan M. 2010. The Legal Basis for Library Video Surveillance. *Against the Grain, 22*(5), 52-54.

CBS News. 2009. "Cops Arrest Priest For Filming Them." *CBS News*, March 13, 2009, http://www.cbsnews.com/ news/cops-arrest-priest-for-filming-them.

Chander, Anupam, and Madhavi Sunder. 2012. Foreword: Occupying Our Hearts. *UC Davis Law Review, 45*, 1585- 1607.

Chermak, Steven, and Alexander Weiss. 2005. Maintaining Legitimacy Using External Communication Strategies: An Analysis of Police–Media Relations. *Journal of Criminal Justice, 33*, 501–12.

Chynoweth, Paul. 2008. Legal Research. Chapter 3 in *Advanced Research Methods in the Built Environment*. Ch. 3 in Knight, A. and Ruddock, L. (eds.), Wiley-Blackwell.

CIA v. Sims, 471 U.S. 159 (1985).

City of Lakewood v. Koenig, 2014 WL 7003790 (Wash. 2014).

City of Seattle v. McCready 123 Wash.2d 260 (Wash. 1994).

Clapper v. Amnesty International USA, 133 S.Ct. 1138 (2013).

Clune, Bronwen. 2013. "Digital Vigilantism: Think Before Putting Pictures of 'Wrongdoing' Online." *The Guardian*, November 28, 2013, http://www.theguardian.com/commentisfree/2013/nov/29/digital-vigilantism-think-before-pictures-of-wrongdoing-online.

Cohen, Julie E. 2012. *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. New Haven: Yale University Press.

Cohen, Julie E. 2013. What Privacy Is For. *Harvard Law Review, 126*, 1904-1933.

Cohen, Stanley. 1985. *Visions of Social Control: Crime, Punishment and Classification*. Cambridge: Polity.

Coin, Glenn. 2013. "NY Safe Act Requires Onondaga County to Release Many Pistol Permit Holders' Names, State Official Says." *Syracuse.com* (Aug. 13, 2013), http://www.syracuse.com/news/index.ssf/2013/08/onondaga_county_must_release_pistol_permit_holders_names_addresses_says_state_op.html.

Colorado Revised Statutes § 24-72-113, "Limit on retention of passive surveillance records—definition." Adopted April 4, 2014.

Columbia Basin Apartment Ass'n v. City of Pasco, 268 F.3d 791 (9th Cir. 2001).

Corey v. Pierce County, 154 Wash. App. 752 (Div. 1 2010).

Coultrup, S. and P.D. Fountain. 2012. Effects of Electronic Monitoring and Surveillance on the Psychological Contract of Employees: An Exploratory Study. *Proceedings of the American Society of Business and Behavioral Sciences, 19*(1), 219-35.

Cowles Pub. Co. v. Spokane Police Department, 139 Wash.2d 472 (Wash. 1999).

Crump, Catherine. "You Are Being Tracked: How License Plate Readers are Being Used to Record Americans' Movements." American Civil Liberties Union. July 2013, at 3. https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf.

Cuccinelli, Kenneth T. 2013. Virginia Opinion of the Attorney General, Opinion No. 12-073, 2013 WL 653025 (Feb. 13, 2013).

Czeskis, Alexei, Ivayla Dermendjieva, Hussein Yapit, Alan Borning, Batya Friedman, Brian Gill, and Tadayoshi Kohno. 2010. Parenting from the pocket: Value tensions and technical directions for secure and private parent-teen mobile safety. *Proceedings of SOUPS 2010.* New York: ACM Press.

Davis, Frederick. 1959. What Do We Mean by 'Right to Privacy'? *South Dakota Law Review, 4*, 1-24.

Dawes, Sharon S. 2010. Stewardship and usefulness: Policy principles for information-based transparency. *Government Information Quarterly, 27*, 377–383.

Dawes, Sharon S., and Natalie Helbig. 2010. Information Strategies for Open Government: Challenges and Prospects for Deriving Public Value from Government Transparency. In M.

A. Wimmer et al. (eds.), *Electronic Government 2010: Lecture Notes in Computer Science*, LNCS 6228, 50-60.

DeGregorio v. CBS, Inc., 473 N.Y.S.2d 922 (N.Y. Sup. Ct. 1984).

Delaware Code Title 11 § 1335(a) (West, 2015).

Denham, Elizabeth. 2012. "Investigation Report F12-04: Use of Automated Licence Plate Recognition Technology by the Victoria Police Department 10-11." Office of Information & Privacy Commissioner of British Columbia. November, 15, 2012). http://www.oipc.bc.ca/investigation-reports/1480.

Dickman, Bethany L. 2011. Note: Untying Knotts: The Application of Mosaic Theory to GPS Surveillance in United States v. Maynard. *American University Law Review, 60*, 731-.

DMLP [Digital Media Law Project]. Legal Guide. Digital Media Law Project. http://www.dmlp.org/legal-guide/.

Doe v. Dearborn Public Schools, Case No. 06-CV-12369-DT, E.D. Mich., March 31, 2008 (unpublished).

Doe v. Gonzaga University, 143 Wash. 2d 687 (2001), *judgment rev'd on other grounds*, 536 U.S. 273 (2002).

Doe v. Gonzaga University, 143 Wash.2d 687 (2001), *reversed on other grounds*, 536 U.S. 273 (2002).

Dow Chemical Co. v. United States, 476 U.S. 227 (1986).

Dow, Paula T. 2010. Directive No. 2010-5: Law Enforcement Directive Promulgating Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data (Dec. 3, 2010), *available at* http://www.state.nj.us/oag/dcj/agguide/directives/Dir-2010-5-LicensePlateReadersl-120310.pdf.

Dow, Paula T. 2013. Va. Op. Att'y Gen., Opinion No. 12-073, 2013 WL 653025 (Feb. 13, 2013).

Draisin, Lilian. 2011. *Police Technology: An Analysis of In-Car Cameras and Body Worn Cameras*. Orlando: University of Central Florida.

Driver Privacy Protection Act, 18 USC §§ 2721-2725 (West, 2015).

Dunne, Anthony, and Fiona Raby. 2001. *Design Noir: The Secret Life of Electronic Objects*. Boston; Berlin: Birkhauser.

Eastwood v. Cascade Broadcasting Co., 106 Wash. 2d 466 (1986).

EFF [Electronic Frontier Foundation]. "Bloggers' Rights." Electronic Frontier Foundation, https://www.eff.org/bloggers (last visited Jan. 21, 2014).

Eikenberry, Kenneth O., and Nancy Thygesen Day. 1988. *Recording Conversations—Emergencies—Central Dispatch*. Op. Wash. Att'y Gen. No. 11 (1988), 1988 WL 404817 (May 20, 1988).

Etzioni, Amitai. 2014. A Cyber Age Privacy Doctrine: A Liberal Communitarian Approach. *I/S: A Journal of Law and Policy for the Information Society*, 10(2), 641-669.

European Commission. 2014. Factsheet on the "Right to Be Forgotten" ruling (C-131/12). http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.

Federated Univ. Police Officers Ass'n v. Superior Court, 159 Cal. Rptr. 3d 541, 543 (Cal. Ct. App. 2013)

Fenton, Justin. 2013. "Claim: Woman Arrested, Camera Destroyed After Recording Baltimore Police." *Baltimore Sun*, May 15, 2013, http://articles.baltimoresun.com/2013-05-15/news/bal-claim-woman-arrested-camera-destroyed-after-recording-baltimore-police-20130515_1_christopher-sharp-camera-phone-wbal-tv.

Ferguson, Bob. 2014. *Video And Audio Recording Of Communications Between Citizens And Law Enforcement Officers Using Body Cameras Attached To Police Uniforms*. Op. Wash. Att'y Gen. No. 8 (2014), 2014 WL 6711950 (November 24, 2014).

Fink, Zera Silver. 1945. *The Classical Republicans: An Essay in The Recovery of a Pattern of Thought in Seventeenth Century England*. Evanston, IL: Northwestern University Press.

First National Bank of Boston v. Bellotti, 435 U.S. 765 (1978).

Fisher Broadcasting-Seattle TV LLC v. City of Seattle, 180 Wash.2d 515 (Wash. 2014).

Fisher v. State ex rel. Dept. of Health, 125 Wash. App. 869 (Wash. Div. 3, 2005).

Fleck v. Trustees of University of Pennsylvania, 995 F.Supp.2d 390 (E.D.Pa., 2014).

Florida Statutes § 316.0777 (West, 2015).

Florida Statutes § 934.03 (West, 2015).

Florida v. Jardines, 133 S.Ct. 1409 (2013).

Florida v. Riley, 488 U.S. 445 (1989).

Floyd v. City of New York, 959 F.Supp.2d 540 (S.D.N.Y. 2013), *vacated in part by* Ligon v. City of New York, 743 F.3d 362 (2nd Cir. 2014).

Floyd v. City of New York, 959 F.Supp.2d 668 (S.D.N.Y. 2013), *vacated in part by* Ligon v. City of New York, 743 F.3d 362 (2nd Cir. 2014).

Forcese, Craig, and Aaron Freeman. 2005. *The Laws of Government: The Legal Foundations of Canadian Democracy*. Toronto, Canada: Irwin Law.

Fordyce v. City of Seattle, 55 F.3d 436 (9th Cir. 1995).

Foucault, Michel. 1975. *Discipline & Punish: The Birth of the Prison*. Translation (1977) by Alan Sheridan. New York: Vintage Books (2nd ed.), 1995.

Franklin, Neill. 2013. "Cameras Could Restore Trust in Police." *New York Times*, Room for Debate, Oct. 22, 2013, at http://www.nytimes.com/roomfordebate/2013/10/22/should-police-wear-cameras/body-cameras-could-restore-trust-in-police.

Freedom Found. v. Gregoire, 178 Wash.2d 686 (Wash. 2013).

Freedom of Information and Protection of Privacy Act. Revised Statutes of British Columbia (Canada) 1996, Chapter 165 (current through February 25, 2015). http://www.bclaws.ca/Recon/document/ID/freeside/96165_00.

Friedman, Batya (ed.). 1997. *Human Values and the Design of Computer Technology*. Cambridge University Press and CSLI New York Stanford University.

Friedman, Batya, and Helen Nissenbaum. 1995. Minimizing bias in computer systems. *Conference Companion of CHI 1995 Conference on Human Factors in Computing Systems*, 444. New York: ACM Press.

Friedman, Batya, and Helen Nissenbaum. 1996. Bias in computer systems. *ACM Transactions on Information Systems, 14*(3), 330-347.

Friedman, Batya, and Helen Nissenbaum. 1997. Software agents and user autonomy. *Proceedings of First International Conference on Autonomous Agents*, 466-469. New York: ACM Press.

Friedman, Batya, and Peter H. Kahn, Jr. 2003. Human values, ethics, & design. In Jacko, J., Sears, A. (eds.), *Handbook of human-computer interaction*, pp. 1177-1201. Mahwah, NJ: Lawrence Erlbaum Associates.

Friedman, Batya, Ian Smith, Peter H. Kahn, Jr., Sunny Consolvo, and Jaina Selawski. 2006. Development of a privacy addendum for open source licenses: Value Sensitive Design in industry. *Proceedings of 2006 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp 2006)*, 194-211. Berlin, Heidelberg; New York: Springer-Verlag.

Friedman, Batya, Peter H. Kahn, Jr., and Alan Borning, A. 2006. Value Sensitive Design and Information Systems. In P. Zhang and D. Galletta (Eds.), *Human-Computer Interaction in Management Information Systems: Foundations*. M.E. Sharpe, Inc.: New York, NY.

Friedman, Batya. 1996. Value-sensitive design. *ACM interactions*, 3(6), 17-23.

Gambino, Lauren. 2014. Staten Island man dies after NYPD officers put him in chokehold, The Guardian, July 18, 2014, at http://www.theguardian.com/world/2014/jul/18/staten-island-man-dies-nypd-chokehold.

Ganascia, Jean-Gabriel. 2011. The Generalized Sousveillance Society. *Social Science Information, 49*, 489-507.

Gaumont, Norm. 2008. The Role of Automatic License Plate Recognition Technology in Policing: Results from the Lower Mainland of British Columbia. *The Police Chief, 75*(11) (Nov. 2008). http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=1671.

Gericke v. Begin, 753 F.3d 1 (1st Cir. 2014).

Gerring, John. 2006. Single-Outcome Studies A Methodological Primer. *International Sociology, 21*(5), 707–734.

Gill, Martin, and Angela Spriggs. 2005. "Home Office Research Study 292: Assessing the Impact of CCTV." Home Office Study, February 2005.

Gillan and Quinton v. The United Kingdom, (2010) 50 E.H.R.R. 45 (ECtHR, 2010).

Glik v. Cunniffe, 655 F.3d 78 (1st Cir. 2011).

Goffman, E. 1971. Relations in Public: Microstudies of the Public Order. New York: Basic Books.

Goffman, Erving. 1990. The Presentation of Self in Everyday Life. London: Penguin.

Goldsmith, Andrew John. 2010. Policing's New Visibility. *British Journal of Criminology, 50*, 914-934.

Goldstein, Joseph, and Nate Schweber. 2014. "Man's Death After Chokehold Raises Old Issue for the Police." *New York Times*, July 18, 2014, http://www.nytimes.com/2014/07/19/nyregion/staten-island-man-dies-after-he-is-put-in-chokehold-during-arrest.html.

Gonzalez, Juan. 2012. "George Holliday, the Man with the Camera Who Shot Rodney Kind While Police Beat Him, Got Burned, Too." *New York Daily News*, June 19, 2012,

http://www.nydailynews.com/news/national/george-holliday-man-camera-shot-rodney-king-police-beat-burned-article-1.1098931.

Goodall, Martin. 2007. *Guidance for the Police Use of Body-Worn Video Devices*. Police and Crime Standards Directorate. London, England: Home Office.

Goodman, J. David, and Al Baker. 2014. "Wave of Protests After Grand Jury Doesn't Indict Officer in Eric Garner Chokehold Case." New York Times, December 3, 2014, http://www.nytimes.com/2014/12/04/nyregion/grand-jury-said-to-bring-no-charges-in-staten-island-chokehold-death-of-eric-garner.html.

Google Spain SL, v Agencia Espanola de Proteccion de Datos (AEPD), Mario Costeja Gonzalez, [2013] EUECJ C-131/12 (2013).

Goold, Benjamin J. 2002. Privacy Rights and Public Spaces: CCTV and the Problem of the 'Unobservable Observer'. *Criminal Justice Ethics, 21*, 21-27.

Greenawalt, Kent. 1995. Rationales for Freedom of Speech. In Adam D. Moore (ed.), *Information Ethics: Privacy, Property, and Power*. Seattle, Wash.: University of Washington Press, 2005.

Greer, Chris, and Eugene McLaughlin. 2010. We Predict a Riot?: Public Order Policing, New Media Environments and the Rise of the Citizen Journalist. *British Journal of Criminology, 50*, 1041–1059.

Grenville, Andrew. 2010. Shunning Surveillance or Welcoming the Watcher? Exploring How People Traverse the Path of Resistance. In Elia Zureik (ed.), *Surveillance, Privacy, and the Globalization of Personal Information*. McGill-Queen's University Press.

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

Gross, Hyman. 1967. The Concept of Privacy. *NYU Law Review*, *42*, 34-54.

Gurnon, Emily. 2013. "Little Canada Man Must Stand Trial in Videotaping of Ambulance Crew." *TwinCities.com*, Aug. 20, 2013, http://www.twincities.com/crime/ci_23902450/little-canada-man-who-videotaped-medical-call-will.

Haggerty, Kevin D. 2006. Tear Down the Walls: On Demolishing the Panopticon. In David Lyon (ed.), *Theorizing Surveillance: The Panopticon and Beyond*. Cullompton, UK: Willan Publishing.

Haggerty, Kevin D., and Richard V. Ericson. 2000. The Surveillant Assemblage. *British Journal of Sociology, 51*(4), 605-622.

Haggerty, Kevin D., and Richard V. Ericson. 2006. The New Politics of Surveillance and Visibility. In K.D. Haggerty and R.V. Ericson (eds.), *The New Politics of Surveillance and Visibility*, pp. 3-25. Toronto, Canada: University of Toronto Press.

Hartzog, Woodrow, and Frederic Stutzman. 2013. Obscurity by Design. *Washington Law Review, 88*, 385-418.

Hartzog, Woodrow, and Frederic Stutzman. 2013. The Case for Online Obscurity. *California Law Review, 101*(1), 1-49.

Hearst Corp. v. Hoppe, 90 Wash. 2d 123 (Wash. 1978).

Heien v. North Carolina, 135 S.Ct. 530 (2014).

Henderson, Stephen E. 2013. After United States v. Jones, After The Fourth Amendment Third Party Doctrine. *North Carolina Journal of Law and Technology, 14*(2), 431-459.

Herbert, Steve. 1998. Police Subculture Reconsidered. *Criminology*, *36*, 343–370.

Herbert, Steve. 2006a. *Citizens, Cops, and Power*. Chicago; London: The University of Chicago Press.

Herbert, Steve. 2006b. Tangled Up in Blue: The Elusive Quest for Police Legitimacy. *Theoretical Criminology*, *10*(4), 481-504.

Hernandez-Lopez v. State, 738 S.E.2d 116 (Ga. Ct. App. 2013).

Hoffa v. United States, 385 U.S. 293 (1966).

Hutchinson, Terry C., and Nigel Duncan. 2012. Defining and describing what we do: doctrinal legal research. *Deakin Law Review*, *17*(1), 83-119.

Iacobucci v. Boulter, No. CIV.A. 94-10531, 1997 WL 258494 (D.Mass, Mar. 26, 1997) (unpublished opinion).

IACP [International Association of Chiefs of Police]. 2003. Impact of video enhancement on modern policing. Alexandria, VA: International Association of Chiefs of Police.

IACP [International Association of Chiefs of Police]. 2004. Impact of video enhancement on modern policing: Research and best practices from the IACP study on in-car cameras. Alexandria, VA: International Association of Chiefs of Police.

IACP [International Association of Chiefs of Police]. 2005. *The Impact of Video Evidence on Modern Policing*, 2005 IACP In-Car Camera Report. Alexandria, VA: International Association of Chiefs of Police. https://www.theiacp.org/LinkClick.aspx?fileticket=5k3IK9SZuz4%3d&tabid=340.

Igarapé Institute. "Smart Policing." http://en.igarape.org.br/smart-policing/.

Illinois Compiled Statutes. 720 ILCS §§ 5/14-1, -2, -4 (West, 2015).

In re Marriage of Farr, 87 Wash.App. 177 (Wash. App. 1997).

In re Request of Rosier 105 Wash.2d 606 (Wash. 1986).

Initiative Measure No. 276, ch. 1, 1973 Wash. Sess. Laws 1, 31 (1972).

Jaeger, Paul T. 2007. Information policy, information access, and democratic participation: The national and international implications of the bush administration's information policies. *Government Information Quarterly, 24*, 840−859.

Jaeger, Paul T., and Gary Burnett. 2005. Information access and exchange among small worlds in a democratic society: The role of policy in redefining information behavior in the post-9/11 United States. *Library Quarterly*, *75*(4), 464−495.

Jaeger, Paul T., and John Carlo Bertot. 2005. Transparency and technological change: Ensuring equal and sustained public access to government information. *Government Information Quarterly*, *27*, 371-376.

Jennings, Wesley G., Lorie A. Fridell, and Mathew D. Lynch. 2014. Cops and cameras: Officer perceptions of the use of body-worn cameras in law enforcement. *Journal of Criminal Justice* 42(6), 549–556.

Johns-Byrne Co. v. TechnoBuffalo, LLC, "Order on Motion for Reconsideration," No. 2011 L 009161 (Ill. Cir. Ct. 2012), *available at* http://www.dmlp.org/sites/citmedialaw.org/files/2012-07-13-Order%20on%20motion%20for%20reconsideration.pdf.

Johnson v. Hawe, 388 F.3d 676 (9th Cir. 2004).

Johnston, Anna, and Myra Cheng. 2002. Electronic Surveillance in the Workplace: Concerns for Employees and Challenges for Privacy Advocates. Paper delivered at the *International Conference on Personal Data Protection*, November 28, 2002, Seoul, Korea.

Johri, Aditya, and Sumitra Nair. 2011. The Role of Design Values in Information System Development for Human Benefit. *Information Technology & People*, *24*(3), 281-302.

Kadoranian v. Bellingham Police Dep't, 119 Wash.2d 178, 190 (1992).

Kalaf, Samer. 2012. "Hackers Take Over Steubenville High School Football Team's Website, Threaten to Release Personal Information of People Involved in Alleged Rape Case." *Deadspin*, Dec. 25, 2012, http://deadspin.com/hackers-take-over-steubenville-high-school-football-tea-5971165.

Kansas Statutes § 21-4001 (West, 2015).

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

Katz, Charles, and Mike Kurtenbach. 2014. "Deploying Officer Body-Worn Cameras in Phoenix." *Office of Justice Programs Diagnostic Center*, August 6, 2014, https://www.ojpdiagnosticcenter.org/blog/deploying-officer-body-worn-cameras-phoenix.

Kearney v. Kearney, 95 Wash.App. 405 (Wash. App. 1999), *review denied*, 138 Wash.2d 1022.

Kelly v. Borough of Carlisle, 622 F.3d 248 (3rd Cir. 2010).

Kerr, Orin. 2005. Searches and Seizures in a Digital World. *Harvard Law Review, 119*, 531-585.

Kerr, Orin. 2009. The Case for the Third-Party Doctrine. *Michigan Law Review, 107*, 561-601.

Kerr, Orin. 2012. The Mosaic Theory of the Fourth Amendment. *Michigan Law Review, 111*, 311-354.

Khouri, Andrew. 2013. "N.Y. Newspaper Removes Online Map of Gun-permit Holders." *L.A. Times*, Jan. 20, 2013, http://articles.latimes.com/2013/jan/20/nation/la-na-nn-new-york-newspaper-gun-permits-map-offline-20130119.

Kilgore, Vickie. 2012. "Washington: The story behind the score." *StateIntegrity.org*. http://www.stateintegrity.org/washington_story_subpage.

King v. City of Indianapolis, 969 F.Supp.2d 1085 (S.D. Ind., 2013).

Klontz, Joshua C., and Anil K. Jain. 2013a. A Case Study on Unconstrained Facial Recognition Using the Boston Marathon Bombings Suspects. Technical Report MSU-CSE-13-4 May 22, 2013, http://www.nec.com/en/global/solutions/safety/pdf/MSU_Case_Study_on_Face_Recognition.pdf.

Klontz, Joshua C., and Anil K. Jain. 2013b. A Case Study on Unconstrained Facial Recognition Using the Boston Marathon Bombings Suspects. *Computer, 46*(11), 91-94. IEEE. DOI: 10.1109/MC.2013.377.

Koenig v. City of Des Moines, 158 Wn.2d 173 (Wash. 2006).

Kohn, Margaret. 2010. Unblinking: Citizens and Subjects in the Age of Video Surveillance. *Constellations, 17*, 572 (2010).

Kopan, Tal. 2013. "Another Lawsuit Filed Over Police Recording." *Politico*, Jan 17, 2013, http://www.politico.com/blogs/under-the-radar/2013/01/another-lawsuit-filed-over-police-recording-154488.html;

Kreimer, Seth F. 2011. Pervasive Image Capture and the First Amendment: Memory, Discourse, and the Right to Record. *University of Pennsylvania Law Review, 159*, 335-409.

Krim, Jonathan. 2005. "Subway Fracas Escalates Into Test of the Internet's Power to Shame." *Washington Post*, July 7, 2005, http://www.washingtonpost.com/wpdyn/content/article/2005/07/06/ AR20050706-01953.html.

La Vigne, Nancy. 2013. "It's One Smart Step, Not a Solution." *New York Times*, Room for Debate, Oct. 23, 2013, at http://www.nytimes.com/roomfordebate/2013/10/22/should-police-wear-cameras/body-cameras-for-police-could-be-one-smart-step.

Lambert v. Polk County, 723 F.Supp. 128 (S.D.Iowa, 1989).

Lautt, Steven A. 2012. Note: Sunlight is Still the Best Disinfectant: The Case for a First Amendment Right to Record the Police. *Washburn Law Journal, 51*, 349-381.

Lee, Eunice. 2012. "N.J. ACLU Unveils 'Stealth' App Allowing Citizens to Secretly Record Police." *New Jersey Online*, July 3, 2012, http://www.nj.com/news/index.ssf/2012-/07/nj_aclu_unveils_stealth_app_al.html.

Leman-Langlois, S. 2008. Afterword. In S. Leman-Langlois (ed.), *Technocrime: Technology, Crime and Social Control*, pp. 243-46. Portland, OR: Willan.

Leslie, Gregg. 2009. Who Is a 'Journalist?' And Why Does It Matter? *News Media & Law*, Fall 2009, p. 4.

Lewis v. State, Dept. of Licensing 157 Wash.2d 446 (Wash. 2006).

Lewis, Paul. 2009. "Ian Tomlinson Death: Guardian Video Reveals Police Attack on Man who Died at G20 Protest." *The Guardian*, April 8, 2009, www.theguardian.com/uk/2009/apr/07/ian-tomlinson-g20-death-video.

Lichtenberg, Illya D., and Alisa Smith. 2001. How dangerous are routine police–citizen traffic stops? A research note. *Journal of Criminal Justice, 29*, 419– 428.

Lithwick, Dahlia. 2012. "Police Tape: Is Chicago really planning on detaining anyone who records protestor arrests at the G-8 summit?" *Slate*, January 31, 2012, http://www.slate.com/articles/news_and_politics/jurisprudence/2012/01/recording_police_making_arrests_the_outrageous_illinois_law_that_makes_it_a_felony_.single.html.

Lomell, Heidi Mork. 2004. Targeting the Unwanted: Video Surveillance and Categorical Exclusion in Oslo, Norway. *Surveillance & Society, 2*(2/3), 346-360.

Lovett, Frank, and Philip Pettit. 2009. Neorepublicanism: A Normative and Institutional Research Program. *Annual Review of Political Science, 12*, 11-30.

Lovett, Frank. 2013. Republicanism. *The Stanford Encyclopedia of Philosophy*, Spring 2013 Edition, Edward N. Zalta (ed.), at http://plato.stanford.edu/archives/spr2013/entries/republicanism/.

Lucia, Bill. 2014. "Massive public records requests cause police to hit pause on body cam programs." *Crosscut*, November 10, 2014, http://crosscut.com/2014/11/body-cams-washington-seattle-privacy-disclosure/.

Lyon, David (ed.). 2003. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London; New York: Routledge.

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

Lyon, David. 2006. The Search for Surveillance Theories. In David Lyon (ed.), *Theorizing Surveillance: The Panopticon and Beyond*. Cullompten, UK: Willan Publishing.

Lyon, David. 2007. *Surveillance Studies: An Overview*. Cambridge, UK: Polity Press.

MacAskill, Ewen. 2010. "Oakland Riots After Verdict in Police Shooting of Oscar Grant." *The Guardian*, July 9, 2010, htttp://www.theguardian.com/world/2010/jul/09/oakland-riots-oscar-grant-shooting-verdict.

Madrigal, Alexis C. 2013. "Hey Reddit, Enough Boston Bombing Vigilantism." *The Atlantic*, April 17, 2013, http://www.theatlantic.com/technology/archive/2013/04/hey-reddit-enough-boston-bombing-vigilantism/275062/.

Maine Revised Statues, Title 29-A §§ 2117, 2117-A (West, 2015).

Mann, Steve, and Joseph Ferenbok. 2013. New Media and the Power Politics of Sousveillance in a Surveillance Dominated World. *Surveillance & Society*, 11(1/2), 18-34.

Mann, Steve, Jason Nolan, and Barry Wellman. 2003. Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. *Surveillance & Society, 1*, 331-355.

Mann, Trischa, and Audrey Blunden. (eds.). 2010. *Australian Law Dictionary*. Oxford University Press.

Marchionini, Gary. 2008. Human–information interaction research and development. *Library & Information Science Research, 30*(3), 165-174.

Martin v. Riverside School Dist. No. 416, 180 Wash.App. 28 (2014).

Marx, Gary T. 1988. *Undercover: Police Surveillance in America*. Berkeley/Los Angeles: University of California Press.

Marx, Gary T. 2003. A Tack in the Shoe: Neutralizing and Resisting the New Surveillance. *The Journal of Social Issues*, 59(2), 369-390.

Marx, Gary T. 2005. Surveillance and Society. In G. Ritzer (ed.), *Encyclopedia of Social Theory*. Thousand Oaks, CA: SAGE Publications.

Maryland Code, Courts & Judicial Process §10-402 (West, 2015).

Maryland Code, General Provisions § 4-236 (West, 2015).

Maryland Code, Public Safety § 3.509 (West, 2015).

Maryland Code, Transportation § 25-113 (West, 2015).

Massachusetts General Laws, Ch. 272 § 99 (West, 2015).

Mathiesen, Thomas. 1997. The Viewer Society: Michel Foucault's 'Panopticon' Revisited. *Theoretical Criminology, 1*(2), 215-34.

Mawby, Rob C. 2002. *Policing Images: Policing, Communication and Legitimacy*. Cullompton: Willan.

Mayer v. Huesner, 126 Wash. App. 114 (Wash. Div. 3, 2005).

MCAC [Maryland Coordination and Analysis Center]. "About the Maryland Coordination and Analysis Center." http://www.mcac.maryland.gov/about_mcac/.

McCahill, Michael. 2002. *The Surveillance Web: The Rise of Visual Surveillance in an English City*. Pertland, OR: Willan Publishing.

McCarthy v. Barrett, 804 F.Supp.2d 1126 (W.D.Wash. 2011).

McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995).

McKay v. Federspeil, 22 F.Supp.3d 731 (E.D.Mich. 2014).

McKinley, Jesse. 2010. "Officer Guilty in Killing That Inflamed Oakland." *New York Times*, July 8, 2010, http://www.nytimes.com/2010/07/09/us/09verdict.html.

McLenan-Kenny v. Washington Dept. of Labor and Industries, 2014 WL 1648501 (W.D.Wash. Apr 24, 2014).

McNulty, Tony, and Patricia Scotland. 2007. Foreward. In Martin Goodall, *Guidance for the Police Use of Body-Worn Video Devices*, p. 5. Police and Crime Standards Directorate. London, England: Home Office.

Meiklejohn, Alexander. 1948. *Free Speech and its Relation to Self-Government*. New York: Harper.

Meiklejohn, Alexander. 1960. *Political Freedom; the Constitutional Powers of the People*. New York: Harper.

Meiklejohn, Alexander. 1961. The First Amendment is an Absolute. *Supreme Court Review, 1961*, 245-266.

Michigan Compiled Laws § 750.539c-d (West, 2015).

Mill, John Stuart. 1859. *On Liberty*. Mineola, NY: Dover, 2002.

Miller, Jessica K., Batya Friedman, Gavin Jancke, and Brian Gill. 2007. Value tensions in design: The value sensitive design, development, and appropriation of a corporation's groupware system. *Proceedings of GROUP 2007*, 281-290. New York: ACM Press.

Miller, Kevin. 2014. Total Surveillance, Big Data, and Predictive Crime Technology: Privacy's Perfect Storm. *Journal of Technology Law & Policy, 19*, 105-146.

Miller, Lindsay, and Jessica Toliver. 2014. "Implementing a Body-Worn Camera Program: Recommendations and Lessons Learned." Police Executive Research Forum. Washington, DC: Office of Community Oriented Policing Services.

Minnesota Department of Administration. 2014. "Current Temporary Classifications." Minnesota Department of Administration, Information & Analysis Division. http://www.ipad.state.mn.us/docs/tccurrent.html.

Mocek v. City of Albuquerque, 2013 WL 312881 (D.N.M., 2013) (not reported).

Mocek v. City of Albuquerque, 3 F.Supp.3d 1002 (D.N.M., 2014).

Monahan, Torin. 2006. Counter-surveillance as Political Intervention? *Social Semiotics, 16*, 515–534.

Montana Code § 45-8-213(1)(c) (West, 2015).

Moore, Adam D. 2000. Employee Monitoring and Computer Technology: Evaluative Surveillance v. Privacy. *Business Ethics Quarterly,* 10(3), 697-709.

Moore, Adam D. 2005. Intangible Property: Privacy, Power, and Information Control. In Adam D. Moore (ed.), *Information Ethics: Privacy, Property, and Power*. Seattle, WA: University of Washington Press.

Moore, Adam D. 2007. Toward Informational Privacy Rights. *San Diego Law Review*, 44, 809-845.

Moore, Adam D. 2010. *Privacy Rights: Moral and Legal Foundations*. University Park, PA: Pennsylvania State University Press.

Moore, Adam D. 2013. Privacy, Speech, and the Law. *Journal of Information Ethics, 22(1)*, 21-43.

Moore, Adam D., and Kristene Unsworth. 2005. Introduction. In Adam D. Moore (ed.), *Information Ethics: Privacy, Property, and Power*. Seattle, WA: University of Washington Press.

Moos, Julie. 2013. "Newspaper Publishes Names, Addresses of Gun Owners." *Poynter.org*, http://www.poynter.org/latest-news/mediawire/199148/newspaper-publishes-names-addresses-of-gun-owners (last updated Jan. 7, 2013).

Munson, Sean A., Daniel Avrahami, Sunny Consolvo, James Fogarty, Batya Friedman, and Ian Smith. 2011. Attitudes toward Online Availability of US Public Records. *Proceedings of dg.o 2011*. New York: ACM Press.

Munson, Sean A., Daniel Avrahami, Sunny Consolvo, James Fogarty, Batya Friedman, and Ian Smith. 2012. Sunlight or sunburn: A survey of attitudes toward online availability of US public records. *Information Polity 17*(2), 99–114.

Murray, Ken, Kerry Burke, Chelsia Rose Marcius, and Rocco Parascandola. 2014. "Staten Island Man Dies After NYPD Cop Puts Him In Chokehold." *New York Daily News*, July 17, 2014, at http://www.nydailynews.com/new-york/staten-island-man-dies-puts-choke-hold-article-1.1871486.

Myers, Steve. 2011. "How Citizen Journalism Has Changed Since George Holliday's Rodney King Video." *Poynter*, Mar. 3, 2011, http://www.poynter.org/latest-news/top-stories/121687/how-citizen-journalism-has-changed-since-george-hollidays-rodney-king-video/.

Nast v. Michels, 107 Wash.2d 300 (Wash. 1986).

Nathan, Lisa P., Predrag V. Klasnja, and Batya Friedman. 2007. Value scenarios: a technique for envisioning systemic effects of new technologies. *Extended Abstracts of CHI 2007 Conference on Human Factors in Computing Systems*, 2585-2590. New York: ACM Press.

National Association for the Advancement of Colored People v. Alabama, 357 U.S. 449 (1958).

National Institute of Justice. "Research on Body-Worn Cameras and Law Enforcement." Accessed February 20, 2015, http://www.nij.gov/topics/law-enforcement/technology/Pages/body-worn-cameras.aspx.

NBC Miami. 2015. "Miami Police Fight Back Against Waze App." *NBC Miami*, February 17, 2015. http://www.nbcmiami.com/news/local/Miami-Police-Fight-Back-Against-Waze-App-290290001.html.

NCSL [National Conference of State Legislatures]. 2015. "Automated License Plate Readers | State Legislation." National Conference of State Legislatures. Last updated February 19, 2015. http://www.ncsl.org/research/telecommunications-and-information-technology/2014-state-legislation-related-to-automated-license-plate-recognition-information.aspx.

Neighborhood Alliance of Spokane County v. Spokane County, 172 Wash.2d 702 (Wash. 2011).

Nelkin, Dorothy, and Lori Andrews. 2003. Surveillance Creep in the Genetic Age. In David Lyon (ed.), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, 94-110. London; New York: Routledge.

Nerone, John. 1994. *Violence against the press: Policing the public sphere in U.S. History*. New York: Oxford University Press.

New Hampshire Revised Statutes § 570-A:2 (West, 2015).

New Hampshire Revised Statutes §§ 236, 261 (West, 2015).

New York Times Co. v. Sullivan, 376 U.S. 254 (1964).

New York Times Editorial Board. 2015. The Walter Scott Murder, *New York Times*, April 8, 2015 (printed in the New York version at p. A28 on April 9, 2015), at http://www.nytimes.com/2015/04/09/opinion/the-walter-scott-murder.html.

Newell, Bryce Clayton, Cheryl A. Metoyer, and Adam D. Moore. 2015. Privacy in the Family. In Beate Roessler and Dorota Mokrosinska (eds.), *Social Dimensions of Privacy: Interdisciplinary Perspectives*. Cambridge, UK: Cambridge University Press.

Newell, Bryce Clayton. 2011. Freedom of Panorama: A Comparative Look at International Restrictions on Public Photography. *Creighton Law Review*, 44, 405-427.

Newell, Bryce Clayton. 2014a. Crossing Lenses: Policing's New Visibility and the Role of 'Smartphone Journalism' as a Form of Freedom-Preserving Reciprocal Surveillance. *University of Illinois Journal of Law, Technology & Policy*, 2014, 59-104.

Newell, Bryce Clayton. 2014b. Local Law Enforcement Jumps on the Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy, and Access to Government Information. *Maine Law Review*, 66(2), 397-435.

Newell, Bryce Clayton. 2014c. Technopolicing, Surveillance, and Citizen Oversight: A Neorepublican Theory of Liberty and Information Control. *Government Information Quarterly*, 31, 421-431.

Newell, Bryce Clayton. 2014d. The Massive Metadata Machine: Liberty, Power, and Secret Mass Surveillance in the U.S. and Europe. *I/S: A Journal of Law and Policy for the Information Society*, 10(2), 481-522.

Newman v. King County, 133 Wash.2d 565 (Wash. 1997).

Newman, Andy. 2014. "The Death of Eric Garner, and the Events That Followed." *New York Times* (interactive online content), December 3, 2014, http://www.nytimes.com/interactive/2014/12/04/nyregion/04garner-timeline.html.

Newman, Lily Hay. 2015. "Police Oppose Police-Tracking Function in GPS App Waze." *Slate*, January 26, 2015, http://www.slate.com/blogs/future_tense/2015/01/26/waze_has_a_police_tracking_feature_that_law_enforcement_opposes.html.

Nieto, Marcus. 1997. "Public Video Surveillance: Is It An Effective Crime Prevention Tool?" Report CRB-97-005, California State Library and California Research Bureau.

Nissen v. Pierce County, 333 P.3d 577 (Wash. App. 2014).

Nissenbaum, Helen. 1998. Values in the Design of Computer Systems. *Computers in Society*, 38-39.

Nissenbaum, Helen. 2004. Privacy as Contextual Integrity. *Washington Law Review 79*(1), 119-158.

Noble, Andrea. 2013. "Police Now Armed with Video: Recording Can Protect Officer, Citizen Through Visual Proof." *Washington Times*, Feb. 25, 2013,

http://www.washingtontimes.com/news/ 2013/feb/25/police-now-armed-with-video/?page=all.

Noriega, David. 2015. "This Is The Texting Service Undocumented Immigrants Are Using To Avoid Police." *BuzzFeed News*. February 5, 2015, http://www.buzzfeed.com/davidnoriega/the-texting-service-undocumented-immigrants-are-using-to-avo#.rrXpOzkOD5.

Norris, Clive, and Gary Armstrong. 1999. *The Maximum Surveillance Society: The Rise of CCTV*. Berg.

Nourse, Victoria, and Gregory Shaffer. 2009. Varieties of New Legal Realism: Can a New World Order Prompt a New Legal Theory? *Cornell Law Review*, *95*, 61-138.

Nussbaum, Martha C. 2000. The Costs of Tragedy: Some Moral Limits of Cost-Benefit Analysis. *The Journal of Legal Studies*, 29(2), 1005-1036.

Nussbaum, Martha C. 2000. *Women and Human Development: The Capabilities Approach*. Cambridge, UK; New York: Cambridge University Press.

Obsidian Finance Group, LLC v. Cox, No. CV-11-57-HZ, 2011 U.S. Dist. LEXIS 137548 (D. Or. 2011).

ODS Consulting. 2011, July. Report: "Body Worn Video Projects in Paisley and Aberdeen: Self Evaluation." Glasgow: ODS Consulting. Accessed February 20, 2015, http://www.bwvsg.com/wp-content/uploads/2013/.../BWV-Scottish-Report.pdf.

Olmstead v. United States, 277 U.S. 438 (1928).

Orwell, George. *Nineteen Eighty-Four*. New York: Harcourt.

Owens, Catherine, David Mann, and Rory Mckenna. 2014. *The Essex Body Worn Video Trial: The impact of Body Worn Video on criminal justice outcomes of domestic abuse incidents*. London: College of Policing.

Palko v. Connecticut, 302 U.S. 319 (1937).

Peck v. United Kingdom, [2003] ECHR 44 (ECtHR, 2003).

Pennsylvania Consolidated Statutes, Title 18 (Crimes and Offenses) § 5704 (West, 2015).

Pennsylvania Consolidated Statutes, Title 30 (Fish) § 901 (West, 2015).

Pennsylvania Consolidated Statutes, Title 34 (Game) § 901 (West, 2015).

People v. Davila, 901 N.Y.S.2d 787 (N.Y. Sup. Ct. 2010).

People v. Weaver, 909 N.E. 2d 1195 (N.Y. 2009).

Perri 6. 2003. The Governance of Technology: Concepts, Trends, Theory, normative Principles and Research Agenda. Paper presented at the *Human Choice and Technological Change conference*, Lisbon Portugal, February 24-25, 2003.

Perry, Mary. 2015. Privacy and the PRA. Legal memo from Seattle City Attorney's office, shared with me by the author.

Pettit, Philip. 1996. Freedom as Antipower. *Ethics, 106*(3), 576-604.

Pettit, Philip. 1997. *Republicanism: A Theory of Freedom and Government*. Oxford, UK: Clarendon Press.

Pettit, Philip. 2001. *A Theory of Freedom: From the Psychology to the Politics of Agency*. Oxford, UK: Oxford University Press.

Pettit, Philip. 2002. Keeping Republican Freedom Simple: On a Difference with Quentin Skinner. *Political Theory, 30*(3), 339–356 (2002).

Pettit, Philip. 2003. Agency-Freedom and Option-Freedom. *Journal of Theoretical Politics, 15*(4), 387–403.

Pettit, Philip. 2008. Freedom and Probability: A Comment on Goodin and Jackson. *Philosophy and Public Affairs, 36*(2), 206–220.

Pettit, Philip. 2011. The Instability of Freedom as Noninterference: The Case of Isaiah Berlin. *Ethics, 121*(4), 693–716.

Pettit, Philip. 2012. *On the People's Terms: A Republican Theory and Model of Democracy*. New York: Cambridge University Press.

Pocock, J.G.A. 1979. *The Machiavellian Moment: Florentine Political Thought And The Atlantic Republican Tradition*. Princeton, N.J.: Princeton University Press.

Post, Robert C. 1993. Meiklejohn's Mistake: Individual Autonomy and the Reform of Public Discourse. *Colorado Law Review, 64*, 1109-1137.

Post, Robert C. 1995. *Constitutional Domains: Democracy, Community, Management*. Cambridge, Mass.: Harvard University Press.

Post, Robert C. 1997. Community and the First Amendment. *Arizona State Law Journal, 29*, 473-484.

Post, Robert C. 2001. Three Concepts of Privacy. *Georgetown Law Journal, 89*, 2087-2098.

Poudrier, Jennifer. 2003. 'Racial' Categories and Health Risks: Epidemiological Surveillance Among Canadian First Nations. In David Lyon (ed.), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, 111-134. London; New York: Routledge.

Privacy Act (Washington), Revised Code of Washington 9.73.010, *et seq.* (West, 2015).

Progressive Animal Welfare Soc. v. University of Washington, 125 Wash.2d 243 (Wash. 1994).

Prosser, William L. 1960. Privacy. *California Law Review, 48*(3), 383-423

Public Records Act, Revised Code of Washington (RCW) 42.56.001, *et seq.* (West, 2015).

Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008).

Rankin, Lee. 2013. *End of Program Evaluation/Recommendations: On-Officer Body Camera System*. Mesa, AZ: Mesa Police Department. Accessed February 20, 2015, http://issuu.com/leerankin6/docs/final_axon_flex_evaluation_12-3-13-.

Rasmussen, Kristen, Jack Komperda, and Raymond Baldino. 2012. *Reporter's Recording Guide: A state-by-state guide to tyaping phone calls and in-person conversations*. Arlington, VA: Reporters Committee for Freedom of the Press.

Reddish, Martin H. 2013. *The Adversary First Amendment*. Stanford, CA: Stanford University Press.

Reddish, Martin H., and Abby Marie Mollen. 2009. Understanding Post's and Meiklejohn's Mistakes: The Central Role of Adversary Democracy in the Theory of Free Expression. *Northwestern University Law Review, 103*(3), 1303-1370.

Regan, Tom. 1992. Introduction to Moral Reasoning. In Tom Regan (ed.), *Matters of Life and Death*, pp. 30-46. McGraw-Hill.

Reid v. Pierce County, 136 Wash. 2d 195 (Wash. 1998).

Resident Action Council v. Seattle Housing Authority, 300 P.3d 376 (2013).

Restatement (Second) of Torts (1977).

Rich, Michael L. 2014. Limits on the Perfect Preventative State. *Connecticut Law Review, 46*, 883-935.

Richard, William D. 2010. Note: Procedural Rules Under Washington's Public Records Act: The Case for Agency Discretion. *Washington Law Review, 85*, 493-516.

Richards, Neil M. 2008. Intellectual Privacy. *Texas Law Review, 87*, 387-445.

Rizza, Caroline, Ângela Guimarães Pereira, and Paula Curvelo. 2013. 'Do-it-yourself justice': considerations of social media use in a crisis situation: the case of the 2011 Vancouver riots. *Proceedings of the 10th International ISCRAM Conference*, pp. 411-15, Baden-Baden, Germany, May 2013.

Robbins, Caroline. 1959. *The Eighteenth-Century Commonwealthman: Studies in the Transmission, Development, and Circumstance of English Liberal Thought from the Restoration of Charles II until the War with the Thirteen Colonies*. Cambridge, MA: Harvard University Press.

Roberts, Andrew. 2014. A Republican Account of the Value of Privacy. *European Journal of Political Theory*. Prepublished May 12, 2014, DOI: 10.1177/1474885114533262.

Robertson, Mark W. and Anthony DiLello. 2008. State by State Employee Monitoring Laws. Paper published by Portfolio Media, Inc. on Law360.com.

Robinson v. Fetterman 378 F.Supp.2d 534 (E.D.Pa., 2005).

Roesner, Franziska, Tamara Denning, Bryce Clayton Newell, Tadayoshi Kohno, and Ryan Calo. 2014. Augmented Reality: Hard Problems of Law and Policy. *Proceedings (adjunct) of 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp 2014)*, 1283-1288. Seattle, WA; New York: ACM Press.

Roper, Eric. 2012a. "Police Cameras Quietly Capture License Plates, Collect Data." *Minneapolis Star Tribune*. Aug. 10, 2012. http://www.startribune.com/local/minneapolis/165680946.html.

Roper, Eric. 2012b. "City Cameras Track Anyone, Even Minneapolis Mayor Rybak." *Minneapolis Star Tribune*. Aug. 17, 2012. http://www.startribune.com/local/minneapolis/166494646.html.

Rosen, Jay. 2011. "Protect our Right to Anonymity." *New York Times* (op. ed.), p. A31, Sept. 13, 2011.

Rosenberg, Matt. 2011. "Seattle Police Memo: Body Cameras Easier Said Than Done, Now." *Social Capital Review*, September 7, 2011. Accessed February 20, 2015, http://socialcapitalreview.org/seattle-police-memo-body-cameras-easier-said-than-done-now/.

Sætnan, Ann Rudinow, Heidi Mork Lomell, and Carsten Wiecek. 2004. Controlling CCTV in Public Spaces: Is Privacy the (Only) Issue? Reflections on Norwegian and Danish observations. *Surveillance and Society, 2*(2/3): 396-414.

Sargent v. Seattle Police Department, 179 Wash.2d 376 (Wash. 2013).

Schneier, Bruce. 2015. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: W. W. Norton & Company.

Sciacca v. Italy, (2006) 43 EHRR 400 (ECtHR, 2006).

Seattle Police Department. 2011. "Seattle Police Department Response to Statement of Legislative Intent: Body-Mounted Camera Pilot Project." Response of September 8, 2011, to

the Energy, Technology and Civil Rights Committee, Seattle City Council. Accessed February 20, 2015, http://clerk.seattle.gov/~public/meetingrecords/2011/etcr20110908_3a.pdf.

Seattle Police Department. 2015. "SPD Launches YouTube Channel for Bodyworn Video." *SPD Blotter*, February 25, 2015, http://spdblotter.seattle.gov/2015/02/25/spd-launches-youtube-channel-for-bodyworn-video/.

Seattle v. Mesiani, 110 Wash.2d 454 (Wash. 1988).

Seawright, J. and John Gerring. 2008. Case Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options. *Political Research Quarterly, 61*(2), 294-308.

Selinger, Evan, and Woodrow Hartzog. 2014. Obscurity and Privacy. In Joseph Pitt and Ashley Shew (eds.), *Routledge Companion to Philosophy of Technology*. Pre-press version available at http://ssrn.com/abstract=2439866.

Sellars, Andy. 2013. "Focus Instead on Empowering Civilians." *New York Times*, Room for Debate, Oct. 22, 2013, at http://www.nytimes.com/roomfordebate/2013/10/22/should-police-wear-cameras/empower-civilians-to-record-the-police.

Sellers, M.N.S. 1994. *American Republicanism: Roman Ideology In The United States Constitution*. New York: New York University Press.

Sen, Amartya. 2004. Elements of a Theory of Human Rights. *Philosophy & Public Affairs, 32*, 315-356.

Shapiro v. United States, 335 U.S. 1 (1948).

Sharp v. Baltimore City Police et al., DOJ Statement of Interest, CA 11–2888, 2012 WL 9512053 (D.Md. Jan. 10, 2012).

Shay, Lisa, Greg Conti, John Nelson, and Woodrow Hartzog. 2013. Beyond Sunglasses and Spray Paint: A Taxonomy of Surveillance Countermeasures. *Proceedings of the IEEE International Symposium on Technology and Society (ISTAS '13)*. Toronto, Canada.

Sher, Scott. 1996. "Continuous Video Surveillance and Its Legal Consequences." Public Law Research Institute, University of California, Hastings College of the Law, Nov. 1996.

Shilton, Katie. 2009. Four Billion Little Brothers. *ACM Queue, 7*(7), 1-8 (August 2009). http://queue.acm.org/ detail.cfm?id=1597790.

Silverman v. United States, 365 US 505 (1961).

Simpson, J.A., and Weiner, E.S.C. (eds.). 1989. value, n. *Oxford English Dictionary*. Oxford: Clarendon Press, 1989.

Skinner, Quentin. 1984. "The paradoxes of political liberty." The Tanner lecture on human values, delivered at Harvard University, October 24 and 25, 1984.

Skinner, Quentin. 1998a. *Liberty before liberalism*. New York, NY: Cambridge University Press.

Skinner, Quentin. 1998b. The republican ideal of political liberty. In G. Bock, Q. Skinner, and M. Viroli (eds.), *Machiavelli and Republicanism*, pp. 239-309. Cambridge, UK: Cambridge University Press.

Skinner, Quentin. 2008. *Hobbes and Republican Liberty*. New York, NY: Cambridge University Press.

Slobogin, Christopher, and Joseph E Schumacher. 1993a. Rating the Intrusiveness of Law Enforcement Searches and Seizures. *Law & Human Behavior, 17*, 183-200 (1993).

Slobogin, Christopher, and Joseph E Schumacher. 1993b. Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at 'Understandings' Recognized and Permitted by Society. *Duke Law Journal, 42*, 727-775.

Slobogin, Christopher. 2002. Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity. *Mississippi Law Journal, 72*, 213-300.

Slobogin, Christopher. 2008. Government Data Mining and the Fourth Amendment. *Chicago Law Review, 75*, 317-341.

Slobogin, Christopher. 2012. Making the Most of United States v. Jones in a Surveillance Society: A Statutory Implementation of Mosaic Theory. *Duke Journal of Constitutional Law & Public Policy, 8*, 1-37.

Smith v. City of Cumming, 212 F.3d 1332 (11th Cir. 2000).

Smith v. Maryland, 442 U.S. 735 (1979).

Smith v. State, 229 Ga.App. 570 (Ga. App. 1997).

Smith, Jonathan M. 2012. Letter from U.S. Department of Justice to Mark H. Grimes and Mary E. Borja of May 14, 2012. http://www.aclu-md.org/uploaded_files/0000/0311/doj_guidance.pdf.

Solove, Daniel J. 2001. Privacy and Power: Computer Databases and Metaphors for Information Privacy. *Stanford Law Review, 53*, 1393-1462.

Solove, Daniel J. 2002. Access and Aggregation: Privacy, Public Records, and the Constitution. *Minnesota Law Review, 86*, 1137-1209.

Solove, Daniel J. 2003. The Virtues of Knowing Less: Justifying Privacy Protections against Disclosure. *Duke Law Journal, 53*, 967-1065.

Solove, Daniel J. 2004. *The Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press.

Solove, Daniel J. 2006. A Taxonomy of Privacy. *U. Penn. Law Review, 154*, 477-564.

Solove, Daniel J., and Paul M. Schwartz. 2009. *Information Privacy Law.* New York: Aspen Publishers.

Solove, Daniel, Marc Rotenberg, and Paul M. Schwartz. 2006. *Information Privacy Law.* New York: Aspen Publishers.

Stalder, Felix, and David Lyon. 2003. Electronic Identity Cards and Social Classification. In David Lyon (ed.), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, 77-93. London; New York: Routledge.

Stanley, Jay. 2013. Report: *Police Body-Mounted Cameras: With Right Policies in Place, a Win For All*. American Civil Liberties Union, available at https://www.aclu.org/files/assets/police_body-mounted_cameras.pdf.

State v. Athan, 160 Wash.2d 354 (Wash. 2007).

State v. Bonilla, 23 Wash.App. 869 (Wash. App., 1979).

State v. Caliguri, 99 Wash.2d 501 (Wash. 1983).

State v. Carter, 151 Wash.2d 118 (Wash. 2004).

State v. Cheatam,150 Wash.2d 626 (Wash. 2003).

State v. Clark, 129 Wash.2d 211 (Wash. 1996).

State v. Collins, 152 Wash.App. 429 (Wash. App. 2009), *review denied*, 168 Wash.2d 1020.

State v. Creegan, 123 Wn. App. 718 (Wash. App. 2004).

State v. D.J.W., 76 Wash.App. 135 (Wash. App. 1994), *review granted*, 126 Wash.2d 1008, *decision affirmed and remanded*, 129 Wash.2d 211.

State v. Dorn, 1993 WL 258690 (Del. Sup. 1993) (not reported).

State v. Eisfeldt, 163 Wash.2d 628 (Wash. 2008).

State v. Flora, 845 P.2d 1355 (Wash. Ct. App. 1992).

State v. Forrester, 21 Wash.App. 855 (Wash. App. 1978).

State v. Gunwall, 106 Wash.2d 54 (Wash. 1986).

State v. Hatchie, 133 Wash.App. 100 (Wash. App. 2006), *review granted*, 159 Wash.2d 1014, *affirmed*, 161 Wash.2d 390.

State v. Hinton, 169 Wash.App. 28 (Wash. App. 2012), *review granted*, 175 Wash.2d 1022, *reversed*, 179 Wash.2d 862.

State v. Jackson, 111 Wn. App. 660 (Wash. App. 2002), *affirmed*, 150 Wn.2d 251 (2003).

State v. Jorden, 160 Wash.2d 121 (Wash. 2007).

State v. Kipp, 179 Wash.2d 718 (Wash. 2014).

State v. Lakotiy, 151 Wash.App. 699 (Wash. App. 2009).

State v. MacDicken, 179 Wash.2d 936 (Wash. 2014).

State v. Meneese, 174 Wash.2d 937 (Wash. 2012).

State v. Miles, 160 Wash.2d 236 (Wash. 2007), *on subsequent appeal*, 159 Wash.App. 282, *review denied*, 171 Wash.2d 1022.

State v. Modica, 136 Wash.App. 434 (Wash. App. 2006), *review granted*, 162 Wash.2d 1001, *affirmed*, 164 Wash.2d 83.

State v. Monaghan, 165 Wash.App. 782 (Wash.App. 2012).

State v. Myrick, 102 Wash.2d 506 (Wash. 1984).

State v. Pejsa, 75 Wash.App. 139 (Wash. App. 1994), *review denied*, 125 Wash.2d 1015.

State v. Roden, 179 Wash.2d 893 (Wash. 2014).

State v. Slemmer, 48 Wash.App. 48 (Wash. App. 1987).

State v. Stroud, 106 Wash.2d 144 (Wash. 1986).

State v. Surge, 160 Wash.2d 65 (Wash. 2007).

State v. Townsend, 147 Wash.2d 666 (Wash. 2002).

State v. White, 141 Wn. App. 128 (2007).

State v. Williams, 94 Wash.2d 531 (Wash. 1980).

State v. Young, 123 Wn.2d 173 (Wash. 1994).

Stevens, Gina, and Charles Doyle. 2012. Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping. Congressional Research Service, CRS Report No. 98-326. October 9, 2012.

Stone, Brad. 2009. "Prop 8 Donor Web Site Shows Disclosure Law is 2-Edged Sword." *New York Times*, Feb. 8, 2009, p. BU3, *available at* http://www.nytimes.com/2009/02/08/business/08stream.html.

Strossen, Nadine. 2005. Safety and Freedom: Common Concerns for Conservatives, Libertarians, and Civil Libertarians. *Harvard Journal of Law & Public Policy, 29*, 73-83.

Strossen, Nadine. 2013. Government Secrecy and Surveillance: We the People Know Too Little About Our Government While It Knows Too Much About Us. Paper presented at the 2013 *Information Ethics Roundtable*, Seattle, WA (April 26, 2013), at http://infoethics.ischool.uw.edu/?attachment_id=346.

Stroud, Matt. 2013. "In Boston bombing, flood of digital evidence is a blessing and a curse." *The Verge*, April 16, 2013, http://www.theverge.com/2013/4/16/4230820/in-boston-bombing-flood-of-digital-evidence-is-a-blessing-and-a-curse.

Sullivan v. Gray, 324 N.W.2d 58 (Mich. Ct. App. 1982).

Sullivan, Jennifer. 2014a. "Man drops massive records requests, will help Seattle police with video technology." *Seattle Times*, updated November 21, 2014, http://www.seattletimes.com/seattle-news/man-drops-massive-records-requests-will-help-seattle-police-with-video-technology/.

Sullivan, Jennifer. 2014b. "'Hackathon' asks techies to aid SPD on sensitive-video issues." *Seattle Times*, December 14, 2014, http://www.seattletimes.com/seattle-news/lsquohackathonrsquo-asks-techies-to-aid-spd-on-sensitive-video-issues/.

Sundby, Scott E. 1994 Everyman's' Fourth Amendment: Privacy or Mutual Trust between Government and Citizen? *Columbia Law Review, 94*(6), 1751-1812.

Sunstein, Cass R. 1992. Free Speech Now. *University of Chicago Law Review, 59*, 255-316.

Sunstein, Cass R. 1993. *Democracy and the Problem of Free Speech*. New York: The Free Press.

Swift, Adam. 2006. *Political Philosophy: A Beginner's Guide for Students and Politicians*. 2nd ed., Cambridge; Malden, MA: Polity.

Swire, Peter, and Kenesa Ahmad. 2011. "'Going Dark' Versus a 'Golden Age for Surveillance'." *Center for Democracy & Technology*, November 28, 2011, https://cdt.org/blog/'going-dark'-versus-a-'golden-age-for-surveillance'/.

Tamanaha, Brian Z. 1997. *Realistic Socio-legal Theory: Pragmatism and a Social Theory of Law*. New York/Oxford: Oxford University Press.

Taylor, James Stacey. 2005. In Praise of Big Brother: Why We Should Learn to Stop Worrying and Love Government Surveillance. Public Affairs Quarterly, 19, 227-246.

Taylor, Paul. 1989. Happiness and Intrinsic Value. In Louis Pojman (ed.), *Ethical Theory: Calssical and Contemporary Readings*. Belmont, CA: Wadsworth.

Ten, C.L. 1968. Mill on Self-regarding Actions. *Philosophy, 43*, 29-37.

Tennessee Code § 55-10-302 (West, 2015).

Terry v. Ohio, 392 U.S. 1 (1968).

The Guardian. 2009. "Video of Police Assault on Ian Tomlinson, Who Died at the London G20 Protest." Youtube.com, posted Apr. 8, 2009, https://www.youtube.com/watch?v=HECMVdl-9SQ (over 1,033,000 views as of April 7, 2015).

Thompson v. City of Clio, 765 F.Supp. 1066 (M.D.Ala. 1991).

Thompson, John B. 2005. The New Visibility. *Theory, Culture and Society, 22*, 31–51.

Thompson, Judith Jarvis. 1975. The Right to Privacy. *Philosophy and Public Affairs, 4(4)*, 295-314.

Time, Inc. v. Hill, 385 U.S. 374 (1967).

Tsesis, Alexander. 2014. The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data. *Wake Forest Law Review*, *49*, 433-484.

U.S. Department of Justice. 2003. Community Relations Service, *Principles of Good Policing: Avoiding Violence between Police and Citizens* (rev. Sept. 2003). http://www.justice.gov/archive/crs/pubs/principlesofgoodpolicingfinal092003.pdf.

UK Information Commissioner. 2013a. Press Release: "Data Protection Act 1998 Enforcement Notice." July, 15, 2013. http://www.ico.org.uk/news/latest_news/2013/~/media/documents/library/Data_Protection/Notices/hertfordshire-constabulary-enforcement-notice.pdf.

UK Information Commissioner. 2013b. Press Release: "Police Use of 'Ring Of Steel' is Disproportionate and Must Be Reviewed." July 24, 2013. http://www.ico.org.uk/news/latest_news/2013/Police-use-of-Ring-of-Steel-is-disproportionate-and-must-be-reviewed-24072013.

United States Constitution, Amendment IV.

United States Constitution, Amendment V.

United States v. Davis, 326 F.3d 361 (2003).

United States v. Hastings, 695 F.2d 1278 (11th Cir.1983).

United States v. Jones, 132 S. Ct. 945 (2012).

United States v. Knotts, 460 U. S. 276 (1983).

United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).

United States v. Miller, 425 U.S. 435 (1976).

United States v. Vargas, Order Granting Defendant's Motion to Suppress, Case No. CR-13-6025-EFS (D.C. East. Dist. Wash., Dec. 15, 2014).

United States v. Vespe, 389 F.Supp. 1359 (D.C. Del., 1975), *aff'd on other grounds*, 520 F.2d 1369 (3rd Cir. 1975), *cert. denied*, 423 U.S. 1051 (1976).

United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

Utah Code §§ 41-6a-2004, 63G-2-305 (West, 2015).

Utah Senate Bill 196. 2013. General Session (Utah 2013). http://le.utah.gov/~2013/bills/sbillenr/SB0196.htm.

Utah Senate Bill 51. 2014. 2014 Utah Laws Ch. 377 (S.B. 51), approved April 1, 2014.

Van den Hoven, Jeroen. 2007. ICT and value sensitive design. In Goujon, P., Lavelle, S., Duquenoy, P., Kimppa, K., and Laurent, V. (eds.), *The information society: Innovation, legitimacy, ethics and democracy in honor of Professor Jacques Berleur*, pp. 67-72. New York: Springer.

Vancouver Police Department. 2011. "2011 Stanley Cup Riot Review." Vancouver Police Department, http://vancouver.ca/police/assets/pdf/reports-policies/vpd-riot-review.pdf.

Vancouver Police Department. 2013. Press Release: "Vancouver Police Department, IRIT Recommends Charges Against 350th Suspected Rioter." Vancouver Police Department. July 23, 2013, http://mediareleases.vpd.ca/2013/07/23/irit-recommends-charges-against-350th-suspected-rioter/.

Vanhemert, Kyle. "Are Cameras the New Guns?" *Gizmodo*, June 2, 2010, http://gizmodo.com/5553765/are-cameras-the-new-guns.

Vermont Department of Public Safety, Division of Criminal Justice. "ALPR End User Agreement." http://www.acluvt.org/legal/docket/files/alpr/dept_of_pub_safety_docs/Vt.%20Dep't%20of%20Pub.%20Safety%20ALPR%20data%20agreement.pdf.

Vermont Statutes, Title 20 (Internal Security and Public Safety) § 2367 (West, 2015).

Vermont Statutes, Title 23 § 1607 (West, 2015).

Virginia Code § 2.2-3800 (West, 2015).

Volokh, Eugene. 2000. Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking about You. *Stanford Law Review, 52*, 1049-1124.

Von Hannover v. Germany (II), (2012) 55 E.H.R.R. 15 (ECtHR, 2012).

Von Hannover v. Germany, (2005) 40 E.H.R.R. 1 (ECtHR, 2004).

Wadhwa, Tarun. 2013. "Lessons from Crowdsourcing the Boston Bombing Investigation. *Forbes* (Apr. 22, 2013, 9:32 AM), http://www.forbes.com/sites/tarunwadhwa/2013/04/22/lessons-from-crowdsourcing-the-boston-marathon-bombings-investigation/.

Walker, Peter. 2012. "Ian Tomlinson Case: PC Simon Harwood Sacked For Gross Misconduct." *The Guardian*, September 17, 2012, http://www.guardian.co.uk/uk/2012/sep/17/simon-harwood-sacked-gross-misconduct.

Walker, Samuel. 2000. *Police Accountability: The Role of Citizen Oversight*. Belmont, CA: Wadsworth Thompson Learning.

Walker, Samuel. 2005. *The New World of Police Accountability*. Thousand Oaks, CA: SAGE Publications.

Warden, Maryland Penitentiary v. Hayden, 387 U.S. 294 (1967).

Warren, Samuel D., and Louis D. Brandeis. 1890. The Right of Privacy. *Harvard Law Review, 4*, 193-220.

Warshak v. United States, 490 F.3d 455 (6th Cir. 2007), *vacated*, 532 F.3d 521 (6th Cir. 2008).

Washington Administrative Code § 44-14-06002 (West, 2015).

Washington House Bill 1910. 2015. 64th Washington State Legislature, First Regular Session.

Washington House Bill 1917 (Substituted Bill). 2015. 64th Washington State Legislature, First Regular Session.

Washington House Bill 1917. 2015. 64th Washington State Legislature, First Regular Session.

Washington Senate Bill 5732. 2015. 64th Washington State Legislature, First Regular Session.

Washington State Constitution, Article I § 7.

Wasserman, Howard M. 2014. Moral Panics and Body Cameras. *Washington University Law Review Commentaries*, November 18, 2014, http://openscholarship.wustl.edu/law_lawreview_commentaries/26.

Wasserman, Howard M. 2015. Epilogue: Moral Panics and Body Cameras. *Washington University Law Review Commentaries*, January 1, 2015, http://openscholarship.wustl.edu/law_lawreview_commentaries/27.

Weber, Ron. 2004. Editor's Comments: The Rhetoric of Positivism Versus Interpretivism: A Personal View. *MIS Quarterly, 28(1),* iii-xii.

Webster, C. William R. 2009. CCTV Policy in the UK: Reconsidering the Evidence Base. *Surveillance & Society*, 6(1), 10-22.

Welsh B. and D. Farrington. 2004. Evidence-based Crime Prevention: the Effectiveness of CCTV. *Crime Prevention and Community Safety: An International Journal, 6*(2), 21-33.

Westin, Alan F. 1967. *Privacy and Freedom*. New York: Atheneum.

Westley, William A. 1956. Secrecy and the Police. *Social Forces, 34*, 254–257.

Weston, Anthony. 2000. *A Rulebook for Arguments*. Indianapolis, IN: Hackett Publishing Co.

Whitaker, Reg. 1999. *The End of Privacy: How Total Surveillance Is Becoming a Reality*. New York: The New Press.

White v. Township of Winthrop, 128 Wash. App. 588 (Wash App. Div. 3, 2005).

White, Michael D. 2014. *Police Officer Body-Worn Cameras: Assessing the Evidence*. Washington, D.C.: Office of Community Oriented Policing Services.

Whiteland Woods, L.P. v. Township of West Whiteland, 193 F.3d 177 (3rd Cir. 1999).

Whitney v. California, 274 U.S. 357 (1927).

Willis, Graham Denyer, Robert Muggah, Justin Kosslyn, and Felipe Leusin. 2013. *Smarter Policing: Tracking the Influence of New Information Technology in Rio de Janeiro*. Strategic Paper 10 (November 2013). Igarapé Institute.

Wilson v. Layne, 526 U.S. 603 (1999).

Wilson, Dean Jonathon, and Tanya Serisier. (2010). Video Activism and the ambiguities of counter-surveillance. *Surveillance & Society, 8*, 166–180.

Wood, David Murakami, & C. William R. Webster. 2009. Living in Surveillance Societies: The Normalisation of Surveillance in Europe and the Threat of Britain's Bad Example. *Journal of Contemporary European Research, 5(2),* 259-273.

Yoo, Daisy, Alina Huldtgren, Jill Palzkill Woelfer, David G. Hendry, and Batya Friedman. (2013). A value sensitive action-reflection model: Evolving a co-design space with stakeholder and designer prompts. *Proceedings of CHI 2013*, 419-428. New York, NY: ACM Press.

York v. Wahkiakum School Dist. No. 200, 163 Wash.2d 297 (Wash. 2008).

Youker v. Douglas County, 178 Wash. App. 793 (Wash. App. 2014), *review denied,* 180 Wash. 2d 1011 (Wash. 2014).

Zureik, Elia. 2003. Theorizing Surveillance: the Case of the Workplace. In David Lyon (ed.), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, 31-56. London; New York: Routledge.