BUILDING GLASS CASTLES: RETHINKING PRIVACY AND SURVEILLANCE FROM THE PANTHEON TO THE PANOPTICON

Edward Percario

Honors Thesis Submitted to the Department of History, Georgetown University
Advisor: Professor Meg Jones
Honors Program Chair: Professor Amy Leonard

9 May 2016
Abstract
This thesis investigates the qualitative shifts of government surveillance regimes across history and the implications of these changes on the role of privacy as a boundary of the surveillance apparatus. It tackles two normative assumptions of current surveillance theory surrounding the model of the panopticon: first, that the panopticon did not arise until after the Enlightenment; second, that the panopticon, while a useful symbol, no longer functions as a model in the twenty-first century due to irreconcilable qualitative paradigm shifts in the mechanisms of surveillance. This paper asserts that fundamental elements of both panoptic and post-panoptic surveillance existed in pre-Enlightenment regimes, and explores the role and significance of the qualitative shifts from the Benthamite-Foucauldian model to present surveillance apparatuses. Mapping the fundamentality and ephemerality of certain qualitative aspects of surveillance regimes and their interplay with role of privacy within them can help distinguish perceived novelties in the present day from what appear to be more normative tenets. Overall, this thesis asks: are the motives, dynamics, actors, functions, and technological changes of surveillance in the twenty-first century really so novel that they require wholly different models, and if so, which elements need revision?
Acknowledgements

I give permission to Lauinger Library to make this thesis available to the public.

This thesis would not exist without the open-mindedness of Professor Amy Leonard. For the past year and a half, you have listened with astounding patience to my perhaps off-kilter qualms with how Georgetown views history as an academic discipline. I am profoundly indebted to your tolerance and grace in the face of my rather brazen arguments for writing a pseudo-history thesis. Moreover, you took such time and care to read not only my own thesis but the theses of our entire cohort, and gave profoundly insightful comments throughout. Your dedication and vitality inspired me to produce content worth reading (because I knew that at least one person would be reading it), and your trust in me allowed me to write the immensely interdisciplinary thesis that lies within these pages. I can only hope to aspire to be such a professor someday.

I am also unspeakably indebted to Professor Meg Jones. By the time you read these acknowledgements, you will already have transitioned into motherhood. But first, you helped me work through some of the most trying transitions in the sunset of my college career. You primed me on the transition from Georgetown to Oxford, and advised me through the existential crises that come with the prospect of long-term career planning. I still have no idea how you managed to teach a class, publish a book, speak at conferences, and read 150 pages of my undergraduate writing while being pregnant all the while. And most of all, you somehow managed to do it with an astonishingly chipper attitude, one that far outstripped my own during a time of far lesser burdens.

Dean Pirrotti, you may indeed have had the biggest impact on my thesis without even reading it. Much of the philosophical slant of the thesis is indebted to our discussions where you spurred my desire for a deeper understanding of what is right, and how we as humans ought to interact with each other and the world. I cannot and will never be able to call myself an historian, but you’ve taught me what it means to approach a problem as a historian does, and why that is fundamentally different from a legal scholar or philosopher’s approach. You have cemented in me the love and value of history, and encouraged rather than dissuaded my fusion of history with law, philosophy, and English. Thank you for the innumerable conversations, the spot-on guidance, and the cheese.

Finally, I wish to thank my family and friends for the indefatigable support throughout the past year of stress and griping. Mom, Dad, and Ryan: thanks for the unwavering love and support that makes holing up and writing a thesis far easier to bear. Likewise for Anthony, Brian, Katie and Sana: thank you for always being honest and telling me when I don’t make sense, and for being my companions during late nights and early mornings and everything in between. Last but not least (and certainly not exhaustively), my immense gratitude goes to my history thesis cohort for taking the time out of your own busy thesis-writing sessions to read my disjointed prose and befuddled arguments.

Isaiah Berlin once wrote an essay attempting to divide people into hedgehogs and foxes. He used an aphorism by Archilochus as a template: “the fox knows many things, but the hedgehog knows one big thing.” This thesis has pushed me further than ever before to know many things, and the process has led me to produce one very big thing. Here’s to many more.
# Table of Contents

**INTRODUCTION** ................................................................................................................................. 5  
I. Seeing Eye to Eye ................................................................................................................................. 5  
II. A Whole New World? .......................................................................................................................... 8  
III. Focusing the Gaze: Argument, Methodology, and Structure ......................................................... 10  

**CHAPTER I: EYEING-OPTICONS** ........................................................................................................... 14  
I. Cracking the Literature: The Academic Myopticon ........................................................................... 14  
II. Theories of Surveillance from the Panopticon and Beyond .............................................................. 17  
III. Lidding the Eye: Privacy as a Boundary of Surveillance ................................................................. 23  
IV. Widening the Philosophical Aperture ............................................................................................. 36  

**CHAPTER II: THE PANTHEON AND THE PANOPTICON** ......................................................................... 40  
I. Building a Surveillance System: Structures of the Surveillance Assemblage .................................... 43  
II. Behind Iron Mask and Pen: Privacy from Government in Rome .................................................... 52  
III. Escaping the Pantheopticon ........................................................................................................... 64  

**CHAPTER III: TRAPPED IN THE AMERICAN PRISM** ........................................................................... 70  
I. Privacy and Surveillance in Colonial America .................................................................................. 70  
II. Building Big Brother: Upstream and Downstream Surveillance .................................................... 78  
III. Picking Apart the Penumbra: Historicizing U.S. Privacy from Government .............................. 88  
IV. Oversight and Out of Mind: American Surveillance (Un)Restricted ............................................. 95  
V. Clusters of Surveillance: Outcasts, Airports, and Aliens ............................................................... 104  

**CONCLUSION** ..................................................................................................................................... 112  
**APPENDIX** .......................................................................................................................................... 117  
**BIBLIOGRAPHY** ................................................................................................................................... 124
INTRODUCTION

I. Seeing Eye to Eye

Consider three stories in the life of a hypothetical character, Mr. Glass, an American citizen and resident of New York during the month of February 2016. To preface, Mr. Glass has grown his company, Eye2Eye, over the past five years from a small technology startup to a multinational corporation. The title “Eye2Eye” references two primary features that define the business model and corporate ethos: when spoken it can sound like “I-to-I,” which speaks to its aim to create a flatter, interconnected world through communication; at the same time, when written, “Eye-to-Eye” embodies the safety of the service and top-of-the-line encryption standards that truly make each communication seen only by the eyes of the sender and receiver. Under this overarching philosophy, the business has grown from providing simple encryption services to expanding its network internationally, offering cloud storage and processing, a reliable internet service (i.e. it is an ISP), and even providing special Eye-Phones for its users to perform various tasks from accessing the Internet to making phone calls. It recently acquired an international user base of over one hundred million, residing predominately in the US and Europe. Indeed, until February 2016 Mr. Glass was an exceptionally happy individual.

Case 1 (February 1, 2016):

Mr. Glass’ morning coffee is interrupted by a call from the FBI. An Iowa native set off three small bombs in cafes in Des Moines and subsequently shot up a restaurant, killing thirty people before being gunned down by the police. The FBI has reason to believe that the gunman is in fact part of a larger terrorist organ and that this event was merely the beginning of a
sequence of attacks across American cities. As a result, the FBI has obtained a warrant to raid his home and property looking for clues to prevent the imminent events. Eye2Eye has provided all requested data related to the individual stored in their servers; however, the FBI cannot access his Eye-Phone due to the fact that it will erase all the data within should they fail to guess the password correctly after five tries. Mr. Glass is therefore required to disable the auto-erase function, but since his software lacks a back door even from Eye-2Eye, he will be forced to create a mechanism to hamper his own service and hand it over to the government.

Though the request is founded on legal precedent, Mr. Glass hesitates to comply. He worries that creating software to bypass mechanisms in the operating system sets a dangerous precedent for other privacy-invasive or surveillance-enhancing operations. To name a few harrowing scenarios, the government could subsequently require Eye2Eye to build surveillance software to track users’ locations, access personal data (e.g. financial and health information), or intercept messages on behalf of government surveillance. Alternatively, should Eye2Eye create this supposedly case-specific key to decrypt the Eye-Phone, the government would see the blueprint of Eye2Eye’s entire encryption software and use the knowledge to create a “master key” to use on all its citizens. Mr. Glass refuses to turn Eye2Eye into Eye3Eye and brings the case to court, to which the New York District Court rejects his appeal, and Mr. Glass must now comply with the government as initially requested.

Case II (February 16, 2016)

1 FBI’s method, called a “brute force attack” uses a trial-and-error method to plug in a large sequence of all possible combinations to open the device. Clearly, such a method would not work with limited guesses.

2 This legal precedent is the All Writs Act of 1789, or more appropriately the Judiciary Act of 1789, Ch. 20, § 14, 1 Stat. 73 81–82 (codified as amended at 28 U.S.C. § 1651[a]). This will be returned to in greater depth in Chapter III.

3 See Tim Cook’s “A Message to Our Customers,” Apple (Feb. 16, 2016) for similar arguments.

4 This phrasing mimics Tim Cook’s rhetoric in the above letter.
A few weeks after this debacle, Mr. Glass discovers that he could potentially lose half his user base. Apparently, the European Court of Justice (CJEU) had been following Glass’ prior case and decided that the US surveillance scheme has finally overstepped its bounds and made it impossible for American businesses to uphold adequate data protection principles. As a result, EU citizens’ fundamental right to privacy had been violated. This decision affects Eye2Eye regardless of Eye2Eye’s own encryption and privacy standards, because the issue is not on business-wide compliance level but rather on the overarching protocols espoused by the government, primarily FISA Article 702 that allows for the US government to intercept cross-border data flows entering American soil, and request corporate data sharing without necessarily having a specific target in mind. As a result, Mr. Glass will be forced to either relocate his data centers – currently housed in the US – to Europe, or hope that the US revamp its surveillance and privacy-oriented legislation.

*Case Three (February 28, 2016):*

Mr. Glass has been plagued by bad dreams riddled with themes of financial loss, injustice, and tyranny. Not only that, but even during his waking hours he feels the creeping sensation of being watched – public cameras seem to be ubiquitous and follow him as he walks down the streets of New York; sometimes he hears a faint whirring noise, but looking around he sees nothing. He begins to think he’s going insane, until today when he finally spots the source of the whirring: a drone. Calling his beleaguered and frankly defeated lawyer, they discover that Mr. Glass has been tracked for the last two weeks. Apparently, the government suspected that Mr. Glass may have been disgruntled with the verdict and could be plotting revenge. Since he is a powerful man and manages a staff of highly capable computer scientists, Mr. Glass could plausibly infiltrate government infrastructure and either sell information to foreign countries or
directly cause damage via computer network attack. Mr. Glass and his lawyer consequently formulate a case based on a Fourth Amendment violation and take the matter to court.

The Court’s decision, again, is not favorable. In a 5-4 ruling, the Court decides in the majority opinion that Mr. Glass had no reasonable expectation for privacy from aerial oversight because “any member of the public” flying in navigable airspace could have seen what the police saw. Furthermore, the drone had not trespassed on his private property or curtilage. The dissenting opinion argued that regardless of how the surveillance was conducted, it had clearly violated Mr. Glass’ expectation of privacy through its ability to glean insight into intricate details of his life beyond mere public activity. The knowledge acquired from this duration of surveillance was intrusive enough to glean the same if not more information that a “search” would under the Fourth Amendment, and therefore the government would have needed a warrant. However, to emphasize, this latter argument constituted the minority opinion and failed. Consequently Mr. Glass retired, dejected and defeated, a Dickensian victim of his aptronymic fate.

II. A Whole New World?

Mr. Glass’ narrative is neither paradigmatic nor true in the sense that a single individual has incurred such a hapless sequence of trials. Yet nor were these events conjured out of thin air. In fact, they all reflect, to large extent, three cases that have emerged in the past four years (two of these in the past six months). Mr. Glass’ first week mirrors the ongoing Apple-FBI case. The only difference here is that while the district court ruled to uphold the mandate, the case still

---

remains undecided and under appeal. Case II reflects the October 2015 *Schrems v. Data Protection Commissioner* ruling, whereby the CJEU invalidated the EU-US Safe Harbor agreement. Mr. Glass’ reaction mimicked those of American tech firms following the ruling, which would prevent US companies from storing and processing EU citizens’ data on American soil. This case deviates from current events in that the US was granted six months to renegotiate terms with the EU and remedy the situation, and as a result the governments have announced the creation of an EU-US ‘‘Privacy Shield.’’ The third case deviates quite a bit from its counterpart, *United States v. Jones* (2012). In this case, a GPS “Q-Ball” tracker was planted on the car of a suspected drug trafficker without a warrant. During the course of four weeks, the suspect was monitored and a large stash of drugs was discovered. The defendant filed a violation of the Fourth Amendment and the Supreme Court ruled that such monitoring indeed constituted a “search” and required a warrant. However, the changes in the narrative alter the case such that it falls out of scope of each Justice’s opinion aside from that of Justice Sotomayor. As a result, the actual outcome of such a hypothetical is speculative at best.

Stepping away from its contextualization in the present day, the cyber-centric narrative of Mr. Glass begs the question of historical exceptionalism. Does this herald the beginning of a new era of surveillance and privacy from government (or lack thereof)? To be sure, no other era’s government has had such urbanized populations to keep track of or porous borders through which communication flows by the terabyte. Nor has any government faced such an immediate threat from its own integration into these networks, and the resulting capacity of mere

---

6 European Commission. *EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield* (Strasbourg: February 2, 2016). This will be further discussed in the Conclusion.

7 My goal here, and further in Chapter III of this paper, is to show the narrow justification in the majority and concurring opinions that fall short of imminent situations posed by modern surveillance in the present day.
individuals to create such havoc on a macro-scale both in and out of the country. At the same
time, never before have governments had the tools to monitor society through drones, GPS,
CCTV cameras, and intangible surveillance mechanisms. Nor have governments been able to
collect and process such massive amounts of information, or had the potential to use “master”
decryption keys to unlock coded data *en masse*. As Jennifer Granick of Stanford’s Center for
Internet and Society remarks, “From an historical perspective, we’re entering a very new
era…Now we have a surveillance-enabled world.”

**III. Focusing the Gaze: Argument, Methodology, and Structure**

Perhaps Granick is right and we have entered a new era of government surveillance over
the individual. In any case, this thesis seeks to take the argument further than the visceral head-
nod and parse out the particulars of Granick’s claim. What did surveillance look like before this
new era, and how are past forms of surveillance different than they are now?

In order to answer these questions, “different” refers to qualitative rather than
quantitative differences in how surveillance functions and how privacy acts as a boundary of
surveillance. Qualitative shifts refer to changes in characteristics and composition of the model
itself; quantitative shifts refer to changes in the degree or penetration of these aspects. For
example (and this will be discussed more in-depth in the following chapter), sociologist and
surveillance theorist James Rule names four factors affecting surveillance capacity, all of which
happen to be quantitative metrics: file size, degree of centralization, speed of information flow,
and number of contacts between administrative systems and subject populations. Alternatively,

---

p. 38 for this particular differentiation.
a qualitative metric instead evaluates changes in who is being kept on file, how centralization is structured, how information flows and by what medium. Returning to Granick’s statement, it is self-evident that government surveillance has historically undergone quantitative shifts as technology allows more people to be surveilled with greater frequency, and as bureaucratization and central administration increase capacities for storage and retrieval. Whether mechanisms of government surveillance have undergone qualitative shifts, and how they have done so, presents a far more ambiguous and complex question.

This thesis engages in a comparative analysis of two case studies: the Roman Empire during the time of Ulpian (circa 200 AD) and the United States under the PATRIOT ACT and PRISM program (2001-2015). Comparing a pre-Enlightenment case study with a modern case study engages the claim made by Canadian surveillance theorist David Lyon: “Surveillance as we know it today – that is, as an institutionally central and pervasive feature of social life – did not emerge until modern times.”\(^{10}\) But is this valid? The following pages respond in the negative. This thesis further contends that the entire approach to surveillance theory – centered on attaching surveillance paradigms to their time periods – gives undue credit to the qualitative similarities of pre- and post-Enlightenment surveillance regimes.

As a metric for gauging qualitative shifts among my case studies, I borrow Kevin Haggerty’s characteristics by which he qualitatively differentiates the post-panoptic from panoptic paradigms.\(^ {11}\) These are broken down into five categories: purpose, hierarchy, targets, agents, and dynamics. These will be explored further in the following chapter, but briefly: “purpose” refers to whether the structures are fit for purpose (and necessarily whether the

---

10 Lyon 1994, p. 24. By “modern times,” Lyon means to distinguish surveillance’s “primitive form,” which persisted until the 19th century, when it took its modern form. This thesis will be further expounded in the following chapter.

purpose of surveillance has changed); “hierarchy” refers to who is the watcher and who is
watched; “targets” refers to the physical nature of those monitored (i.e. whether they are people
or other things); “agents” asks the similar question about the conductors, alluding to automated
versus human modes of surveillance; finally, “dynamics refer to the interactions between the
watcher and the watched (e.g. cognizance of the person being watched, as well as her active
resistance).

The above methodology is fundamentally structuralist, which deviates from the
traditionally narrative approach undertaken by historians. In such a case, the above components
of the “surveillant assemblage” are held as independent variables, while the qualities or
relationships of the components to individuals or privacy are determined dependent variables.13
To examine their ability to answer and hone in on the above claims, we can once again turn to
the narrative of Mr. Glass. From a structuralist perspective, the three cases each illustrate distinct
yet central components of both Haggerty’s metric and surveillance studies throughout history.
The Apple case orients itself around capacity, focusing on the technical structures of government
surveillance and their physical abilities to surveil. The Schrems case focuses on actors, and asks,
“Whom can governments conduct surveillance on? How different are other governments’
surveillance regimes? Is international harmonization required in a globalized world?” The Jones
case explores methods and constraints along with boundaries of public and private, asking, “How
does a government conduct surveillance? For how long can the government surveil with
legitimacy? At what time and extent must surveillance be curbed, even in public?”

12 I use “things” deliberately. See Chapter III in which I discuss the qualitative change in targets due to
the advent of the Internet of Things.
13 This term originates in Kevin D. Haggerty and Richard V. Ericson, "The Surveillant Assemblage" 51
British Journal of Sociology 4 (Routledge: December, 2000). I also do not mean to imply that individuals
lack agency and influence in creating the structures. For the purposes of this paper, however, individuals
are examined as reactive to the structures in which they exist (a rather Foucauldian assumption).
Taken together, these cases all ask one fundamental question that underpins the thematic focus of this thesis: *To what extent can governments surveil?* Rephrased, this question stays the same but touches on a separate academic body of scholarship: *To what extent do individuals have privacy from government surveillance?*

To systematically answer these questions, the thesis takes the following course. Chapter I explores theoretical and historiographical approaches to surveillance as well as the concept of privacy as a boundary of government surveillance. Chapters II and III subject Rome and the U.S., respectively, to the scrutiny of the theoretical models set up in Chapter I. The thesis concludes with a return to the original cases behind the narrative of Mr. Glass by superimposing and synthesizing them with the paper’s main case studies and subjecting them with renewed vigor to Haggerty’s metrics.
CHAPTER I: EYEING-OPTICONS

I. Cracking the Literature: The Academic Myopticon

Surveillance and privacy as academic disciplines are oddly disjointed. Modern surveillance theorists are largely composed of Anglosphere sociologists. Surveys of modern surveillance theorists typically root themselves in a triad of post-structuralist French philosophers such as Jean Baudrillard, Gilles Deleuze, and Félix Guattari. At the helm of surveillance theory sits Michel Foucault, whose groundbreaking book *Discipline and Punish* forms the cornerstone of surveillance structures: the panopticon. Other non-French philosophers contributing to surveillance theory include Giorgio Agamben, Karl Marx, and Max Weber.

Modern privacy scholarship integrates none of these academics or philosophical founders. Instead, privacy as an academic discipline typically comprises a cohort of legal scholars. This is likely because privacy is typically analyzed in rights-based rhetoric, which inherently entrenches itself in legal philosophy and scholarship. Arguably, privacy’s conception as a right was birthed in law with its most cited work written in a law review by two lawyers,

---


Samuel Warren and Louis Brandeis. Their article produced a number of academic offspring, interestingly situated around technological change. As Warren and Brandeis published their article in reaction to the development of the Kodak camera, one can see a correlation if not causation of privacy scholarship to technological advancement. The first batch of privacy scholars published seminal works on the right to privacy as computers increasingly began functioning as tools for administrative processing. After the normalization of computers in society firmly situated privacy in the information age, computers moved to networks and provided increased tools for surveillance. The following batch of scholars reflected on the policy implications of privacy and its legal manifestation in a networked world surrounding the advent of the clipper chip in 1993. The twenty-first century exponentially exploded technological advancement, causing a similar effect in academia by creating a more diffuse array of scholarship. At their root, the majority of privacy scholars point to John Locke, J.S. Mill, and Jean-Jacques Rousseau to justify the inherent presence of a “right to privacy” in Western democratic societies.
Granted, there are a few scholars that straddle the line of surveillance and privacy theories, methods, and philosophy. Canadian historian, legal scholar, and political scientist David Flaherty surfaces in surveys of both camps.\(^\text{23}\) His works range from comparative legal and technical analyses of privacy within surveillance mechanisms (e.g. 1979, 1985, 1989) to historical chronologies of privacy in a particular society (e.g. 1972). Julie Cohen, chiefly a privacy legal scholar, intertwines sociological and legal studies along with postmodernist and phenomenological theory in her analysis of privacy’s function in the processes of self-formation in networked societies.\(^\text{24}\) David Lyon, the aforementioned Canadian surveillance theorist, also pops up in privacy literature.\(^\text{25}\)

However, these scholars make up the lion’s share of the intersection between surveillance and privacy theories. While surveillance theorists mention privacy and privacy theorists mention surveillance, the camps rarely cite or critique each other’s literature or ideas. When they do, it seldom surpasses the brevity of a footnote.\(^\text{26}\) As a result, surveillance theorists tend to view both the philosophical and legal idea of privacy as a dependent variable, changing as a result of altered or expanded surveillance structures.\(^\text{27}\) Privacy theorists, on the other hand, often view

\(^\text{23}\) In the surveillance camp, David Lyon mentions two of Flaherty’s books (1986 and 2014) five times in *The Electronic Eye*. David Flaherty both self- and externally defines his current specialization in “privacy management,” and held the position of Information and Privacy Commissioner for the Province of British Columbia between 1993 and 1999.
\(^\text{26}\) E.g. Solove, *Conceptualizing Privacy*, p. 1130. Gary Marx, David Flaherty, and David Lyon each receive short parenthetical explications within footnote 247. However, in fairness to Solove, Flaherty is discussed further throughout the piece.
\(^\text{27}\) A paradigmatic example can be found in James Rule, *Private Lives and Public Surveillance* (Schocken, 1974). In a 358-page book that implies a contrast between the “private life” and “public surveillance,”
surveillance as the dependent variable that either changes or must change due to changing philosophical and legal notions of what constitutes privacy.

The next sections address each camp’s respective theories of surveillance and privacy. The final section attempts to merge their rather pigeonholed approaches around a more unified general philosophical framework by which they can speak to each other and together engage the objectives of the thesis’ case studies.

II. Theories of Surveillance from the Panopticon and Beyond

What is Surveillance?

Anthony Giddens’ defines government surveillance as “the symbolic material that can be stored by an agency or collectivity” to “mobilize administrative power...through the storage and control of information.”28 David Lyon expands upon Giddens’ definition to create two axes or processes of state surveillance. The first axis defines surveillance as the “accumulation of coded information,” resulting in the “internal pacification of nation-states.”29 The second axis, according to Lyon, refers to surveillance as “the direct monitoring of subordinates within the capitalistic workplace.”30 On the other side of the spectrum, privacy scholar Daniel Solove...
defines surveillance as “the watching, listening to, or recording of an individual’s activities.” Melding together Solove’s and Giddens’ definitions with Lyon’s axes, surveillance can be said to generally emphasize the collection of data. For the purposes of this paper, surveillance will be restricted to the government’s collection of its individuals’ data. Why do governments conduct surveillance?

Why Surveil?

David Lyon highlights three sociological traditions of surveillance imbued in Giddens’ axes (and absent in Solove’s definition) that emphasize the purpose of surveillance itself. The first is a Marxist conception of surveillance as an aspect of “the struggle between labor and capital.” Here, surveillance is used as a tool to enforce productivity and maintain class relations in a factory setting. The second is a Weberian revision of bureaucratic structuralism, emphasizing surveillance as a neutral means of organization in capitalistic society. In this case, surveillance expands from the factories of Marx to all capitalist organizations both public and private, distinguished by their “rationality.” Finally we turn to the Foucauldian tradition, which

---

32 Lyon, The Electronic Eye, 7.
33 As opposed to Marx’s vision of surveillance, which is inherently negative.
34 See Lyon, The Electronic Eye, 25. Essentially, Weber is saying that through mechanisms like double entry book-keeping, bureaucratic organizations could make data-driven decisions. This is in effect a quantitative-turned-qualitative change. It is not that the Romans were “irrational” or didn’t make data-driven decisions, but that they simply didn’t have the same amount of data. As a result, they had to make more subjectively biased decisions. From a structuralist perspective, however, it is ambiguous whether Romans – the progenitors of bureaucratic centralization – would have qualitatively different surveillance mechanisms in a Webers sense.

Weber does emphasize one more distinction – the impartiality aspect of “rational,” and this will make sense when looking at the governmental biases and discrimination within surveillance of the Romans. However, when moving into an examination of the pervasive racial and xenophobic structures within the US surveillance program, I leave it to the reader to assess whether such impartiality really exists in the modern day.
returns to a negative view of surveillance as a means of reinforcing traditional power (distinct from class) relationships.

**Mapping Historical Models of Surveillance**

The Foucauldian view of surveillance, called panopticism, is the focal point through which Lyon and others historically separate eras of surveillance. Panopticism marks the midway of three chronological baskets of surveillance regimes: primitive, modern and post-modern. The “primitive” form of surveillance lasted until the nineteenth century, vaguely characterized by “traditional methods of brutal public punishment” and a lack of centralized record keeping.\(^{35}\) However, this notion of primitive surveillance – wrapped up in rudimentary forms of watching and savage punishment – is about the extent of academic rigor that scholars give to this “primitive” era. Indeed, primitive surveillance is defined more by a qualitative lack in the characteristics of its subsequent iterations. According to Lyon, the shift from primitive to modern was mainly quantitative: the state was able to collect larger files of information on individuals and better process the data; information flowed quicker and to a greater degree than before; finally, the state itself consolidated in administration and in the growth of towns and cities.\(^{36}\)

---

\(^{35}\) Lyon, *The Electronic Eye*, pp. 7, 24, 29.

\(^{36}\) Ibid, pp. 24, 38. Few scholars mention the concept of a “primitive” surveillance model. Most (similar to privacy scholarship beginning with Warren & Brandies) begin with the panopticon and branch out from there. As a result, little besides Lyon’s brief model can show what “primitive surveillance looks like.
Out of these quantitative shifts sprung a qualitative change in surveillance: namely, the possibility of a panoptic - or total surveillance - state. Foucault charted the implications of this possibility through the visual representation of Jeremy Bentham’s panopticon. Bentham’s architectural prison model envisioned a coliseum-like building separated on the edges into individual cells. These cells would have glass walls facing the center of the circle. In the center would stand a large tower, within which a guard could observe while remaining imperceptible to those outside. Bentham marveled at the societal implications of his own design: “Morals reformed—health preserved—industry invigorated—instruction diffused—public burthens lightened—Economy seated, as it were, upon a rock—the Gordian knot of the Poor-Laws not cut, but untied—all by a simple idea in Architecture!”

There are a number of qualitative shifts representative of the panopticon in the “modern world.” First, panoptic surveillance became routine and systematic, based on individuation, self-regulation, and bureaucratic organization. Second, it had either a perfect (Foucault) or converse (Rhodes) impact on the individual psyche. In Lorna Rhodes’ case study of the ‘supermax’ prison, the “calculated manipulation” of both body and mind by completely eliminating the perception of privacy did not create “docile bodies” but resulted in its exact opposite. Third, Lyon emphasizes that the panopticon arose and functions in democratic societies; the tools of

---

37 The Bentham Project. "The Bentham Papers" (University College London).
individual domination are not simply imposed on the individual but often self-imposed and self-perpetuated.\footnote{Lyon, \textit{The Electronic Eye}, 24.}

Alongside the Foucauldian panoptic investigation of the prison lies another panoptic vision: the Orwellian totalitarian state of \textit{1984}. Similarities between the two subthemes include the idea of surveillance as a negative phenomenon connected to coercion, repression, discipline, power, and domination of one group towards another through the perception of an unblinking eye.\footnote{Allmer, \textit{Critical Studies in Surveillance Theory}, 578.} Power also tends to be centralized (via the single central tower and the single state apparatus). However, while the panopticon targets all members within the prison, “Big Brother” only does so for the top two social classes (fifteen percent of the population).\footnote{See Orwell p. 60 in which he mentions that surveillance did not target the Proles, which constituted 85\% of the population. This feature is emphasized in Stanley Cohen, \textit{Visions of Social Control} (Wiley, 1991), p. 142, and in Lyon, \textit{The Electronic Eye}, 61.}

The years following the publication of \textit{Discipline and Punish} saw the increase of new technologies and tools of watching, leading to the phenomenon of post-modern surveillance theory. Post-panopticism increases pervasiveness but becomes a neutral phenomenon, often decentralized through private sector and even individual abilities to surveil. Kevin Haggerty offers a convincing argument for the changed notions of surveillance, in which he uses his five metrics to distinguish panoptic from post-panoptic society. First, the panopticon is no longer fit for purpose. While the panopticon intended to centralize, automate, and solidify power relations between the watcher and the watched, we now use surveillance for alternative notions such as child-rearing, health promotion, and entertainment.\footnote{Haggerty, \textit{Tear Down the Walls}, 28.} Second, the hierarchies of surveillance are different: while the panopticon focuses marginalized or dangerous groups under its lens, post-modern surveillance now scrutinizes all members and often focuses more on the powerful.

\begin{footnotesize}
\begin{enumerate}
\item Lyon, \textit{The Electronic Eye}, 24.
\item See Orwell p. 60 in which he mentions that surveillance did not target the Proles, which constituted 85\% of the population. This feature is emphasized in Stanley Cohen, \textit{Visions of Social Control} (Wiley, 1991), p. 142, and in Lyon, \textit{The Electronic Eye}, 61.
\item Haggerty, \textit{Tear Down the Walls}, 28.
\end{enumerate}
\end{footnotesize}
members of society, from celebrities to politicians.\footnote{Ibid, 29-30.} Third, whereas the targets of panoptic surveillance concern themselves exclusively with people, post-panopticism often focuses on information technologies.\footnote{Ibid, 32. Common examples include automated processes that follow the stock market, or gauges that track oil flow in a pipeline and send the information back to a central hub. Mechanisms of targeted advertising such as clicks, cookies, or web site visitations are more ambiguous processes. On the one hand they do not physically track humans, but at the same time that is the goal - panoptic indeed.} Fourth, the agents of surveillance are no longer humans but often automated processes. While Foucault would emphasize that the point is not who is in the tower but the belief that someone is in the tower, Haggerty argues that humans may act very different under the belief that a computer is watching them instead of a human.\footnote{Ibid, 33.} Finally, Haggerty asserts that Foucault left out the dynamics of surveillance – the political element so pervasive in modern debate, and the visibility element by which we often have little realization that we are even being watched.\footnote{Ibid, 35.}

Indeed, in the post-Snowden age the number of –opticons governing society seems to have metastasized. Through reality TV shows and People magazine we engage in the synopticon, in which the masses control the microscope. Governments and people even outsource surveillance to companies, turning ‘Big Brother’ into many ‘Little Brothers.’\footnote{Dobson, Jerome E, and Peter Fisher. "The Panopticon's Changing Geography." 97 The Geographical Review 3 (American Geographical Society, July 2007), p. 311.} By following a few processes (companies) or people (intelligence agencies), entities often choose the oligopticon, which hampers breadth for gains in clarity and depth.\footnote{I.e. rather than spread your resources across a city, one could concentrate them on a particular community.} In the end, however, it
seems that in the current day these oligopticons interconnect through a system of networks, creating a dispersed yet total form of surveillance: a *super-panopticon* or *omniopticon.*\(^{50}\)

Surveillance theorists typically begin and end their discussions with a return to Foucault’s panopticon. When engaging in this theoretical and typically temporal debate during which a particular case is scrutinized, surveillance theorists have aligned themselves along a binary, either offering support to the panoptic theory of surveillance or espousing a post-panoptic theory.\(^{51}\) Where do our cases align? Do they really fall under the primitivism of the ‘neither’ category? Before we can answer these questions, we must first examine the boundary of surveillance over the individual: privacy. As we shall see, this boundary proves the limiting factor in a technologically-enabled world, restricting the prying eye of the panopticon, the oligopticon, the synopticon, and the omniopticon.

**III. Lidding the Eye: Privacy as a Boundary of Surveillance**

Before justifying the use of privacy as a boundary of surveillance, particularly when using a wide breadth of historical case studies, one must first establish that privacy exists. This section first grapples with privacy’s existential debate, justifying the idea of privacy as an applicable metric for the purposes of this historical study. Then it delves into the definitional debate of *what* privacy is, which proves a particularly contentious and nebulous topic depending on time period, culture, and philosophical background. Third, with definitional tools in hand, it

---


\(^{51}\) I will refrain from making a structural determinist pun whereby biopticism inherently leads to theoretical binaries, so the reader will simply have to imagine.
surveys the scant historiographical scholarship surrounding privacy to further situate the forthcoming case studies and justify their applicability in this study.

Privacy Is

Surveillance has the luxury and detriment of being more or less blatant. One can count CCTV cameras, discover wiretaps, unfurl massive data collection programs and immediately decry, “that’s surveillance!” Privacy, on the other hand, has at most been upheld by the United States as a “penumbral right” and at least been deemed nonexistent. The legal controversy is that when such violations occur throughout history, they are typically defended or rejected with words other than “privacy,” which in its written form does not exist in the U.S. Constitution. This absence hampers attempts to justify privacy’s legal application through stare decisis, and this further divides privacy’s affirmed or rejected existence into two legal philosophies: originalism and intuitionism. An intuitionist sees privacy’s implicit embodiment in existing Constitutional provisions and would hesitate less to make such a ruling, particularly if cultural or

---

52 Both claims originate in Griswold v. Connecticut 381 US 479 (1965). Justice Douglas, writing for the majority, parsed out privacy in the “penumbras” of the First Amendment (specifically association), the Third and Fourth Amendments (privacy of one’s personal property), and the Fifth Amendment (self-incrimination, which we will see argued in Chapter IV when returning to the Apple v. FBI case). To justify this penumbral justification, he cites the Ninth Amendment, which declares those rights afforded in the Bill of Rights non-exhaustive (for the above arguments, see U.S. 483–485). Justice Black, dissenting, writes, “The Court talks about a constitutional ‘right of privacy’ as though there is some constitutional provision or provisions forbidding any law ever to be passed which might abridge the ‘privacy’ of individuals. But there is not” (U.S. 508).

53 Latin: “to stand by that which is decided.” Judges are expected to follow the doctrine of precedent and uphold the principles laid down by previous decisions unless the context has fundamentally changed such that it is no longer just to do so.

54 Also referred to loosely as strict constructionism versus interpretivism. Justice Scalia, in his book A Matter of Interpretation, said, “I am not a strict constructionist, and no one ought to be.” Instead, he calls himself a “textualist.” Robert Bork has been accused of strict constructionism but claimed to be an “originalist” in a 2003 interview with Peter Robinson. For the purposes of this paper and for the discussion on privacy, I will classify them as originalists and leave the nuance for this footnote. The reason being that their stances on privacy, from Black to Bork to Scalia, all rest on strikingly similar jurisprudential reasoning and end in the same spot with regards to privacy.
technological change had made such a defense imperative.\footnote{Paragons of intuitivist legal reasoning can be found in the majority opinions of \textit{Griswold v. Connecticut} (see fn 49) and \textit{Roe v. Wade}, in the concurring opinions of Sotomayor and Alito in \textit{U.S. v. Jones} (2012), and in the dissenting opinion of Justice Brandeis in \textit{Olmstead v. U.S.} (1928).} An originalist could arrive at a similar conclusion (e.g. Scalia in \textit{U.S. v. Jones}) but through jurisprudence entrenched in more explicit constitutional protections (e.g. trespass instead of privacy). Robert Bork, a famous originalist and former U.S. Attorney General, notes that a lot of the unsound reasoning for privacy’s existence as a right stems from historical bastardization. In a small attack on \textit{Roe v. Wade}, he says:

> What you get in [the majority opinion] is a history of abortion in the Egyptian days. You get history of abortion under English common law. You learn about the attitudes of the American Medical Association towards abortion. You learn all these things. All of a sudden, he says there is a right of privacy and it's broad enough to cover abortion and that's it.\footnote{Robert Bork, interview by Peter Robinson. "Robert's Rules of Order: A Conversation with Robert Bork." \textit{Uncommon Knowledge}. The Hoover Institution, (July 16, 2003).}

With this historiographical admonition in mind, does a right to privacy really exist? Did it?

Bork’s diatribe may indeed caution against historical non-sequiturs and contextual fallacies, but it may prove a graver error to claim privacy’s absence as a right simply because it was not defined in consistent semantics. Millennia-old Talmudic law provides for an “injury caused by seeing” (in Hebrew, \textit{Hezzeq Re’iyah}) where “even the smallest intrusion into private space by the unwanted gaze causes damage, because the injury caused by seeing cannot be measured.”\footnote{This quote is the epigraph of Jeffrey Rosen’s \textit{The Unwanted Gaze}.} One of the most foundational tenets in the practice and scholarship of medicine, the Hippocratic Oath, incorporates a pledge of privacy from 400 BC: “And about whatever I may see or hear in treatment, or even without treatment, in the life of human beings - things that shouldn’t ever be blurted out outside - I will remain silent, holding such things to be unutterable [sacred,
not to be divulged].” 58 David Flaherty, in response to attacks on the existence of privacy, commented:

There is no sentient being in the Western world who has little or no regard for his or her personal privacy; those who would attempt such claims cannot withstand even a few minutes’ questioning about intimate aspects of their lives without capitulating to the intrusiveness of certain subject matters. 59

But Bork does make an important point, one that rings true far more among privacy scholarship than in surveillance studies. His admonition does not attempt to take on privacy as a desired value, nor does he attempt to deny its past existence in various legal forms. Instead, he warns against the danger of committing a fallacy of equivocation by using privacy as an ambiguous term to provide umbrella protections for unique “rights” that may not exist. 60 At the heart of every fallacy of equivocation lies definitional ambiguity, and it is to this we now turn. If we agree that privacy is, then what is it?

What We Talk About When We Talk About Privacy

Writing about the state of privacy in 1956, Circuit Judge John Biggs called it “a haystack in a hurricane.” 61 Indeed, the number of definitions and scope given to the term “privacy” has begun to follow Moore’s law: with every advancement in technology, the number increases

---

58 Hippocratic Oath, quoted in Nissenbaum, Privacy as Contextual Integrity, 146.
60 Take the Fourth Amendment and Griswold v. Connecticut as an example. Bork, Justice Black, and other originalists argue that when the Framers penned it, they referred specifically to privacy of one’s home, office, and effects in these places from government searches or seizures. Abortion is a completely different issue, and while perhaps it is a matter of bodily privacy, it would be stretching the Fourth Amendment to cover something the Framers did not intend. Such a matter of law-creation is for the legislative branch to deal with, not the judicial. However, it’s easy to say that both fall under some nebulous “privacy” right.
exponentially. Until the turn of the twentieth century, privacy rights were predominately attached to property. Then, in 1890, Warren and Brandeis demanded the inclusion of personal information to the right to privacy. Seventy years later, William Prosser synthesized Warren and Brandeis to separate privacy into four distinct interests. In 2006, Daniel Solove determined that four were simply not enough to refer to privacy in the information age, and consequently developed a taxonomy of sixteen distinct embodiments. In 2011, Benjamin Wittes observed that ‘privacy’ had become so convoluted that we no longer have any idea what we want when we demand it from our government and the governments of other states. Instead, he proposes a semantic shift away from the “unsalvageable” notion of privacy in the information age, to “a right against the unjustified deployment of user data in a fashion adverse to the user's interests, a right, we might say, against databuse.”

Wittes and Bork may be right that ‘privacy’ has become amoebic and uncontainable under a single form. Dan Solove, who has arguably done the most work on parsing out the many forms privacy in the past decade, claims that the many shortcomings and revisions to each definition of privacy stems from the fact that they attempt to derive a core essence, when privacy

---

62 Moore’s law, attributed to Gordon Moore in 1965, is a rule of thumb common to computer scientists and developers. It proposes that the number of transistors in an integrated circuit doubles approximately every two years.
in fact has none. Instead, privacy should be approached as one would approach making a biological taxonomy. Privacy is an “animal” and its physical manifestations are but species.

**Surveilling Species of Privacy**

So what species of privacy are there? The classic definition of privacy, coined by Samuel Warren and Louis Brandeis in 1890, is “the right to be let alone.” This particular piece of work is to privacy scholars as Foucault’s panopticon is to surveillance studies. One rarely sees an article about privacy – in America or Europe – without referencing Warren and Brandeis. Typically most scholars cite Warren & Brandeis to pay tribute to its novelty, but the more recent zeitgeist over the past few decades seems to criticize it for vagueness and irrelevancy. While the historical context of this article will be left for the U.S. case study, the definition itself can be lumped into what Solove calls a “harms-based” notion of privacy. Warren & Brandeis, using the publication of personal pictures by yellow journalists as the locus of their diatribe, claimed that one could cause harm to someone without physically intruding on their property. This harm was to a person’s honor, dignity, or “inviolable personality” by publishing material that would

---

68 Solove, in *Conceptualizing Privacy*, divides prevailing theories of privacy into six different categories, eventually dismissing all of them because of the vagueness or narrowness that results from attempting to assert a core catch-all definition for privacy.


72 Whitman, for example, criticizes both the value and novelty of the article: “[I]t is best not to think of the Warren and Brandeis tort not as a great American innovation, but as an unsuccessful continental transplant” (*Two Western Cultures of Privacy*, 1204). Priscilla Regan adds that privacy as ‘the right to be let alone’ “draws attention to the possible reasons why an individual might want to be let alone” (*Legislating Privacy*, 215). Solove criticizes it for being too vague and narrow a definition: “If you shove me, you are not leaving me alone. You may be harming me, but it is not a problem of privacy” (*Conceptualizing Privacy*, 9).
misappropriate or abuse their public identity.\textsuperscript{73} When distinguishing privacy from property, Warren & Brandeis say, “the principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality.”\textsuperscript{74} Note, however, that the harm done is upon publication, not on the very act of watching. Warren & Brandeis did not attack the single act of taking pictures of people, but instead the publication of those pictures in an unauthorized manner that would unjustly harm the person whose picture was taken.

Ben Wittes and Richard Posner offer similar contemporary notions of harm and the boundary of surveillance and privacy. As Warren and Brandeis argued that the harm was done on publication, Wittes argues that harm is done when information is used in a “fashion adverse to the [owner’s] interests.”\textsuperscript{75} In other words, our privacy is not invaded (or at least we do not care about its invasion) when our personal information is used, but rather when it is used against us.\textsuperscript{76} Posner agrees but adds a slight nuance: “[W]hen people today decry lack of privacy, what they want, I think, is mainly something quite different from seclusion; they want more power to conceal information about themselves that others might use to their disadvantage.”\textsuperscript{77} If privacy is

\textsuperscript{73} Warren and Brandeis, The Right to Privacy, 205.
\textsuperscript{74} Ibid. The vagueness that proves most vexing in the modern day may be the ambiguity behind “publishing in any form.” If the government looks at my emails without releasing it to the world, is this a form of publication to Warren & Brandeis? We will return to this dilemma in Chapter III.
\textsuperscript{75} Wittes, Database: Digital Privacy in the Mosaic (2011).
\textsuperscript{76} Here Wittes also expands the scope of privacy’s violation outside tort law. When Warren and Brandeis wrote The Right to Privacy, their attack was on the lack of protections from individuals and private slander. They refrained from mentioning government surveillance, and their use of the word “publication” refers specifically to civil, not constitutional, disputes.
the ability to conceal information, or the ability to keep things secret, then it is invaded

“whenever private information is obtained against [the person’s] wishes.”78

So far, Warren & Brandeis, Wittes, and Posner all offer control-oriented views of
privacy, whereby the harm caused by surveillance is in the removal of the individual’s autonomy
over portraying himself as he wishes to society. Wiretapping, eavesdropping, or taking pictures
does no harm unless it is published or used against the individual. With respect to government
surveillance, the individual should not mind surveillance if he has “nothing to hide,” i.e. nothing
that can be used to harm him or his dignity. Such a view is ends-based: “The government can
look at my data all it wants. Only when they use it against me will I throw my hands up and
decry a rights violation.” However, two very different species of privacy offer a more restrictive
idea of government surveillance. To examine these, let us return to two previously mentioned
notions of privacy, the Talmudic Hezek Re’iyyah and the Hippocratic Oath.

The Talmudic “injury caused by seeing” offers a rather unique take on the harms-based
approach by implying that harm may be done to a person simply by the person’s knowledge of
being watched. Like Winston Smith in 1984, a person’s actions and eventually the subconscious
development of the self changes with the constant knowledge of potential surveillance.
Philosopher Stanley Benn agrees with this surveillance-as-existential-harm notion, adding a
Sartrean flavor of object conscientiousness to the argument. In Privacy, Freedom, and Respect
for Persons, he states, “an object of scrutiny, as the focus of another’s attention, brings one to a
new consciousness of oneself, as something seen through another’s eyes.”79 In short, this view
links privacy directly to the development to the self and the preservation of one’s personhood.

78 Posner, The Economics of Justice, 46, in Solove, Conceptualizing Privacy, 1105.
79 Stanley I. Benn, “Privacy, Freedom, and Respect for Persons” in Conceptualizing Privacy, ed. Daniel
Solove, p. 1116.
Privacy’s degradation through even the perception of government surveillance (even without its actualization) would inhibit the very essence of personal self-development.

The Hippocratic Oath differs from the Hezek Re’iyyah by delineating the boundary between surveillance and privacy in terms of relationship. Helen Nissenbaum calls this view of privacy “contextual integrity,” and defines a privacy harm as such:

[W]hether a particular action is determined a violation of privacy is a function of several variables, including the nature of the situation, or context; the nature of the information in relation to that context; the roles of agents receiving information; their relationships to information subjects; what terms the information is shared by the subject; and the terms of further dissemination.\textsuperscript{80}

In essence, we expect certain facets of society to know certain aspects of our lives, and to divulge or withhold that information in different ways. If I have cancer, I will tell a doctor and divulge my medical history to him along with other personal information. That information is no longer “private” in the sense that it is privy only to me, but my privacy is still violated if the doctor discloses that information to other people. At the same time, the doctor has no reason to know my financial information, and if my accountant tells him then my accountant has also violated my privacy. Personal information, then, is always “tagged with context” that governs the acceptability of its disclosure to others across different spheres of societal relation.\textsuperscript{81}

This notion aligns with a form of privacy-related jurisprudence called the “reasonable expectation of privacy” test. Adopted in \textit{Katz v. United States} and used in privacy cases since, the test aims to establish whether the individual was justified in expecting privacy in the context

\textsuperscript{80} Nissenbaum, \textit{Privacy As Contextual Integrity}, 138.
\textsuperscript{81} Ibid, 143. Nissenbaum uses Michael Walzer’s “spheres of justice” metaphor to model society. Essentially, each individual has a baseline of social goods. Society is coordinated into different spheres defined by a specific social good internal to them (140). Each sphere has its own order of preferences and standards, and people and skills are ranked differently according to these rules (141).
of the situation at hand. However, as Nissenbaum points out, these norms of contextual integrity are relative and non-universal. Whether I expect my doctors to abide by the Hippocratic Oath depends on a number of cultural or temporal factors. Similarly, whether I expect my government to engage in constant surveillance through ubiquitous CCTV cameras depends on whether I live in the United States (the answer would be no) or the United Kingdom (the answer would be yes).

Nissenbaum’s privacy-as-contextual-integrity model is likely the most accurate approach to privacy due to its historical and cultural sensitivity. Following Solove’s definitional warning, she offers less a definition of privacy than an approach to defining it in particular case studies. However, when looking at our case studies for privacy as a boundary of surveillance, we cannot use Nissenbaum as a differentiating factor but rather as a toolbox to assess differentiation. Like Haggerty’s metrics for assessing surveillance system shifts, Nissenbaum offers similar metrics for evaluating privacy in a contextual model.

But now we run into another problem: if privacy is so nebulous that we cannot truly define it and barely come up with an approach for defining it across history, then how do we write histories of privacy, even with the concrete context of privacy as a boundary of government surveillance? Before leaving the privacy myopticon and merging it with the surveillance

82 In *Katz v. US* (1964), a person was found to have a reasonable expectation of privacy from government wiretap, even in a public phone booth. In *Smith v. Maryland* (1979), the use of pen registers or trap-and-trace devices were ruled not invasive because a person had no reasonable expectation to think that his telephone metadata was private – how else would a phone company be able to bill him other than to see where and to whom he was calling? Nissenbaum would likely disagree with this latter ruling by distinguishing the government’s relationship with the individual from the telephone company’s relationship with the individual, which the court neglects to do.

83 For a study of this particular example, see Paul Schwartz, “German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance,” 54 Hastings Law Journal 751 (2002).

84 We cannot use her as a differentiating factor in the sense that we cannot claim, for example, a qualitative shift of Roman to Genevan perceptions of privacy as a shift from a contextual integrity view to a “right to be let alone” view. We can, however, say there was a qualitative shift from a privacy-as-personality view (Talmudic) to a privacy-as-misuse (Wittes) view.
myopticon, we must first explore the historiography of how scholars write historically about privacy. David Lyon observes that surveillance is bounded through privacy legislation, and privacy has historically developed similarly through law. Thus the following historiography restricts itself to privacy’s legal history.

*From Definitional Ambiguities to Legal Ambiguities: Privacy’s Historiography*

When people trace privacy in law as relevant to modern constitutions, how far back do they go? Legal historiography on privacy is unfortunately as diffuse as the definition for privacy itself. Some begin their histories of American privacy law in 1890 with Warren & Brandeis. Others begin in the 1760s with the British common law cases of Wilkes and Entick. Others still see privacy in America molded from the Greeks, Romans, the Reformation, or the Puritans in the early 17th century.

Picking a starting point for a history of privacy in law is not as arbitrary as it may seem: scholars appear to choose their starting point depending on the type of legal argument they wish to make and the type of legal philosophy they adhere to. For example, Alan Westin, in his seminal work *Privacy and Freedom* argues privacy as a primordial right attached to man. Such an argument would do well to link privacy rights to events as early as possible. As such, Westin

---

begins his journey by examining animal behavior and starts his institutional analysis with the Ancient Greeks.\textsuperscript{90} Whitman, in \textit{Two Western Conceptions of Privacy}, looks at the cultural and historical influences that factor into current stances on privacy in France, Germany and the US. He too starts with Western privacy law (the Greeks) and sees Warren & Brandeis as a continuation of earlier 19\textsuperscript{th} century French privacy developments. Lusky, on the other hand, espouses an entirely different notion of privacy, one that requires scrapping old antiquated definitions in favor of new paradigms tailored to societal needs.\textsuperscript{91} With a view that understandings of even foundational legal principles must mutate as the setting changes, Lusky begins his discussion of privacy law one hundred years after the framers in an overarching attempt to discard antiquated notions and rebuild anew.\textsuperscript{92}

Lusky’s shallow historiographical approach (or lack thereof) makes sense in pragmatic terms, and is particularly tempting to use when formulating policy on current topics such as data privacy as a fundamental right. The confusion and resulting domestic and international tensions over privacy arise chiefly from this attachment to past triggers related to the word ‘privacy’, and a failure to commonly define privacy and recognize the change in its very meaning over time and space. Privacy is in desperate need of a semantic and legal overhaul, one that would perhaps fare better by scrapping the term and starting anew with a wholly different word. As pundits, politicians, and plebeians alike decry their loss of “privacy” in the digital age, it is exceedingly difficult to know whether they lament their loss of Brandeis’ privacy, Westin’s privacy, Solove’s

\textsuperscript{90} Alan Westin, “The Origins of Modern Claims to Privacy,” from \textit{Privacy and Freedom} (1967), pp. 1, 70.
\textsuperscript{91} “[Privacy] needs a forward leap…a fresh and more exact rationalization than Westin accomplished” (1972, p. 695).
\textsuperscript{92} I do not mean to paint Lusky as one who sees absolutely no value in history. In his concluding remarks, he states that the development of a useful lexicon on privacy “will not involve the scrapping of good work that has already been done by Westin and his followers, any more than Einstein scrapped the work of Newton” (710).
privacy, or Wittes’ *database* (to name but a few disparate definitions). When the U.S. and EU call for policy reforms on data privacy, how is one to know whether the EU perceives privacy as “dignity”, “personality”, “property”, or otherwise?\(^93\) Perhaps an awareness of the historical evolution of the word serves to confound and entitle rather than clarify.

At this point I echo Lusky’s philosophical lamentation but deviate from his method of approach and thereby his historical point of origin. While Lusky aptly recognizes that keeping a word attached to old or vague definitions can deteriorate the relevance and applicability of the word in the present day, he shies from probing into the origins of the vagueness to pull out a sense of clarity.\(^94\) If my own and Nissenbaum’s historiographical methodology (of which she has yet to write) had to be categorized in one of the above clusters, it would sidestep Lusky and take the route of Whitman, et al.

Extricating myself from the three paradigms, my own philosophical inclinations and approach regarding historiography take a more Derridean form. When Derrida tackled the concept of brotherhood during the advent of Christianity in *Politiques de l’amitié*, he noted the imperative to constantly refer back to the Aristotelian and Platonic notions of brotherhood in Greece.\(^95\) In his own words,

> The way the Christian concept of brotherhood transformed the concept of brotherhood was at the same time…an inauguration, a mutation, a break…[and] we have to go back to

\(^93\) Each interpretation derives from a different point during the evolution of privacy; at each point in time a different translation was stressed. See Whitman (2004), pp. 1161, 1173, and 1185.

\(^94\) One particular example involves his investigation into Westin’s notion of privacy as a “claim” versus Arthur Miller’s notion of privacy as a “right” (1972, 708-9). Lusky deconstructs and scraps both terms, suggesting “condition” as an alternative (709). However, by proposing an alternative word with intentionally less legal onus, he rejects the trajectory of hundreds of years of political theory and case law (not to mention political climate during the 1960s) that all move towards the development of privacy as some form of right, thereby requiring some form of legal assessment.

the Greek origin, not to cultivate the origin, or in order to protect the etymology, the philological purity of the origin, but in order first to understand where we come from.\(^9\)

Therefore, in order to understand the contemporary conversation on privacy, one must understand the origins of the debate, particularly on the broader topic of privacy law. From this we can analyze precisely the fissures between privacy law in physical and cyberspace, and gain a better understanding of why privacy as a legal concept has become so elusive. Furthermore we can analyze disparities and commonalities to determine which laws and surveillance structures remain the same and which need alteration. Will we be able to find a privacy from government in pre-modern times as Lyon denies?

Yes we will; but before we do so, we must establish working definitions and theoretical assumptions to privacy and surveillance, along with their values within the context of government surveillance. As it stands, we still have no definition for privacy, no clear-cut historiographical model for parsing out its relation to surveillance, and no comparison or intermixing between surveillance and privacy scholarship. The final section before embarking on the case studies will synthesize these esoteric sets of ideas and create a unique model of approach based on both academic disciplines.

IV. Widening the Philosophical Aperture

Establishing Theoretical Assumptions

As previously mentioned, privacy and surveillance theorists tend to ground their literature in different philosophical foundations, and further fail to define each other’s (or often their own) terms. It is to these differing philosophies and definitions that I will now discard and then

reassemble to establish a common medium to create a theoretical link between the two disciplines.

As it stands we have no working definitions for either privacy or surveillance. We will establish these and their relationship by examining a set of descriptive premises that I assert are intrinsic to both, working from the theories given in the previous sections. I contend that the link between the two terms rests in the underlying tenets of the relationship between government and society, which reside (in Western democracies) in social contract theory. I pose the following theoretical assumptions to intertwine our academic silos:

1. **Privacy and surveillance only occur in social systems.** If there is nothing and no one to hide from, one does not have privacy. At the same time, one cannot conduct surveillance without an “other” to watch.  

2. **Privacy and surveillance are dipoles within the social system.** For example, note the extremes: a system with 100% surveillance inherently has 0% privacy. Likewise, a perfectly private system would be one with no capacity for surveillance.

3. **Social systems require social contracts:** Social contracts are established to build a third party system to protect a body of rights. A number of these rights are reduced from what they were, but certain core elements or rights – those to which the contract was established to

---

97 To assert that surveillance occurs in a social system is rather obvious and self-justifying. Each theory and author unambiguously takes this as a premise. Privacy is slightly more obscure, so let us regard this premise in relation to each of our definitions: The right to be “let alone” implies something from which to be left alone. The misuse of data and “nothing to hide” arguments imply an “other” to misuse the data or cause harm to the individual through defamation etc. The existential (or Talmudic, shall we say) thesis asserts that self-development exists in relation to one’s existence in society. Julie Cohen, a proponent of this thesis, contends that the individual is a “situated subject” whose subjective self evolves from the interaction between the individual and the cultural context of the society in which she lives (see *Configuring the Networked Self*, 2014).
protect – cannot be relinquished without overthrow. These rights are called “fundamental,” or “inalienable.”

4. Fundamental rights are inherent to man: fundamental rights, such as those granted in the Constitution, are akin to natural rights in that they are intrinsic to individuals prior to social contract formation; they do not suddenly spring up in the midst of a system. Such rights would simply be called rights. ‘Fundamental’ implies historical ubiquity of a tenet inherent to humans and requisite to their happiness, a property extrinsic to ‘culture’ or context of a social system.

*Balancing Privacy and Surveillance*

These four premises set the stage for analyzing privacy and surveillance in tandem within a social system. Privacy and surveillance still have no discrete definitions but rather, as Solove and Nissenbaum contend is only possible, a set of associations. Yet when discussing privacy as a boundary of surveillance, all our authors make the implicit assumption that privacy and surveillance represent the power relationship between the individual and government in a social contract. This does not necessarily mean that a gain in privacy results in a loss in the state’s

---

98 This draws directly from Locke’s *Second Treatise on Government*. My separation of “fundamental” and “inalienable” refers to the attempt to encompass both European and American terminologies. Europeans tend to use the former (see Article 8 of the European Convention on Human Rights) and Americans the latter (see the Declaration of Independence).

99 Lyon actually discourages the study of privacy as a boundary of surveillance because he fears that speaking of surveillance in terms of privacy would be to view privacy “as a means of countering [surveillance’s] unlimited spread” (*The Electronic Eye*, 189). In other words, using privacy as a means to critique surveillance. He says that Marxian and Foucauldian theorists would both admonish such a notion because it “detracts from the real issues at stake” (189). The former would say that it detracts from surveillance as a struggle between classes in capitalist society; the latter would say that it detracts from the fact that surveillance places individuals “in the grip of ubiquitous power” (189). However, I contend that these are merely species of surveillance that can only be viewed in the context of their cases – for example early 19th century factories or 1984. In the social contract, we are indeed situated in a realm of ubiquitous power, but that power is not solely monopolized by the government to control the individual but rather is balanced between the individual, the government, and other entities such as businesses. We
capacity to surveil, nor does it mean that privacy offers a single and positive value of utility while surveillance offers only negative utility to the individual. The entire purpose of couching the relationship in the social contract and through a “contextual integrity” approach to privacy denies such a black-and-white approach. Privacy and surveillance have many different species, to which different cultures allot different values. As Napoleon dictates in Orwell’s *Animal Farm*, “all animals are equal but some animals are more equal than others.”

Now we will move into our case studies with a conception of the species or theories of surveillance and privacy. As we examine Rome and America, we must be wary of the value of privacy from government surveillance, or the very existence of privacy at all. Is privacy truly a social good throughout history, and is it a “fundamental” right as defined in Premise 4? Did governments legally protect privacy, and if they did, through which definition of privacy did they use to protect it?

We also must keep tabs on the value of surveillance: is it negative, positive, constantly changing depending on cultural context? When our first two cases conducted surveillance on their citizens, did they do it according to Lyon’s primitive form of surveillance, i.e. “irrationally” without a centralized (or even decentralized) system of information collection and control?

Finally, on the macro scale, we must keep in mind our structural metrics. How do the purpose, hierarchies, dynamics, targets, and agents of surveillance change across our case studies?

---

see the same power dispersion across surveillance mechanisms – i.e. I relinquish my personal information to the potential harm of both the government and Google. Similarly, surveillance viewed as class struggle is only one of the ‘issues at stake’ in past and present society.
CHAPTER II: THE PANTHEON AND THE PANOPTICON

Introduction: The Panopticon's Primordial Root

Imagine you are on a trip to Rome. Self-respecting tourist that you are, you find time in your itinerary to visit the Pantheon. You approach from the Piazza Della Rotunda, situated directly outside the edifice. Looking at the building, your left eye glued to the viewfinder of your newly purchased Leica S Type (a necessity for the trip, half the price of the trip itself, but nonetheless an imperative addition), you spy a seven-story barrel of windowless concrete and reinforced brickwork. Zooming out, you look for the Pantheon. Perhaps you were expecting the ornate façade of the St. Peter’s Basilica, or the polychrome marble exterior of the Florentine Duomo. Either way, your Frommers guidebook did not prepare you for what can only be described as a glorified second century prison. You walk up the marble steps, hauled from the faraway colony of Numidia and assembled at your feet in AD 125 under the behest of Emperor Hadrian, and emerge on the portico, or entrance to the building. Here three aisles of Corinthian pillars stand sentry, monolithic bars across the solitary door into and out of the building.100

Passing through your entry and exit, you emerge in a circular room. It is vast and open, a great rotunda with nowhere to hide. Around the curved walls stands an assembly of gods to which the name of the structure harkens: pan (all) - theon (gods). As you raise your camera to finally snap some Instagrammable shots, you are thrown by the single band of light that asymmetrically favors the statue of Venus, shrouding the others in the contrast of its limelight. Luckily, your boy scout of a Leica has flash, and you artfully snap shots of Mercury and Mars.

100 The details of the following description of the Pantheon are indebted to William Lloyd MacDonald’s *The Pantheon: Design, Meaning, and Progeny* (Harvard University Press, 2002).
Indeed, the only natural source of light by which you can see is a gaping hole at the top of the domed ceiling, the oculus. If Jupiter were to look down at the Pantheon he might perceive it as an eye staring up at him. This monstrous eye would stand 142 feet in diameter with a 27-foot diameter iris. But you, rooted to a more terrestrial perspective, might see the oculus as an inverted microscope for the deities whose facsimiles stare at you from their alcoves etched into the walls.

The Pantheon, a Concrete-lidded Eyeball

Had you been a Roman citizen in the time of Hadrian, you might have watched the emperor speak here, a living deity at home among his stony peers. If the emperor was not present - and if Panini’s seventeenth century interpretation proves accurate - the open space of the Pantheon might be filled by crowds of Romans from all social strata, chatting and gossiping under the unblinking oculus.
Consider, for a moment, the panoptic qualities of the Pantheon. The all-seeing eye centers the structure, peering into the souls and conversations of the people within its gaze. The individual cannot see the watcher, nor can he know for certain that he is the focus of the gaze, but the statues and openness of the construction remind him that he cannot hide from the omnipotence, omniscience, and omnipresence of the entity symbolized by the oculus. Physical privacy from peers is nonexistent, and neither is mental privacy from the gods. Jeremy Bentham’s architectural blueprint of the panopticon, juxtaposed with the design of the pantheon, only amplifies their parallel qualities (see Appendix, Figures 1 and 2).
However, Foucault and Lyon would probably not be won over with shallow structural parallels of likely flawed surveillance metaphors. From a sociological standpoint, a huge difference in the mechanisms and dynamics of surveillance might lie in the fact that the panopticon is capped while the pantheon is not. One could argue that people act fundamentally different under the scruples of a deified watcher, and further that Roman society restricted such omniscience to a power more equipped and worthy. Bentham’s model, on the other hand, secularizes surveillance; the model uproots past principles and alters the watcher, hierarchies, and dynamics of the surveillance system.\textsuperscript{101} Such an argument, valid without a doubt, requires us to abandon the \textit{pantheopticon} for now and surveil Roman society itself during the second and third centuries. Outside the pantheon, how did Romans conduct and respond to surveillance?

**I. Building a Surveillance System: Structures of the Surveillance Assemblage**

For the emperor, maintaining order and security throughout the entirety of the Roman Empire presented a herculean task. By the second century, the four corners of the empire (in present-day terms) stretched its southern borders from central Morocco to southern Egypt, and its northern borders from the Scottish highlands to the perimeter of the Black Sea (see Appendix, \textit{Figure 3} for detailed map). Such breadth required heavy decentralization. Accordingly, the emperor divided his army into thirty legions of about 4,200 infantry and 300 cavalry each and deployed them across areas of particular instability, typically in the empire’s frontiers.\textsuperscript{102}

\textsuperscript{101} Lyon makes a similar argument when he describes the Panopticon as the “secular parody of divine omniscience” (\textit{Electronic Eye}, 63).

\textsuperscript{102} Adrian Goldsworthy, \textit{The Complete Roman Army} (Thames & Hudson, 2003), p.27. According to the picture in the appendix, approximately one third of the legions were deployed on the Eastern borders in
Coordinated decentralization required bureaucracy and a clearly delineated system of command and control. The Roman security apparatus was thus divided into three levels, with many subordinate hierarchies in between. On the imperial level, the emperor gave macro-level policies: these included decrees for the construction of a system of security stations on main roads (we will examine this later), for launching campaigns, and for setting general standards for troop operation and behavior throughout the empire. He also controlled a force of his own, called the praetorian guard. The second level of administration was provincial, in which law and order resided in the hands of a governor. They too had troops of their own, and were responsible for maintaining stability in their province and keeping up correspondence with the emperor. The third level involved outposted soldiers performing administrative and policing duties among civilian communities. They always reported to a superior, be it the governor or legion commander, but in practice they were only loosely supervised and often developed institutions of their own.

But even with a few hundred thousand legionnaires and just as many auxiliary troops, keeping watch over every community in the empire was impossible. The Romans had no officially instituted form of police officer, so communities over time became substantially self-regulated. Their abilities were typically sanctioned and loosely supervised by the provincial governor, but overall some form of self-regulation was necessary in a period without police, CCTV, or rapid transportation. How did mechanisms of surveillance differ and communicate between each level of society?

Judea, Syria, and Cappadocia. Another 15 legions were deployed on the northern European borders with Dacia, the Goths, and the Saxons. The final concentration (about 4 legions) was deployed in Britannia. During the rule of Hadrian there were around 56 provinces, with one governor each. See appendix. These three levels correspond with Christopher Fuhrmann’s levels of policing, in Christopher J. Fuhrmann, *Policing the Roman Empire* (New York: Oxford University Press, 2012), pp. 10-11.
Policing the Roman Polis

The English noun “police” borrows from the thirteenth-century French word ‘pollice’ meaning “regulation…administration of trades.” The French word, however, harkens to the Latin politia, meaning “civil order or organization,” which in turn is indebted to the Greek polis. City and police, then, originate in the same place. And it is to the largest of cities and police forces that we now turn. By AD 6, Augustus had ten thousand military personnel patrolling Rome, which corresponded to approximately one per one hundred inhabitants of the city. This ratio was indeed exceptional even for modern standards: at the turn of the nineteenth century Berlin and Paris each had a ratio of about one to 300, and Washington D.C. at the turn of the twenty-first century had one policeman for every 150 people.

However, these statistics may prove slightly misleading because Roman policemen did far more than police, and so they were not always agents of surveillance. The vigiles, for example, served as both night watchmen and firefighters. Cohorts urbanae are believed to have served as the traditional day-to-day policemen, although accounts by Romans and historians hardly distinguish between their function and that of the praetorian guard.

The police forces of provincial governors and local communities had to multitask far more. According to the Roman jurist Ulpian (d. 228 AD), the pacification of the province was the governor’s sole and primary responsibility. Justinian, whose Digest (also known as the

---

105 Oxford English Dictionary.
106 Fuhrmann, Policing the Roman Empire, 117. According to Fuhrmann (p.118) this ratio only increased with Augustus’ successors.
107 Ibid, 118.
108 Ibid, 117.
Pandects) catalogued Roman law nearly 400 years later, records Ulpian’s description of the governor’s duties:

A good and serious governor should see to it that the province he rules remains pacified and quiet. He will achieve this without difficulty if he earnestly pursues evil men and clears them from his province. For he must hunt out committers of sacrilege, bandits, kidnappers and thieves, punishing each in proportion to the crime he committed. He must also repress their abettors, without whom a bandit cannot lie hidden for long.¹¹⁰

One of the main ways the governor could ensure law and order with limited forces was to create a central locus of power and strong communication line with the local magistrate (aedile). He and his attendants (apparitores) served as rough equivalents to a standing local police force, and served enough functions to make a Swiss army knife look like a metal stick.¹¹¹ The municipal charter of Irni, an Iberian town near the larger colony of Urso, describes the multifaceted functions of the magistrate: “The aediles…are to have the right and power of managing the food supply, temples, sacred places, town, roads, districts, drains, baths, market…and of managing watches when occasion arises.”¹¹² From this constitution, we can see that not only did the magistrate control administration of essentially every public and commercial activity in his locality, he also had the ability to create potentially ad hoc watches depending on the level of perceived danger.

Was Irni unique? Granted, the Spanish colony during the Flavian era (the time in which the constitution was created) was known for being rather temperamental and could have thus required a more centralized locus of power and tailored constitution. Historian Peter Heather contends that the municipal charter of Irni is actually fairly representative of other municipal

¹¹⁰ Ulpian, Digests 1.18.13, in Fuhrmann 182. Recall Gidden’s first axis of surveillance: applied for the “internal pacification of nation-states,” and bound up with the growth of bureaucratic administration, defense, and policing. It seems his first axis hits the mark with Roman surveillance.
¹¹¹ Fuhrmann, Policing the Roman Empire, 58.
¹¹² Lex Irnitana (c. AD 91), in Furhman 55.
constitutions during the time. By comparing the constitution with tablet fragments from other areas, he concludes:

There was one basic constitution, composed in Rome, which all of these towns adopted, changing just a few of the details to suit their own circumstances. Amongst other things, the laws laid down who should qualify for the local council, and how the magistrates (here called duumviri, ‘two men’) should be chosen from it; which legal cases could be handled locally, and how financial affairs could be managed and audited. It was only such details as the number of councilors appointed that varied from place to place.\textsuperscript{113}

Heather’s findings drill home two points. First, local magistrates across the empire had an immense amount of power and duties; second, Heather reinforces the balance between a centralized top-down legal and administrative system, and highly decentralized modes of operation and implementation. As we delve deeper into how surveillance actually worked on the ground, we will see this concept of decentralized self-policing emphasized even further.

Why am I stressing this? What does this have to do with surveillance theories described in Chapter I? We will discuss this more in depth later, but while the groundwork is freshly laid and about to be further paved, recall two central claims made by renowned surveillance theorists. First, Gary Marx, describing the qualitative shift brought by the advent of the computer, said that computers fundamentally alter the nature of surveillance by allowing for “decentralized self-policing.”\textsuperscript{114} Second, Lyon (and others) crucially distinguishes primitive, panoptic, and post-panoptic surveillance theories as movements along an axis from no centralization (primitive) to centralization (panoptic) to decentralization (post-panoptic). Consider the validity of this model as we continue to pry into the apparently unorganized Roman surveillance regime.

\textit{Secret Services: Surveillance on the Ground}

\textsuperscript{113} Peter Heather, \textit{The Fall of the Roman Empire: A New History of Rome and the Barbarians} (New York: Oxford University Press, 2007), 39.
Despite the lack of cameras, telephones, or an institutionalized police force, surveillance in the Roman Empire was remarkably functional. Cassius Dio (d. 235 AD), a senator and historian of Rome, complained on behalf of the senate regarding the seemingly ubiquitous surveillance capacities of the Emperor Caracalla in his History:

He held court rarely or never, but devoted most of his leisure to gratifying his curiosity as much as anything. For people brought him word from everywhere of everything, even the most insignificant things; and he accordingly ordered that the soldiers who kept their ears and eyes open for these details should not be punished by anyone but himself. Nothing good came of this order, but rather another set of tyrants to terrorize us, — even these soldiers.\(^{115}\)

Caracalla, supposedly in response to the senators, wrote: “I know that my behavior does not please you; but that is the very reason that I have arms and soldiers, so that I may disregard what is said about me.”\(^{116}\)

How did Caracalla and others implement successful surveillance regimes? As we see from the above quote, emperors used soldiers (vigiles, the praetorian guard, or otherwise) to be on the constant lookout for suspicious characters as they patrolled the city. The vigiles were even known to act as undercover agents, to converse with civilians under false guise and root out potential rebellious characters. Epictetus (d. 135 AD), writing during the reign of Domitian, described this practice from the point of view of a civilian:

A soldier, dressed like a civilian, sits down by your side and begins to speak ill of Caesar, and then you, too, just as though you have received from him some guarantee of good faith in the fact that he began the abuse, tell likewise everything you think, and the next thing is – you are led off to prison in chains.\(^{117}\)

\(^{115}\) Cassius, Dio, The Roman History, (c. 220 AD), XVII. Trans. Loeb, Vol. IX (University of Chicago, 1927).
\(^{116}\) Cassius Dio, The Roman History, XX (Trans. Loeb).
\(^{117}\) Epictetus, Dissertationes (c. 89 AD), in Policing the Roman Empire, ed. Christopher Fuhrmann, p. 143.
We cannot be sure to what extent the *vigiles* were used as undercover police outside the reign of Domitian, but the use of informants and soldier-spies was relatively common across emperors and senators alike.

The most notorious, and perhaps interesting, of the soldier-spies were a class of soldier called the *frumentarii*. Their name derives from their original function as supply sergeants who distributed provisions of grain (*frumentum*) to troops. However, their use eventually evolved into the multi-purpose occupation of courier, tax collector, policeman, and provincial spy. Aurelius Victor, a politician and historian writing during the fourth century, stresses the latter function, noting that the *frumentarii* were predominately “instituted to search out and report on whatever disturbances were emerging in the provinces.” This function was particularly effective in the provinces because of the soldiers’ secondary roles as tax collectors and policemen, which allowed them to be justifiably more privy to private conversations and matters. But even in Rome itself, Hadrian was known to use *frumentarii* soldiers to “snoop into not only the affairs of his own household but even into the private lives of his friends.” William Sinnigen affirms Aurelius’ comment, emphasizing that their original use was to spy on the imperial court.

These “snoopers” provide crucial insight into the world of Roman surveillance, specifically a high (and timelessly pervasive) correlation between communication networks and surveillance. It seems not a matter of chance that out of all the different classes of soldier, including perhaps the more trustworthy and dedicated *praetorians*, the *frumentarii* were picked as the agents of Roman intelligence. After their disbandment, their successor class – *agentes in*

---

120 Ibid, 144.
rebus – took on the exact same dual role as couriers and imperial informants. When the
frumentarii were not eavesdropping during their duties in Rome or the provinces, they were
reading letters that they were hired to deliver.122

But not only the “data packet” – shall we say – was intercepted and read; the entire
communication network was under constant and ubiquitous surveillance. This network of roads
was called the cursus publicus, created during the time of Augustus, and served as the primary
means of governmental communication throughout the Empire.123 Joey Williams, an
archaeologist and social historian, analyzed the placement of Roman watchtowers along the
cursus publicus and identified their function as not only a preventative structure but also as a
visual deterrent.124 By putting almost unnecessarily close watchtowers on the roads and
combining it with security checkpoints through which all couriers had to pass, the Romans
engendered a sense of panoptic (or rather oligoptic – emphasizing the thematic concentration)
surveillance to let people know that they were being watched throughout the entirety of the
Roman communication backbone.

Panoptic surveillance should be considered both lightly and poignantly here. Unlike the
enclosed prison structure and central control hub of Bentham’s panopticon or of Orwell’s 1984,
Roman surveillance as we see is highly decentralized with spy networks operating on all three
levels of government. The frumentarii may have been institutionalized spies during Hadrian’s
rule (and agentes in rebus during Diocletian’s), but they by no means monopolized the

122 Ibid.
123 I stress governmental communication. Local communities nearby each segment of road maintained the
system, but nevertheless the primary travelers on the cursus publicus were military and government
personnel, not private couriers. See: Colin Adams and Ray Laurence, Travel and Geography in the
Roman Empire (New York: Routledge, 2001), p. 37. I will expound on this further below.
124 See: “‘E dahi desceo a dar-lhe batalha…’: a ocupação prerromana e a romanização da região da Serra
d’Ossa (Alentejo Central, Portugal),” Los Paisajes Rurales de la Romanización II, Anejos de Archivo
Español de Arqueología with R. Mataloto and C. Roque; also, “Surveillance and Espionage in the Roman
Empire.” TEDx (2015).
information control and interception network. Informers (delatores) comprised of an occupation in itself and the Romans (particularly rich ones) lived in constant fear of blackmailers. Effrontery or slander against the emperor would give the loose-tongued a quick ticket to meet the jailor or Pluto, and the informer would typically be remunerated for bringing the act to “justice.”

At the same time, silence could also be bought. The combination of public spies and private money-grubbing informants caused the following remark on the state of surveillance by Tacitus (d. 117 AD):

> The city was in deep alarm; never was there need of greater caution against a man’s nearest relatives. Men were afraid to meet; afraid to talk…they even feared things dumb and inanimate, the roofs and the walls.

Tacitus’ statement takes on an even more acrid note with the knowledge that his comment was spurred by a son’s accusation of his own father’s treason against the state. Overall, while surveillance in the Roman Empire was hardly as centralized or technologically adept as the Germany’s during the late 1930s, or Orwell’s Big Brother state, it would hardly be a stretch to make such a comparison.

How did the Roman citizen live in such a time of paranoia? Was there no privacy from snoopers, peeping toms, and hired informants? Could Romans find any shade from the prying gaze of insecure tyrants and their ubiquitous ears? Did they even recognize a right to privacy not given to them, or was our dystopia their norm? Let’s delve deeper.

---

126 Ibid.
II. Behind Iron Mask and Pen: Privacy from Government in Rome

When we break down the word “person” into its Latin root, we arrive at a compound verb: *per-sonare*. Etymologists explain the logic behind this combination as “the mask through which (*per*) resounds (*sonare*) the voice of the actor; and Roman citizens were defined by the legal privileges that attached to the masks, names, and images of their ancestors.”\(^{127}\) As Jeffrey Rosen alludes and as we shall see in the following section, a person’s mask of privacy depended on socioeconomic, religious, or racial privilege; their ability to wear it depended on a tenuous balance with the interests of the community and establishment of imperial order.

*Privacy, A Fundamental Right in Rome?*

The English noun ‘privacy’ derives from the Latin word *privatus*. Since *privatus* was not explicitly used or defined in Roman law,\(^ {128}\) the connotation of this word in the Roman context is disputed. A negative interpretation views *privatus* in reference to an outcast – one “withdrawn from public life.”\(^{129}\) This interpretation usually gains support from the pre-antiquity association of solitude or privacy as “dangerous…an effective method of punishment” since survival required community and its de-privation meant death.\(^ {130}\) These advocates also look to the architecture of public spaces during Greco-Roman antiquity. For a crude visual, historian James Whitman jests:

---

\(^{130}\) Such proponents include Serge Gutwirth, *Privacy and the Information Age* (Oxford: Rowman & Littlefield, 2002), p. 20; Posner, “The Uncertain Protection of Privacy by the Supreme Court,” p. 174. Although Posner states that when societies became more secure and developed, privacy/solitude began to lose its negative connotation.
Anyone who wants a vivid example [of how privacy mutated over time] can visit the ruins of Ephesus, where the modern tourist can set himself down on one of numerous ancient toilet seats in a public hall where well-to-do Ephesians gathered to commune...as they collectively emptied their bowels.\footnote{Whitman, “Two Western Cultures of Privacy,” 1154.}

But just because privacy did not exist in the defecatory crannies that it exists today does not mean it was lost as a legal or moral value. In fact, there is good reason to believe in the idea of \textit{privatus} as a social good, or at least as a neutral facet of Roman law. Gloria Gonzales Fuster credits an interpretation of \textit{privatus} in contrast with \textit{publicus} and \textit{communis}, therefore meaning something along the lines of “private, individual, own.”\footnote{Dictionnaire Gaffiot Lain-Français (1934), p. 1239, in \textit{The Emergence of Personal Data Protection as a Fundamental Right of the EU}, Gloria Gonzalez Fuster (2012), p. 22.} In fact, explicating \textit{privatus} as a contrast of more explicit and concrete notions such as \textit{publicus}, \textit{injuria}, and \textit{personalitas} (as Fuster does) could prove a more accurate route than a positivist approach.\footnote{Not to mention it would follow in Derrida’s method of deconstruction. In his essay, \textit{Différence}, he highlights the value in gleaning philological meaning from a word’s spatial distinction from other associated words. See particularly pp. 266-268 of Jacques Derrida, “Difference,” 62 \textit{Bulletin de la Société française de philosophie} 3 (1968) trans. Northwestern University Press.} Indeed, in one of the few hints of privacy in Roman law, the Roman jurist Ulpian (d. 223) categorized legal perspectives into two categories: \textit{publicum et privatum}.\footnote{Ulpian, “Huius studii duae sunt positiones, publicum et privatum” \textit{De Iusticia et Iure}, in \textit{Liber Primus: Titulorum Conspectus}. I.I paragraph III. http://www.thelatinlibrary.com/justinian/institutes1.shtml} This semantic shout-out means little for privacy as we regard it today, but it nonetheless highlights a distinction between aggressions within the public sphere and the private. In order to have the latter, one must have a conception of private property, and in the Roman case, they included notions of the private self, or \textit{personalitas}. This aligns with Fuster’s interpretation of \textit{privatus}, and in practice this was embodied through private law cases that addressed aggressions both physical (of the self or one’s property) and non-physical (of “aspects of the personality”).\footnote{Called \textit{action iniuriarum}. See Periñán (2012), 190.} Thus, while privacy was not
explicitly parsed out, its actualization as a right that would be fought for by the injured party implies that privacy not only existed but also was cherished as a positive utility value.

Before claiming that Warren and Brandeis recycled a 1600 year-old idea, it is important to note that while privacy may have existed as a right, it certainly was not interpreted as fundamental or primordial. The Romans indeed believed in natural rights, which were actually embodied in private law.\textsuperscript{136} However, these included, \textit{inter alia}, marriage, procreation, and family.\textsuperscript{137} We can safely conclude that privacy was not included as an aspect of freedom or \textit{personalitas} because of the institution of slavery. Justinian says “slavery is an institution of the law of nations, by which one man is made the property of another, contrary to natural right.”\textsuperscript{138} This latter phrase presents a perplexing paradox (how can two natural rights conflict?), but one that does not require digging unnecessarily into the weeds of slavery in Roman times to make its point about privacy. If a person is property of another, he certainly does not receive a fundamental right of privacy in any interpretation of the word.

But before leaving Roman privacy law and turning to its manifestation with surveillance on the ground, let us dig a little deeper into this apparent paradox. If we compare the above ideas of privacy with the previous chapter’s three baskets, we can see a theme highlighted in pre-Constitution privacy from Rome to the French \textit{Ancien Régime}: privacy as a function of individuality. In this case, privacy was conditional of status and granted by the state. When we say “person” today, we could replace it with “human being” to the same effect (albeit not unscathed from the bemused eye). To the Romans, not every human had a \textit{personalitas}, which could be translated into “legal personality.” In the Justinian Codex, there are laws of people and

\textsuperscript{136} Tribonian, \textit{Corpus Iuris Civilis} (535) I.II.I “The people of Rome, then, are governed partly by their own laws, and partly by the laws which are common to all mankind.”
\textsuperscript{137} Ibid, I.III.I
\textsuperscript{138} Ibid, I.III.III
laws of objects. Within the laws of people, there are three different layers – people, freemen, and slaves – each of which holding certain rights. In order to be a “person” and be afforded rights of personality (of which privacy is ambiguously one), a human must have freedom, citizenship, and a family. The middle of the three requisites implies necessitates the existence of the state. Even the Justinian notion of freedom (“the natural power of doing what we each please, unless prevented by force or by law”) while a natural right in the sense that we had it before the state, becomes a function of the state once subsumed by it. Privacy as a right, then, can only exist in the Roman conception as a latter function of the state, and only to a certain few.

Those without Masks: Outcasts and Runaways

Perhaps due to the belief that the gods would punish a community for the transgressions of one of its members, privacy in the Roman Empire was a communitarian value. Hesiod, writing of early Greek life in 700 BC, commented, “very often even a whole city suffers for the crime of one man.” In Rome, this statement rang true on both a theological and political level, and it provided a strong incentive for community self-policing. However, with self-policing came community biases. These biases combined with the majority of power resting in the hands of state-employed magistrates. Predictably, those who ended up losing privacy rights correlated highly with marginalized social groups and perceived enemies of the state.

How did this play out in Rome and the provinces? First, it was not uncommon for emperors to establish security in Rome through homogeneity, and so an initial operative was to

---

140 Tribonian I.III.II
expel or repress scorned ethnic groups such as Jews and Christians.\textsuperscript{142} Towns functioned similarly. Before adopting Christianity as the religion of the Empire, Romans often blamed Christianity and its followers for all woebegone states from crime to natural disaster: “Christians to the lion!” was a panacea with a ring to it.\textsuperscript{143}

Certain occupations got the short end of the stick alongside ethnic minorities. Astrologers were banished or repressed because people believed they had foresight into people’s destinies that could undermine the emperor’s power and omniscience. Domitian (d. 96 AD), a rather maladjusted emperor, had particular qualms with astrologers. In Cassius Dio’s historical account, people could be killed for merely conversing with an astrologer.\textsuperscript{144} Nerva, Domitian’s eventual successor after his assassination, was in the “peril of his life as the result of being denounced by astrologers who declared that he should be sovereign,” and was only spared by Domitian because other astrologers predicted Nerva’s imminent death.\textsuperscript{145} Unfortunately, Domitian’s death preceded Nerva’s, who then became emperor.

Philosophers and soothsayers were also persecuted and targeted for surveillance far more than other occupations. Philosophers were considered “notoriously outspoken,” and it is no coincidence that a great deal of complaints regarding privacy violations came from disgruntled philosophers like Seneca, Epictetus, and Augustine of Hippo.\textsuperscript{146} Christopher Fuhrmann gives a broad-brush affirmation of these prejudices in the provinces:

Traditionally minded Romans had an almost eugenic disdain for the former slaves, strange easterners, and charlatans whom they saw infiltrating the populace. But ordering these people to leave Rome or Italy was mostly about public posturing on the part of the princeps; there were no door-to-door searches.\textsuperscript{147}

\textsuperscript{142} Fuhrmann, \textit{Policing the Roman Empire}, 142.
\textsuperscript{143} Ibid, 47.
\textsuperscript{144} Cassius Dio, \textit{The Roman History}, Book LXVII, Chapter XII.
\textsuperscript{145} Ibid, LXVII, Chapter XV.
\textsuperscript{146} Fuhrmann, \textit{Policing the Roman Empire}, 142.
\textsuperscript{147} Ibid, 143.
Fuhrmann fails to elaborate how many “traditionally minded” Romans there were, or what that term really meant besides seeming a euphemistic synonym for ‘xenophobic.’ Yet his final clause is incredibly elucidating: despite the fact that these groups were despised, targeted in public, and often killed, there was a certain privacy of the home that such disdain curiously refrained from breaching. Whether this privacy was a function of property or attached to liberty or dignity is up to speculation, but in conjunction with the latter section one might be safest to guess the latter (personalitas).

There were a few occasions, however, when nobody had the right to privacy from door-to-door searches, and these instances pertained almost exclusively to the search for runaway slaves. According to Ulpian, a government mandate for the purpose of catching fugitives gave anyone – soldier or civilian – the right to search another’s property as long as they had a letter from the local magistrate:

This senatorial decree...gives a soldier or civilian the right to enter the estates of senators or civilians in order to search for a runaway, which the lex Fabia and the senatorial decree passed in Modestus’s consulship also provided for...It also set the same penalty against anyone who prevents his own property from being searched. There is also a general letter from the deified Marcus and Commodus, in which it is declared that provincial governors, magistrates, and milites stationarii (outposted soldiers) must help a master who is searching for fugitive, and that they must return the runaways after they find them, and that the people with whom they hid must be punished, if a criminal offense was involved.¹⁴⁸

This instance also shows the efficacy of the Roman’s ability to administrate decentralized surveillance on all four levels of bureaucracy (imperial, gubernatorial, detached soldiers, and civilian) to coordinate and triangulate a single slave without sophisticated communications technology. Indeed, citizens certainly had more agency than in the modern day, and one would viscerally hope that the sacrifices to privacy of the home are peculiar to Rome in comparison to

¹⁴⁸ Ulpian, Digests, II.IV.I.1 in Fuhrmann, 31.
today. Nevertheless, the coordination of private entities and public administration for surveillance purposes seems an almost timeless issue (which we will see in the next chapter).

So far, the examples in this section seem like etches in a somber (and perhaps long-winded) epitaph of the fledgling seed of privacy as some sort of right in the Roman Empire. Each example dispelled the notion of a fundamental or inalienable right to privacy in this social system, particularly when privacy of the home or self potentially conflated with the disruption of social order.\textsuperscript{149} But there is far more nuance to the situation, and there are far more instances where privacy is upheld and government bounded. Let us now consider those.

\textit{On the Road to Privacy: Bounded Surveillance in Communications Networks}

In the previous section, Roman information networks were painted as securely locked down by the state. Courier-spies (\textit{frumentarii}) intercepted messages; watchtowers and security stations gave eyes to both the network and the data as it traveled through a system of decentralized panoptic surveillance on the \textit{cursus publicus}. But here in the central gaze of the \textit{pantheopticon} we find curious vestiges of privacy, both top-down and bottom-up.

Beginning from the bottom, individuals and communities lashed out, perhaps at the perception of total surveillance. By the end of the third century, peasants in the provinces had knighted the \textit{frumentarii} with the epithet \textit{curiosi}.\textsuperscript{150} This new title was distinctly negative (roughly translated as “snooper”), and around the same time the peasants began to revolt –

\textsuperscript{149} One might still regard runaway slaves as relatively innocuous to social order. But recall the pressing memory of the Spartacus slave rebellion a few hundred years before. Also, from a proprietary or rights-based perspective, slaves were property and so fugitives represented both economic harm (through the slave owner’s property loss) and social disruption.

\textsuperscript{150} Sinnigen, \textit{The Roman Secret Service}, 68.
particularly in Asia Minor – due to their “unbearable” snooping and abuse of power.\textsuperscript{151} At first they were censured along with their lesser-ranked and static outposted counterparts, the \textit{stationarii}. A third century complaint by a local magistrate suggests a reason:

\begin{quote}
[The \textit{frumentarrii} and \textit{stationarrii} have assaulted] the town with intolerable burdens and damages…The community having been completely exhausted by the immense costs of the outside visitors and by the great mass of [collections], it (the town of Iudda) is being deprived of its baths on account of this difficulty, and it is being deprived of the things necessary for life.\textsuperscript{152}
\end{quote}

We can only speculate whether privacy was included as one of the “things necessary for life,” but combined with the unbearable snooping accounts we may assume that privacy violations were implicated as a reason for revolt and state censorship. Is it important to note, though, that it was not just the snooping that caused the \textit{frumentarrii}’s hatred and eventual abolition by the emperor, but rather their combined function of tax collecting and policing. This power, when in the hands of the corrupt, would strong-arm communities out of their livelihoods and make even a quick dip in the public bath a pecuniary problem.

The \textit{cursus publicus} also gives us insight into the roots of the prohibition of warrantless searches and seizures that we now see in the U.S. Fourth Amendment, as well as the stationing of soldiers in civilian houses embodied in the Third Amendment. These developments surfaced during Hadrian’s rule, and had to do with a series of edicts with respect to citizens’ complaints of activities from soldiers on the \textit{cursus publicus}. The first mandate given by the Marcus Petronius Memertinus, the Prefect of Egypt, stated:

\begin{quote}
I am informed that without having a warrant many of the soldiers when traveling through the country requisition boats and animals and persons improperly, in some cases seizing them by force, in others obtaining them from the \textit{stratégoi} through favor or obsequiousness, the result of which is that private persons are subjected to insults and abuses and the army is reproached for greed and injustice. I therefore command the \textit{stratégoi} and royal scribes never in any case to furnish to any person without a warrant,
\end{quote}

\textsuperscript{151} Ibid, 69.
\textsuperscript{152} Fuhrmann, \textit{Policing the Roman Empire}, 218.
whether traveling by river or by land, any contribution for the journey, understanding that I will vigorously punish anyone who after this edict is discovered receiving or giving any of the aforesaid things.  

Another edict, given by Hadrian himself, responded to soldiers traveling on the road and using private homes as free bed-and-breakfasts during their trips:

Free lodging shall not be allowed for any soldier to take while travelling on private business. But if someone is passing through while on duty or if they are bringing the ruling power’s money, or transporting prisoners or wild animals, public lodgings shall be given only to them and provisions at the market price which was effective ten days earlier. Then if anyone contrary to this shall make an exaction or use force, the names of those who take shall be sent to the provincial governor and my procurator.

Hadrian’s edict does not prohibit lodging soldiers from lodging in towns, but rather requires the lodgings to be “public” rather than private, even while on business that is not private. Again, privacy of the home is upheld, and when it is not (perhaps during wartime) it is properly remunerated. Furthermore, looking at the penultimate quote, the emphasis on “private persons…subjected to insults and abuses” implies both a harm-based and dignity influenced rationale in providing rights of personality to citizens.

Even though the frumentarii were remonstrated, hated, and disbanded, they were replaced by the agentes in rebus who turned out to be similarly corrupt and nosy. As a result, plebeians and senators alike took it upon themselves to establish their own forms of privacy within information networks. People began developing special wax seals with which to secure their messages. If the recipient found the seal broken, it had been opened and possibly tampered with. According to Harold Johnston, every Roman “of position” had special slaves used for

---

153 Papiri greci e latini (Pubblicazioni della Società Italiana per la ricerca dei papyri greci e latini in Egitto). Florence ed. Vitelli and Norsa. 5.446 c. AD 133-137 in Fuhrmann, p. 235.


155 Harold Whetstone Johnston. The Private Life of the Romans (New York: Scott, Foresman & Company, 1903), p. 289. Communications were sent through two different mediums during this time. Johnston notes
delivering messages (the messenger-slaves were called *tabellarii*) so they did not have to use the *cursus publicus*. Alternatively, before traveling, friends would notify each other with enough time to prepare letters and pool their deliveries through a trusted third party. Poor and less popular citizens still had an option for delivering messages, and would simply hail kind strangers who were traveling in the same direction. In order to maintain the integrity of their documents, particularly since miscarriage and interception was so common, many citizens would disguise the content of their letters information in code. According to Suetonius, Augustus used a simple three-letter cipher modulation (A equals D, B equals E, etc.).

Privacy of Roman information networks illuminates the primordial stirrings of rights that would not be constitutionalized in western governments until the 18th century. Interestingly, surveillance and privacy were neither mutually exclusive nor absent on the legal level from local colonies to Roman senators. Before leaving the Romans, we will examine yet another example of the tenuous duet between surveillance and privacy, focusing now the use of privacy and surveillance in institutionalized mechanisms of punishment. Familiar characters will make their appearance: sanctity of the home, privacy privileges stratified by social hierarchies, and the use of privacy as both a negative and positive value.

*Crime and Punishment (and Privacy) in the Roman Empire*

that parchment did not come into widespread use until the fourth century, and even then all but the longest letters were typically written on tablets (*tabellae*) of wood fastened by wire hinges (289). The inner faces would be hollowed out and filled with wax, upon which people traced letters with an ivory or metal tool (*stilus*). Parchment was written on with split reed pens and ink made of soot mixed with resinous gums. Letters would be rolled and sealed with wax; tablets would be tied with knots and upon each knot would be placed softened wax and a seal.

157 Ibid, 288.
We began this chapter with a look at the prison-like architecture of the Roman pantheon; now we will end it with a look at how actual Roman prisons functioned. Recall the original purpose of Bentham’s panopticon: a prison whereby the state entity could monitor (and subdue, as Foucault adds) the prisoner, and the prisoner could eventually be neutered through total surveillance. According to one of the most famous Roman jurists, Julius Paulus Prudentissimus (who we shall now call Paul), the Roman prison also acted to protect society and neutralize the offender. As we shall see, these prisons also had a way of attempting 100% surveillance. Interestingly, unlike contemporary punishment, prison had an alternative: 100% privacy.\footnote{158} This was enacted through exile, typically on an island out of the zone of “society.”\footnote{159}

Before diving into what prisons for the guilty looked like, we must first look at prisons for the potentially guilty: defendants during criminal procedures. During this time, jurisprudence was extremely interpretive and loosely organized. Judges were not required to hear a case, and acceptance would often depend on a fee of initiation.\footnote{160} If they accepted and the fee was paid, a judge ruled to his will, so long as it remained within the abstract realm of “moderation.”\footnote{161}

\footnote{158} Recall theoretical assumption #2, which is only reinforced here. Social systems cannot have 100% privacy (hence exile out of the system as another form of neutralization).


\footnote{161} Ibid.
take into account the gravity of the crime, the honor and wealth of the person in question, as well as their “harmlessness” (*innocentia*).\(^ {162}\)

During this pivotal point time in which a person’s dignity and danger to society was held in question, what kind of privacy (in the positive sense) did they have? Apparently, house arrest was an age-old tradition even in late antiquity, and the relationship an individual has with the sanctity of his home gets thrown into a dubious state of affairs. In 186 BC, the senatorial priests of the Baccanalia cult were detained in their own homes, guarded by the *triumviri capitales*, and in AD 375 the Roman deputy Aginatius was held under guard in his own villa.\(^ {163}\) Using the aforementioned discretionary parameters, the governor could decide whether the individual should be held guard in his own home (*custodia libera*) or in the home of his guard (*custodia militaris*).\(^ {164}\) Augustine of Hippo, regarding the curious situation of the pseudo prisoner in *custodia militaris*, commented: “the defendant inhabited the very same room as his guard, so that the room became a *carcer* to one while it was a home to the other.”\(^ {165}\) Only senators and those with very high social status (or “honor” so to speak) could escape surveillance during the time of a trial; otherwise, everyone – regardless of social standing – was under some form of surveillance.\(^ {166}\)

If people were unlucky enough to be found guilty in a judicial proceeding (and if they were not executed), they would then be filtered through a system of different forms of spatial punishment depending on their crime and status. I use “spatial punishment” rather than “prison”

\(^{162}\) Hillner, *Prison, Punishment and Penance in Late Antiquity*, 131.


\(^{164}\) Hillner 130. With this in mind, consider the implications of *custodia militaris* on the sanctity of the guard’s own home. It seems that those privacy rights would be forsaken for the security of the state (although likely obligingly so).

\(^{165}\) St. Augustine, *en. Psalm* 141.17, in Hillner, 130.

\(^{166}\) Julia Hillner (131-132) notes that this exemption for those of high status only really existed under Julian (AD 361-363).
because – like policing at this time – there was no institutionalized “prison” structure. Julia Hillner speculates that it was hard to tell what prisons actually looked like, “[perhaps] due to the often improvised nature of legal imprisonment in a variety of public spaces.”167 Higher-class citizens were typically condemned to exile (relegatio) over imprisonment within the province. More severe victims suffered its aggregate form (deportatio), which combined exile with loss of property and civic rights. Alternatively, prisoners could be sent to hard labor in imperial quarries or mines (metallum).168 One can only guess as to why exile was preferred over local imprisonment, but it was likely a matter of publicity and exposure brought by each prison. Since public prisons usually occupied central and public spaces, one would be in constant surveillance not only by the prison guards but also by the populace as they walked by.169

III. Escaping the Pantheopticon

As we jump from the third century pantheopticon to a variety of twenty-first century – opticons, we must bear in mind the qualitative characteristics of Roman surveillance and privacy. These will be further synthesized in Chapter 4, but for now consider some previously discussed views of pre-panoptic surveillance apparatus and filter or narrative of the Romans through the lens of our theoretical categories.

Beginning with the first of Haggerty’s metrics, the purpose of surveillance during Roman times was fourfold; information was valuable for political, economic, moral, and personal security reasons. Delatores became an informal occupation, selling information to others and

167 Hillner, *Prison, Penance and Punishment in Late Antiquity*, 125. Hillner goes on to comment that even temples were sometimes used as prisons. If so, just imagine the panoptic imagery were the pantheon ever used in this capacity.
168 Ibid, 119.
169 This hypothesis must be taken with a grain of salt, however. Publicity was not likely part of the punishment because the worst prisoners were put underground in “dark pits” (Hillner, 125).
selling their silence to the victims of their snooping. Emperors, senators, and other political aspirants or incumbents hired spies to seek out information of their rivals in order to gain leverage or uncover plots to usurp their power. Across the imperial and provincial levels, surveillance was used to keep the morality of others in check: heretics were banished and radicals (mainly philosophers) were kept under closer watch. But at the most fundamental level, surveillance provided physical security for households and for the proper functioning of the empire itself. That helps explain why the most heavily surveilled territories consisted of the borders and disruptive areas of the empire.

In terms of hierarchies, the Romans portrayed elements of panoptic (targets the masses and marginalized) and synoptic (targeted watch over the few, typically celebrities) surveillance. The more wealthy and powerful could afford more guards, more spies, and greater abilities for privacy through private couriers and walled/guarded estates. At the same time, people of higher status were more often targeted by spies and other powerful citizens due to the greater value contained in their information. The emperor, who had “eyes and ears all over the city,” also had the greatest amount of eyes on him. On the other hand, and as previously mentioned, marginalized groups such as slaves, Christians, astrologers, and philosophers were victims of a more intense gaze than less occupationally or socially ostracized plebeians.

In terms of targets, both humans and communications were objects of surveillance. Agents were always human, and surveillance was always performed through the physical eyes of the physical observer. *Vigiles* would obtain information by shadowing targets or eavesdropping on communications. *Frumentarii* on the other hand obtained information in large part from the contents of the letters they carried. This also sheds light on the dynamics of surveillance. People were often unaware that they were being watched during the act (thanks to the use of shadowing,
eavesdropping, and even disguises), but they had general knowledge that such activities were a part of life. For example, Cicero and Seneca knew (and lamented) that their communications were never private, or that undercover agents existed in society.

With respect to surveillance theories, can we really categorize the Roman case in terms of pre-panoptic, panoptic, and post-panoptic models? The image of pre-panoptic surveillance that Lyon depicts is rife with brutal imagery, disorganization, and a lack of systematization. Recall the Foucauldian view:

Modern societies have developed rational means of ordering society that effectively dispense with traditional methods like brutal public punishment. Instead we have more covert disciplinary practices to provide order, which in turn strengthens traditional power relationships.¹⁷⁰

Foucault asserts the novelty of the panoptic image through its systematic and bureaucratic organization, and the perception of constant watching that results in self-regulation and creation of docile bodies among the populace. But how does this differ qualitatively from what we have just seen of the Romans? They heavily bureaucratized surveillance: institutions and occupations were created specifically for the purpose of obtaining and organizing information (e.g. the frumentarii and the agentes in rebus, who had their own physical hub in Rome), and provincial governors and local magistrates were assigned positions and roles within the surveillance apparatus. According to the testimonies of many citizens, the surveillant assemblage penetrated deeply into communication networks and into the city of Rome itself. In the provinces, local communities and Roman citizens engaged in methods of self-surveillance, perhaps due to a combination of fear and a desire to preserve the status quo and prevent repercussions from above (in both a theological and political sense).

But many facets of Roman surveillance fail to meet the criteria set forth by the panoptic model. “Docile bodies,” in the terms that Foucault and Rhodes imagined, did not form; such an assertion, even if evident in some cases, would find it difficult to claim that such a result was a due solely to the government surveillance regime. But we can maintain that surveillance never reached the extent that Bentham’s panopticon, Orwell’s *1984*, or other panoptic imagery depicts. Aside from fugitive slave hunts, surveillant authorities were usually curbed at the curtilage of the home, failing to intrude as deeply as the hidden cameras in the television of Winston Smith’s apartment. Yet such a high bar and chilling visuals set a rather high precedent that one might regard with skepticism in real life, making one wonder if such an example does in fact exist historically.

Disregarding the historical segregation of our three surveillance theories, Rome may indeed exhibit post-panoptic characteristics more than it portrays the other theories. Outside the heavily policed and heavily centralized city of Rome, surveillance was highly decentralized. As mentioned earlier, the emperor created policy and often macro-level mandates; but the bulk of the surveillance mechanics and agents operated on a highly localized level, and information rarely needed to disseminate or coordinate past provincial administrators. We will expound on this idea later, but perhaps both a dearth and excess of technological means leads to decentralized surveillance, either out of necessity or out of luxury.

Roman connections with post-panopticism need not stop with decentralization. Roman surveillance, by focusing its limited resources on powerful members (usually of the senate) nearly as much as it did with marginalized populations, touches on the post-panoptic synoptic/panoptic conflation that panopticism lacks. The asymmetrical clumping of Roman surveillance structures (around roads, Rome, and rebellious areas) reflects the post-panoptic
notion of the *oligopticon*, which sacrifices breadth for concentrated gains in depth. Finally, the fact that the Roman government and its citizens hired third parties to spy, transmit, and protect information bears great resemblance to post-panopticism. This deviates from the panoptic model whereby the state apparatus monopolizes the mechanisms of surveillance. This distinction may be best exemplified by the Roman approach to transmitting communications, whereby individuals often contracted private couriers for reasons of speed, reliability, and secrecy of the letter. As we will see shortly, these reasons for using third-party service providers are not unlike modern decisions to use certain telecommunications companies or Internet service providers (ISPs) like Google or Apple. Security of one’s private information, now and then, in many ways resembles a pay-for-service market.

On a similar note, privacy too was a value for the privileged few. This privilege manifested itself both monetarily and socially. The law of personality did not protect those who were not legal “persons” (e.g. slaves), but nor did it protect those who could not pay the court fee to defend themselves. And when under investigation or in a criminal process, it paid to be rich: those in the upper echelons of the social totem pole would be placed under house arrest rather than be arrested. When they faced jail time, more powerful individuals would often be banished to an island – the less harmful (in terms of reputation) option – rather than placed in a public prison. This latter use of privacy demonstrates its flexible value in Roman society as simultaneously a privilege and a punishment.

In terms of sorting the Roman view of privacy into one of our three definitional paradigms, it seems best labeled as a harms-based and control-oriented privilege connected to dignity. In other words, it aligns with the definition espoused by Posner and Wittes: privacy is
the power and ability to conceal information about oneself and prohibit its use in a fashion adverse to the owner’s interests.

Moving into the information age of drones, wiretaps, and new panoptic acronyms like PRISM and TEMPORA, let us see whether privacy looks the same, and whether surveillance has or has not qualitatively changed.
CHAPTER III: TRAPPED IN THE AMERICAN PRISM

I. Privacy and Surveillance in Colonial America

“Privacy”

Remember the Proverb, *Bene qui latuit, bene vixit*, They are happy that live Retiredly. If this be true, Princes and their Grandees, of all Men, are the Unhappiest: For they live least alone: And they that must be enjoy’d by every Body, can never enjoy themselves as they should. It is the Advantage little Men have upon them; they can be private, and have leisure for Family Comforts, which are the greatest Worldly Contents Men can enjoy. But they that place Pleasure in Greatness, seek it there: And we see Rule is as much the Ambition of some Natures, as Privacy is the choice of others.

--William Penn, *Some Fruits of Solitude*, c. 1749

According to William Penn, privacy is seclusion, isolation, the act of being “retired” from the body politick and the *res publica*. In his opening quote, Penn harkens back to an aphorism in Ovid’s *Tristia*, which he interprets literally: “They are happy that live Retiredly,” out of the limelight and in a state of privacy. But Penn sorely misinterpreted Ovid’s meaning and the context in which he composed the lyric. When Ovid wrote the poems compiled in the *Tristia*, he had been banished by Emperor Augustus to the island of Tomis. His banishment is paradigmatic of Roman punishment discussed in Chapter II: as a poet he acquired the fame of the public and eye of the government to a similar degree as a philosopher; luckily, his family name (and that of his wife’s) got him exiled rather than imprisoned or killed. The morose reflections of the *Tristia* (“Sorrows”) pine for Rome, for family, and for community. With this in mind, Ovid’s proverb could perhaps be better interpreted ironically rather than literally, as Penn takes it.
Penn reminds us that privacy has always been double-edged, and one cannot cut corners when searching for its true meaning in earlier uses of the word. As we pause at colonial America, privacy becomes more easily parsed due to decreasing linguistic and chronological separation. At the same time, the recanting and quoting of history, particularly surrounding the American Constitutional framers, becomes far more biased and tainted by gilded nostalgia and modern political rhetoric.

The cases in colonial America, particularly precipitating the American Revolution, give us a framework in which to interpret privacy and surveillance in America and in the Constitution that dictates the government’s powers over its star-spangled citizens. Furthermore, we can ease the gross 1500-year historical hop from Rome to America by at least dampening the technological bells and whistles of twenty-first century surveillance. The creation of the United States, after all, was founded in part on a rebellion against panoptic surveillance and a dystopian Big Brother state. King George caused the splintering of the British Empire through the same lackadaisical overreaches in surveillance that Hadrian safeguarded against and preserved his empire 1500 years before. Let us see how.

*Give me War, or Give me Privacy*

The French and Indian War (1754-1763) left the Crown strapped for cash with a large army stuck on the American Continent. To solve the monetary problem, Charles Townshend, then Chancellor of the Exchequer of Britain, installed a bundle of eponymous decrees to sap the colonists of the usual accoutrements to a happy colonial Briton’s life.\(^\text{171}\) His justification: the colonists needed to pay up for “further defraying the expenses of defending, protecting, and

---

securing the said dominions [of the American colonies].” Townshend’s acts ruffled colonial cap-feathers for a political reason too. They explicitly asserted Britain’s right to tax its colonies by whatever means (reinforcing his predecessor Lord Rockingham’s Declaratory Act of 1766), and weakened the power of the assemblies by upping the salaries of colonial officials.\footnote{Richard R. Johnson, Review of “The Townshend Duties Crisis: The Second Phase of the American Revolution, 1767-1773,” in 49 The William and Mary Quarterly 2 (Omohundro Institute of Early American History and Culture, 1989), p. 400.}

Within Townshend’s decree, almost attached as an addendum, contained a renewal of a curious surveillance law that came into contentious legality during the 1750s, called the \textit{Writs of Assistance}. Like any self-respecting imperial epicenter with a mercantilist agenda, Britain wanted to ensure that it was its colonies’ primary trade partner. Britain thus passed the Navigation Acts in 1651, which restricted American imports and exports from other countries (primarily the Dutch at the time). For the colonies, prices became generally higher than on the open market, and so Americans took Adam Smith’s “invisible hand” into their own hands and began smuggling goods from other nations. The Writs of Assistance were meant to seize these smuggled (“uncustomed”) goods.\footnote{There are three different types of Writs of Assistance. The first are “writs of aid,” addressed to the sheriff and commanding him to help public servants enforce the payment of their dues. This type of writ is “ancient,” according to Philip Kurland and Ralph Lerner of the University of Chicago (See: Kurland & Lerner, 5 The Founders Constitution, Amendment IV, Doc. II.). The second kind of writ implores the sheriff to assist a party – under Court decree – to acquire lands withheld from him by another party. The third form, to which I refer above, did not exist prior to these mercantilist imperial models. James Otis picks up on the a-historicity of the writ in his argument against the writs in 1761.} The 1752 edict justifies that, because tax collectors had difficulty collecting their dues (particularly in Boston), “the sheriff and his Deputies and Servants from Time to time at his or their will” were allowed to “go on board any ship, boat, or vessel and then and there to view and search and strictly examine in the same, touching the
customs and subsidies [due to the government].”¹⁷⁵ They could also go into any “shops, warehouses or other places” and “open any trunks, chests, boxes, fardels or packs made up or in bulk.”¹⁷⁶

This first act of bulk data collection in America brought with it a hefty verbal broadside launched not by the ACLU but by James Otis. His diatribe against government surveillance, published as “Against the Writs of Assistance” in February of 1761, still brings shivers of delight to modern privacy advocates.¹⁷⁷ Otis first argued the writ’s historical anachronism, saying that such a broad and general warrant could only be found in “the old books.” Modern books, on the other hand, “[have] only special warrants to search such and such houses, specially named, in which the complainant has before sworn that he suspects his goods are concealed.”¹⁷⁸ However, as we can see from the “old books” of the second- and third-century Romans, such a thing as a general writ was highly uncommon and only existed in Hadrian’s time with reference to runaway slaves.

Nevertheless, the writ did indeed proffer some troubling stipulations that Otis handily culled and quashed. The meat of Otis’ thesis packages a number of recurring themes already seen in the polemic of third-century Roman provinces, and which we will see pop up in contemporary arguments against the PATRIOT Act. In terms of Haggerty’s metrics, Otis renounces the general nature of the writ’s targets, agents, and its dastardly hierarchical implications. While on the one

¹⁷⁶ Ibid.
¹⁷⁷ To name but a few, see: Thomas Clancy, “The Importance of James Otis” 82 Mississippi Law Journal 2 (2012), pp. 487-489; American Civil Liberties Union, "Massachusetts Residents Oppose NSA’s Dragnet Spying, True to Our History." Privacy Matters (June 17, 2013); Radley Balko, “General Warrants, NSA Spying, and America’s Unappreciated Founding Father, James Otis Jr.” The Huffington Post (July 4, 2013).
hand the writs were terribly general in whom they targeted, they also gave broad powers not just to the constable but also to his whole motley crew of “menial servants.”[^179] Subjecting merchants and lawyers to the scrutiny of the indentured servants and low-class commoners would upset established social hierarchies of power and subordination in a Foucauldian way, not unlike how Roman provinces felt about the *stationarii*.[^180] Otis asks, “What is this but to have the curse of Canaan with a witness on us: to be the servants of servants, the most despicable of God’s creation?”[^181] Even worse, Otis argues, this edict is “perpetual; there is no return;” in short, it has as many sunsets as the British Empire did at the time.[^182] Otis sums up his censure in one final jab that strikes at issues of hierarchy, oversight, property loss, and general injustice:

> Custom-house officers may enter our houses when they please; we are commanded to permit their entry. Their menial servants may enter, may break locks, bars, and everything in their way; and whether they break through malice or revenge, no man, no court can inquire. Bare suspicion without oath is sufficient.[^183]

If these allegations were true and ubiquitous throughout the colonies, then why was Townshend so daft and unjust as to renew them in 1767? Perhaps his logic went something like this. First, the writs were not meant to be surveillance laws in the sense that they aimed to monitor a populace for disturbances against national security. Instead, their goal was merely monetary - a means of enforcing a trade law that was being badly abused (perhaps on both sides) in port areas. Second, Townshend was not oppressing the colonists but merely keeping them to the same standards that Britain had for its own citizens: this type of writ was actually used

[^179]: James Otis, “Against Writs of Assistance.”
[^180]: In the Roman Empire, the *stationarii* were a lower class of soldier than the *frumentarii*, typically far less respected socially but initially endowed with similar duties of tax collecting and policing in the provinces. Eventually their powers were disbanded due to popular discontentment with such authority given to so low a status. See Furhmann, *Policing the Roman Empire*, 218.
[^181]: James Otis, “Against Writs of Assistance.”
[^182]: James Otis, “Against Writs of Assistance.” The lack of what we now call sunset clauses will return in full force with the perceived interminability of PATRIOT Act provisions.
[^183]: James Otis, “Against Writs of Assistance.”
among the British populace itself, and without rebuke. The Attorney General of Britain, William DeGrey, used this sort of justification when musing over whether to renew the writs in 1768 after Otis’ condemnation.\footnote{In his opinion, DeGrey remarks, “there can be no doubt, but that the Superior Courts of Justice in America are bound…to issue such Writs of Assistants, as the Court of Exchequer in England issues in similar Cases, to the Officers of the Customs.” William De Grey, "Opinion of Attorney General De Grey upon Writs of Assistance." 1768, in The Founders’ Constitution, ed. Kurland & Lerner (University of Chicago Press, 2000) Vol. V. Amendment IV. Document 2.} Third, perhaps Townshend did not foresee the potential for constables and their servants to abuse this power and destroy or expropriate property for their own gain. We can only speculate as to why Townshend renewed the Acts to such anticipated fervor, but we do have him to thank for the explicitness of the Fourth Amendment.

But Townshend went further. Just two years before the Townshend Acts, the Quartering Act attempted to solve the surplus soldier problem. Soldiers could occupy all manner of buildings: “inns, uninhabited houses, livery stables” and even in the houses of wine-sellers.\footnote{"The Quartering Act of 1765," trans. The Avalon Project (New Haven: Yale University Press).} Not only were they housed, but also fed and watered with “diet, and small beer, cyder, or rum mixed with water, by the owners of the inns…and other houses in which they area allowed to be quartered and billeted.”\footnote{The Quartering Act of 1765, V.} Moreover, the army could appropriate the town’s carriages, carts, and all modes of transportation when a detachment was passing through. The justice of the peace would give writs (i.e. warrants) “requiring the [village, town, city, etc.] to make such provision for carriages, with able men to drive the same.”\footnote{The Quartering Act of 1765, XV.} If they lacked in vehicles, other towns would have to pitch in their own carriages to “make up such deficiency.”\footnote{The Quartering Act of 1765, VI.}

The soldiers hardly got such amenities scot-free. Any soldier who took money from their hosts would be “cashiered” (pun likely unintentional) and kicked out of the army.\footnote{The Quartering Act of 1765, IX.} Also, the
edict attempted to retain some semblance of privacy from search and seizure by stipulating, “No commission officer shall break open any house…to search for deserters without a warrant from a justice of the peace, and in the day time.” Finally, persons who provided housing and food would be reimbursed in the following manner:

That the respective provinces shall pay unto such person or persons all such sum or sums of money so by them paid, laid out, or expended, for the taking, hiring, and fitting up, such uninhabited houses… and such sum or sums are hereby required to be raised, in such manner as the publick charges for the provinces respectively are raised.

This form of remuneration had a slight snag in it. The phrase “in such manner as the publick charges for the provinces respectively are raised” was another way of saying “through municipal taxes.” If colonists were to be compensated by funds acquired from municipal taxes, they were essentially being paid from their own pockets for a service they did not want. Moreover, this was yet another example of externally imposed taxation (via dictating how it should be used), and one that compounded on the purportedly egregious Townshend Acts.

It is easy to see how this motley combination of decrees caused the already heated colonial stew to boil over. We could dismiss this ease as a product of hindsight bias, but such a dismissal fails to recollect that even third-century Roman emperors recognized and skirted the blunders made by Townshend and King George III. Recall Hadrian’s edict that denied soldiers the ability to be quartered in private homes, or Marcus Petronius’ mandate that prohibited soldiers from requisitioning transportation vehicles without an individual warrant. Perhaps impositions of this sort were condoned in other societies, but in these two they were wholeheartedly rejected.

190 The Quartering Act of 1765, XXIV.
191 The Quartering Act of 1765, VIII.
192 See Footnotes 151 and 150, respectively.
Yet such draconian decrees were accepted – rather, tolerated – in times of war and for national (or imperial) security purposes. The appropriation of carriages and the quartering of soldiers in public houses or private stables had been accepted without uproar when the French came knocking on colonial doors just a few years earlier. In less than ten years after the Townshend acts, the Continental Congress had begun bureaucratizing bulk surveillance for itself. Through the newly established Committee for Detecting and Defeating Conspiracies, American revolutionaries rooted out spies and sympathizers for the British government through information gathering. The Sons of Liberty became the “mechanics” of domestic intelligence gathering, charged to regularly intercept and open Tory mail.

After the war was won, the Constitution expunged a good deal of the colonial and wartime surveillance regime. The Third Amendment banned soldiers from being quartered in private houses; the Fourth Amendment granted the right for people to be “secure in their persons, houses, papers, and effects” against unwarranted, “unreasonable searches and seizures;” the Fifth Amendment protected individuals from having to provide potentially self-incriminatory information, or from being convicted without a trial by an impartial jury (the “due process” clause), and ensured that they would be compensated fairly for any seizure of private property (e.g. carriages or livery stables).

For the next 212 years, these laws were enforced, ramified, and expanded to ensure the strength and equality of individual protection from government invasions of people’s life, liberty, and property. But by the time the smoke had dissipated from the wreckage of the World Trade

195 U.S. Const. amend. IV.
Center on September 11, 2001, people began to wonder whether those same protections, too, had been swept up with the rubble. 196

II. Building Big Brother: Upstream and Downstream Surveillance

How does the modern-day American surveillance apparatus function? As with Rome, we will start with macro-level government surveillance and work our way down to more decentralized systems of the U.S. surveillance regime. Before beginning, it is important to note that the vast majority of surveillance in the twenty-first century does not involve physical human watching. Certainly, we have policemen who monitor the roads for speedy drivers and patrol the streets to intimidate potential hooligans. But the days where the frumentarii or eighteenth-century constables sift through tangible goods on the frontier and communication networks are over. We have now entered the age of bits and bytes and strings of data that cross national borders like they were made of Swiss cheese. Information no longer passes through physical checkpoints but through satellites and fiber-optic cables where it travels at light speed and by the terabyte-per-second. Not only that but the information can be armed with malicious code that can steal billions of fingerprints or cause billions of dollars in damage by dismantling an entire country’s critical infrastructure. If parsing out privacy from the penumbra of law is like picking a needle out of a haystack in a hurricane, then finding malicious code in such a deluge of data is like threading that needle. How does the U.S. navigate such a herculean task?

196 For the sake of precision, I do not mean to imply that 9/11 suddenly eradicated Constitutional protections in one grand vanishing act. In fact, a more in-depth historical account than this one would show that these protections had been slowly eroding since the end of the Second World War or perhaps even before. For example, the US Operation SHAMROCK began following WWII and served as a rough analogy to modern upstream and downstream surveillance programs used by the NSA. The Foreign Intelligence Surveillance Act (FISA), which serves as the legal groundwork for the USA PATRIOT Act, was codified in 1978 to both fear and fanfare. I will briefly make reference to these erosions and others in the following section, but they will be handled with far more brevity and roughness than they deserve.
The American government surveillance apparatus is sorted into two basic organs: upstream and downstream surveillance (See Appendix, Figure 4). To understand the difference, one must first understand the way surveillance works in cyberspace. Computer surveillance can be separated into three different components: data collection, processing, and disclosure. This can be understood through human analogy as seeing, understanding, and telling. Information itself is tagged under two qualitative labels in cyberspace: information in motion, and information at rest. Upstream surveillance refers to the government’s collection (or interception) of information in motion as it travels through fiber-optic cables. The government then processes and disseminates the information internally among its bureaus and agencies. Downstream surveillance refers to the government’s collection of information at rest, stored and transferred by large telecommunications companies that manage the fiber-optic cables. These operative terms are rather fluid and based on the perspective of the agent: in downstream surveillance, for instance, the government’s “data collection” is functionally equivalent to the company’s “data disclosure.” Even so, it is crucial to distinguish between the three operations in order to understand how the different processes of surveillance function as well as the different ways in which they are regulated. With these categories of information flow under our belts, let us further dissect the two major organs of American dataveillance.

Data Collection

197 Orin Kerr actually separates computer surveillance into four stages, which he calls “evidence collection,” “data manipulation by machine,” “disclosure to a person inside the program,” and “public disclosure.” The only difference here is that Kerr parses out the “disclosure” aspect. This distinction is useful when discussing legal procedure, and proves particularly relevant when looking at tort law. However, for general purposes and for specifically regarding government surveillance (particularly in a functional sense), I combine the two. See: Orin Kerr, "Use Restrictions and the Future of Surveillance Law." In Constitution 3.0: Freedom and Technological Change, eds. Jeffrey Rosen and Benjamin Wittes (Washington: Brookings Institution Press, 2011), pp. 41-2.
International by nature, the Internet is a complex and convoluted network that sprawls the globe. Yet like an amorphous electronic vertebrate, it has a “backbone,” an international network of fiber-optic cables that carries over 80 percent of global telecommunications and Internet data (See Appendix, Figure 5).\footnote{The statistic floats between 80 and 99 percent of global data. Justin Elliot justifies the latter statistic of “99\% of international phone and Internet data” via a Telegeography report. See: Justin Elliot, "Does the NSA Tap That? What We Still Don't Know About the Agency's Internet Surveillance," ProPublica (July 22, 2013). Conversely, James Bamford produces his “80\% of telecommunications” from an interview with former NSA official William Binney. It is ambiguous whether his statistic would be higher if it included Internet data, or whether “telecommunications” implicitly refers to Internet data. See: James Bamford, "They Know Much More Than You Think." The New York Review of Books (August 15, 2013).} It is by accessing this backbone that the National Security Agency (NSA) conducts its upstream surveillance. The NSA uses a quartet of meteorologically schizophrenic programs (e.g. FAIRVIEW and STORMBREW) to “tap” the undersea cables with devices called ‘optic splitters’ as they beach on American shores (See Appendix, Figure 6). This method of upstream data collection rewards the NSA with information at a rate of approximately 10 gigabytes per second, or about 21 petabytes per day.\footnote{Data gathered from simple addition based on Slide 2 of “PRISM/US-984XN Overview,” released by The Guardian. See: Ewen MacAskill and Gabriel Dance. "NSA Files: Decoded, what the revelations mean for you." The Guardian (November 1, 2013), Slide 2.} In more humanly digestible terms, 21 petabytes is roughly equivalent to transferring all the information in all the books of the Library of Congress back and forth 108 times per day. To put that in even further perspective, this amount only adds up to roughly nine percent of total NSA signals intelligence.\footnote{John D. Bates. “Memorandum Opinion,” No. B.1.b.3. (Foreign Intelligence Surveillance Court October 3, 2011), pp. 23, 71.}

As a physical process, fiber-cable tapping is a far more intrusive exercise than most other forms of wiretapping. The majority of wires are made of copper wire cable, through which data passes by alternating the voltage in the cable: for example, “on” (or 1 in binary) could represent 5 volts, while “off” (or 0) could represent 0 volts. This constant alternation in current produces an electromagnetic field around the wire, allowing the NSA to “tap” (or “read” the data) in the
wire without penetrating the wire itself. While this process works well for short- to medium-range transmission, the change in voltage needs to be more pronounced over long distances, which costs more energy and therefore more money.\textsuperscript{201}

Telecommunications companies mitigate the monetary loss of attenuation by changing the medium by which the data flows. Instead of copper wire, fiber-optic cables consist of glass tubes through which data travels via photons, or light waves. Consequently, data packets of binary travel as light across the cables, and zeros and ones are differentiated through changes in frequency.\textsuperscript{202}

Unfortunately for the NSA, fiber-optic cables are far more difficult to tap. Frequency change emits no electromagnetic field, which means that the NSA must physically penetrate into the actual wire itself.\textsuperscript{203} Even worse, seven rings of petroleum jelly, Mylar tape, plastic coating, and thick steel cables surround the fibers.\textsuperscript{204} Data in each cable travels through one of around 100 fibers at the core (AT&T has 96), and the NSA has to install an optic splitter on each one.\textsuperscript{205} The optic splitter allows the NSA to copy the stream of data going through the fiber, transferring the duplicated light across another fiber, and causing only a slight decibel reduction (but no change in terms of content) in the original strand (see Appendix, \textbf{Figure 7}). This copied light then, once collected, gets channeled to a massive data center to be processed.

\textit{Data Processing}

\textsuperscript{201} This process is called \textit{attenuation}, defined as “a reduction in signal strength commonly occurring while transmitting analog or digital signals over long distances.” (Techopedia, \textit{Attenuation}).
\textsuperscript{202} HowStuffWorks. \textit{How does a Fiber Optic Cable Work} (June 15, 2000).
How does the NSA sift through massive amounts of data and make sense of it? Once the data has been collected, it undergoes a process called “Massive Volume Reduction” (MVR). MVR consists of a series of filters that look for specific tags, or “selectors,” in the information. The telecommunications company aiding the NSA often establishes the first filter. AT&T, for example, filters 30 percent of upstream data before entering government data centers by scanning and deleting “high volume, low-value” traffic (e.g. peer-to-peer downloads, films, computer programs). Next, the final 70 percent of the data passes through approximately 31,000 selectors determined by the NSA. These selectors include keywords based on potentially nefarious content searches, phone numbers connected to terrorist networks, or particular subject headings. For instance, if I call or email a suspected terrorist or his/her friends, my message will be stored in a data center and flagged for an NSA agent. Alternatively, if I look up sales of uranium enrichment equipment, my activities will likely be flagged and my phone number and IP address will be added to the “watch list” as a “selector” for further monitoring.

At this point one might ask: “well, this is certainly a lot of information, but if we are looking for international terrorist networks, then won’t we only be able to capture their data if it crosses through U.S.?” This certainly presents a bit of a pickle, but a pickle that gets diced in two ways. The first way has to do with fact that data travels across the Internet not based on directness but by cost-effectiveness. Like a capitalist Occam’s razor, the best answer is always the cheapest. This means that senders and recipients of communications need not be located in

---

206 Ian Brown, ECHR Witness Statement, 15.
207 Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies, and James Ball. "GCHQ taps fibre-optic cables for secret access to world's communications." The Guardian (June 21, 2013).
208 The “watch list” will be discussed in further detail in the legal section that follows. Furthermore, I will distinguish between metadata and content with regards to selectors, because the limitations for each vary greatly.
209 See “PRISM/US-984XN Overview” Slide 2, in MacAskill et al.
the U.S. for data to travel through the U.S. This works well for the NSA because the U.S. typically offers the most serviced routes.\textsuperscript{210}

Second, even if the data sidesteps the American fiber-optic beachhead, the U.S. has help from a collaborative network of intercontinental Anglosphere governments, called the “Five Eyes.”\textsuperscript{211} Spread out across three continents, this global surveillance alliance is able to pick up the vast majority of global communications.\textsuperscript{212} According to the British watchdog Privacy International, this information-sharing partnership has since mushroomed into multiple cohorts called the 14 Eyes (including various EU countries) and the 41 Eyes (all of the above, including a coalition in the Middle East).\textsuperscript{213}

But this also presents another slight dilemma for governments: now there is a \textit{lot} more information processed by different data centers with different selectors. Fortunately, governments often share selectors (GCHQ adds about 40,000 to the list) and forward each other information that may be of interest. Alternatively, the NSA can use a data query tool called XKEYSCORE. Like a souped-up Google for Big Brother, this program is essentially a massive search engine that accesses over 700 servers in 150 government data centers throughout the world (see Appendix, \textit{Figure 8}).\textsuperscript{214} The value and uniqueness behind XKEYSCORE lies in its ability to retrieve prodigious amounts of similar information for “shallow” analysis by agents looking for macro-level anomalies. On the front-end, an NSA agent fills out a simple form with a query, and receives a giant log of matches from any country (or countries) in the world. On the

\textsuperscript{210} Ibid.
\textsuperscript{211} The governments include the U.S., UK, New Zealand, Australia, and Canada. See MacAskill et al. “GCHQ taps fibre-optic cables for secret access to world's communications” (June 2013).
\textsuperscript{212} See Appendix Figure 6: International Internet Bandwidth Capacity in 2011.
back-end, XKEYSCORE accesses the databases of cooperating governments and aggregates the relevant information, revealing it to the agent in the form of a list of metadata. An example from a 2008 NSA presentation to the Five Eyes shows an agent ask, “Show me all the encrypted Word documents from Iran,” or “Show me all the exploitable machines in Country X.” Within a matter of minutes, the agent has trove of answers.

But even NSA agents have to sleep, and even massive data centers have capacity limits; so what happens to all this information after it is processed? A leaked document from the Snowden revelations suggests that the 250 or so NSA agents operating these programs can only access data content within three to five days of its collection, and metadata for 30 to 45 days. This data gets stored according to its type (e.g. voice, text, video, metadata) in an assortment of storage programs (e.g. NUCLEON, MARINA, PINWALE, see Appendix Figure 9).

Yet even with such a massive international surveillance infrastructure, the NSA has gaps in its surveillance apparatus. Despite the fact that the acquired information ranges upwards of 21 petabytes a day, the lost information accounts for potentially just as much or more data in terms of sheer quantity. The bulk of this information, oddly enough, comes from within the country. If you think about it, any information traveling across domestic networks will by definition not pass through the international fiber-optic cable network. And in the mindset of the NSA and Department of Homeland Security (DHS), the most dangerous “agents of foreign powers” are those that have already made it into the homeland. To compensate for this rather dire panoptic cataract, it engages in “downstream surveillance.” Here, it partners up with telecommunications

---

215 Ibid. See slides 10 and 12.
216 Ibid. See slides 15 and 23, respectively.
217 Morgan Marquis-Boire, Glenn Greenwald, and Micah Lee. "XKEYSCORE: NSA's Google for the World's Private Communications." The Intercept (July 1, 2015). For the number of NSA agents operating the program, see MacAskill et al. “GCHQ taps fibre-optic cables for secret access to world’s communications.”
companies and Internet service providers (ISPs) like Microsoft, Apple, and Google to retrieve information from both local and international networks. The information is again queried by selectors and stored by the NSA in a similar fashion through an umbrella collection and processing program called PRISM. There it combines with data gathered in upstream surveillance to create what surveillance scholars understandably call the omniopticon, a chillingly panoptic surveillance world.

*Justifying our self-imPRISMent*

After peering into the omnipresent and omniscient model of modern surveillance, one might pull out their Tocqueville and question freedom and democracy in America. But the government retorts with an equally somber philosophical rebuttal: it is the government’s sole function to provide the security of the collective rights of its citizens. This argument goes back to the Lockean social contract that built Madison’s Constitution. According to Locke’s social contract model, all humans are endowed with a set of natural rights (to Locke: life, liberty and property); by entering into the social contract and establishing government, they agree to decrease some of their individual autonomy for the preservation of these rights.\(^{219}\) The purpose of the state, then, is to provide security for the collective good of its body politick.

Now the government must justify its massive unwarranted surveillance regime by arguing that the gravity of the threat matches the pervasiveness of the surveillance. This proportionality argument is neither difficult to make nor is it hard to believe. In short, computer networks govern *inter alia* the nation’s electrical infrastructure, water supply, healthcare system,

and government administration. If any of these functions were compromised, the functioning of
integral aspects of life would sputter to a halt. For example, in 2008 the Estonian government
was “brought to its knees” by a Russian cyber attack that disrupted the country’s electrical grid,
banking system, and the water supply in Tallinn.\(^{220}\) Shortly after, President Obama made digital
infrastructure a “strategic national asset” and its protection a “national security priority” in a
2009 presidential address.\(^{221}\) Just last year, American companies faced 160 cyber attacks per
week (an increase of over 300% from 2010), costing each firm an average of $15.4 million per
annum.\(^{222}\) Finally, and perhaps most poignantly, the U.S. Office of Personnel Management
suffered a data breach in which 21.5 million social security numbers and 5.6 million fingerprints
were lost along with the personal records of 4.2 million government employees and contractors
(including this paper’s author).\(^{223}\) In short, it is no surprise that threats of “cyberwar” or a “Cyber
Pearl Harbor” have sprung up and created the cyber-paranoia that we see today.\(^{224}\)

In short, while the ends of initiatives like the USA PATRIOT Act may appear similar to
the \textit{Writs of Assistance}, their purpose could not be more different. First of all, and returning to
the threat to “democracy in America,” many people forget that we voted (overwhelmingly) for
our surveillance legislation. In 2001, Congress passed the USA PATRIOT Act with a vote of 357

\(^{220}\) Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational
\(^{221}\) Barack Obama, "Remarks by the President on Securing Our Nation's Cyber Infrastructure," \textit{The White
House} (May 29, 2009).
\(^{222}\) Riley Walters, "Cyber Attacks on U.S. Companies Since 2014." \textit{The Heritage Foundation} (November,
2015).
\(^{224}\) See: Richard Clarke and Robert Knake, \textit{Cyberwar: The Next Threat to National Security and What to
Do about it} (New York: Ecco, 2010). “Cyber Pearl Harbor” is a term coined by Defense Secretary Leon
in favor to 66 against.\textsuperscript{225} Ten years later when the Act was due to expire, the Senate extended its sunset provisions by another sweeping vote of 72 in favor to 23 against.\textsuperscript{226} While the \textit{Writs} were imposed for economic purposes and rebelled against due to the lack of representation and threat to national security (the French were long gone for British soldiers to justify appropriations of house and horse), modern bulk surveillance was legislated as a reaction to this threat. In fact, with the renewal of each surveillance law we have actually increased the mechanisms of our own surveillance.

And why not? More surveillance means more protection of our fundamental right to life, since PRISM’s job is to seek out terrorists and prevent them from causing harm to civilians! More surveillance means more liberty to walk in a subway or airport without fearing for our safety! Most importantly, more surveillance means the preservation of our fundamental right to property! Anyway, what cost is PRISM to us? The government need not break down our doors and rummage through our homes looking for ‘uncustomed’ goods, or install creepy cameras in our rooms and public spaces like \textit{1984}. In fact, we hardly realize that the government \textit{can} and \textit{does} monitor our information, and the degree to which it surveils. Philosophically, if we fail to realize we live in a fishbowl, does this not safeguard us from the existential harm to self-development outlined by the \textit{Hezek Re’iyyah}? Since surveillance is based on keyword selectors that only scoop me up if I am part of a terrorist network, privacy rights will be protected if I have nothing to hide, right?

Wrong. We believe that automated surveillance flattens the hierarchies of surveillance because robots are not racist. We believe that our surveillance program gives NSA agents

\textsuperscript{225} U.S. Congressional vote on H.R. 3162 #398: “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT).” \textit{107th Congress} (October 24, 2001).

unwarranted access to the lives of only the people dumb enough to Google-search how to buy Uranium 235 in Costco quantities. And we believe that precedential reasoning according to old privacy-related case law serves as adequate logic to protect our constitutional rights. The following two sections attempt to debunk these fallacious beliefs. The first part examines the main body of case law surrounding privacy from government surveillance. The second part discusses the ramifications of our perceptions of privacy by outlining the more discriminatory and chilling effects of the American surveillance apparatus. In this regard, it speaks to the intricacies of the hierarchies, dynamics, and targets of surveillance.

III. Picking Apart the Penumbra: Historicizing U.S. Privacy from Government

“[T]he house of every one is to him as his castle and fortress, as well for his defence against injury and violence as for his repose.”

--Justice Sir Edward Coke, *Semayne’s Case* (1604)

*The Cases that Framed the Framers: Semayne and Entick v. Carrington*

*Semayne v. Gresham*, or *Semayne’s Case* of 1604, seems rather banal in story and judgment, yet it provides the foundation for the Fourth Amendment and the property-based notion of American privacy law (not to mention the catchy adage “a man’s home is his castle”). Peter Semayne sued Richard Gresham for property that was owed him; the police obtained a writ (warrant) to seize the goods from Gresham, but before they could enter the threshold of Gresham’s house, he closed the door on them. As a result, the officials kicked the door down and took the property anyway. The court ruled in favor of Gresham, and determined,

---

227 *Semayne's Case*, 668 (Court of King's Bench, 1604).
“In all cases when the King is party, the sheriff may break the party’s house, either to arrest him, or to do other execution of the K[ing]'s process, if otherwise he cannot enter. But before he breaks it, he ought to signify the cause of his coming, and to make request to open doors.”

In other words, if the official has a valid warrant, he may break down the doors (or intrude on the sanctity of a person’s home); however, he must try peaceful methods first, like knocking. In American law, this principle is codified as the “knock and announce” rule.

Semayne’s Case stretches beyond matters of property to more obscure notions of liberty; always in the penumbra, if privacy were to be found it would be found within these shadows. For one, Edward Coke’s portrayal of the home stands out in history because of the notions of liberty and sanctity attached to it that constrain even a valid warrant. Previously – and particularly with a valid warrant – the state was unhampered by such ideological principles of the home. Suddenly with Coke, the state finds itself forced to engage in niceties even when legally justified in entering the house in the end. These odd rights attached to a person’s home extend even further to relations with other individuals outside the state: namely, one is legitimated in using deadly force against an intruder should the trespasser threaten a man in his home. This concept, while not particularly new (disputes had normatively been settled through the extrajudicial use of force for millennia) nevertheless rescinds an element of the state’s monopoly over the use of force for the sole context of the home.

---

228 *Semayne’s Case*, 198.

229 Indeed, Wittes (2011) begins his brief chronology of privacy with *Semayne’s Case.*

230 Recall the Justinian notion of freedom, for one: “the natural power of doing what we each please, unless prevented by force or by law.” Freedom is contingent on state acquiescence.

231 “If thieves come to a man’s house to rob him, or murder, and the owner or his servants kill any of the thieves in defence of himself and his house it is not felony, and he shall lose nothing.”
Entick v. Carrington (1765) enshrined the requirement of a valid ‘writ’ or warrant along with due notification before intruding in a person’s affairs. Lord Camden, justifying his ruling in favor of Entick, stated:

The great end, for which men entered into society, was to secure their property. That right is preserved sacred and incommunicable in all instances, where it has not been taken away or abridged by some public law for the good of the whole. The cases where this right of property is set aside by private law are various. Distresses, executions, forfeitures, taxes etc. are all of this description; wherein every man by common consent gives up that right, for the sake of justice and the general good. By the laws of England, every invasion of private property, be it ever so minute, is a trespass.\textsuperscript{232}

However, Camden’s speech hardly enshrines privacy as a fundamental right. This idea rests entirely on interpreting Camden through a Lockean or Hobbesian lens, and Camden seems to suggest both. The first sentence appears to refer to Locke, who believed property inherent (yet insecure) to man prior to state formation.\textsuperscript{233} Property, clearly, would be considered an inexorable right. Camden’s second sentence, however, implies that the right to property is granted by the state only insofar as it does not impede the interests of the common good. There is no clear consensus on how to interpret Entick,\textsuperscript{234} and governments, depending on their own national security environments, vacillate between views. Moreover, neither Camden nor Locke explicitly determine whether these rights – if read as fundamental to man – justify protection from other sovereignties.

A background in Semayne and Entick helps us understand the stance James Otis took only four years before Lord Camden defended private property in Entick. As with the Romans, a


\textsuperscript{233} John Locke, Second Treatise on Civil Government Ch.V (1689). See, specifically, Sec. 27 (“every man has a property in his own person: this no body has any right to but himself.”) and Sec. 30 (“amongst those who are counted the civilized part of mankind, who have made and multiplied positive laws to determine property, this original law of nature, for the beginning of property, in what was before common, still takes place”).

man’s home is his castle and should not be intruded on by the government unless there is valid occasion to do so; namely, for the protection of the common good. This idea influenced the first judicial ruling on data privacy outside the home and in communication networks in *Ex Parte Jackson* of 1877.  

*The Gilded Age of Privacy: Ex Parte Jackson and Warren & Brandeis*

*Ex Parte Jackson* came in the wake of Civil War Reconstruction and the first act of “dragnet” surveillance. The telegraph, which had been invented in the late 1830s, became centralized by the government during the war effort and used heavily by the military for coordination.236 On a darker note, the War Department’s newly established 1500-man Military Telegraph Corps, with the help of telegraph companies, seized all telegrams in major cities at the start of the war to “uncover rebel treason.”237 After the war ended, Congress retained the ability to authorize a “wholesale seizure of telegrams” under a subpoena (not a warrant) for the purpose of lustrating Congress of indecent politicians, which reached its zenith at the impeachment of Andrew Johnson in 1868.238 By 1876 politicians realized that no ones letters were safe from snooping, and many tried (and failed) to strike the provision. Even Western Union, in an act of defiance before submitting heir telegrams over to the state, authorized “the speedy destruction of all written messages as the necessary keeping of accounts would allow.”239 The year after, the Supreme Court emphasized that the contents of “letters and sealed packages…in the mail are as

---

235 *Ex Parte Jackson*. 96 US 727 (Supreme Court, 1877).
fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles.”

*Ex Parte Jackson* makes a few distinctions that – while logically sound in the second half of the nineteenth century – prove problematic in the information age. First, Justice Field, writing for the majority, distinguishes between two different types of mail: “letters and sealed packages” intended to be kept free from inspection, and “other printed matter” (e.g. newspapers, pamphlets) that were allowed to be examined. The general principle behind his logic was that if the message was sealed, it should be kept secret from all but the intended recipient. Of this latter category, the government was allowed to inspect and fine the owners and authors of “any article or thing intended or adapted for any indecent or immoral use or nature.” Second, and perhaps most crucially, the Court differentiates between data and metadata; in other words, between information content (the message itself) and information about the information (sender, weight, recipient, date of sending). This makes perfect sense at such a time period, because obviously the mailman would have to know to whom the document was addressed and where they lived. A ban on metadata secrecy would inhibit the functionality of the postal service.

Thirteen years later, Warren and Brandeis penned *The Right to Privacy* in the attempt to extend privacy away from a property right and towards an inherent right of individual dignity. The impetus behind their seminal work stemmed not from government surveillance but from yellow journalist’s exploitation of photographs to publicize intimate details of American citizens in newspapers. In the modern context, Warren and Brandeis were the first outcry against Victorian age paparazzi.

---

240 *Ex Parte Jackson*. 96 US 727 (Supreme Court, 1877), at 733.
241 *Ex Parte Jackson*. 96 US 727 (Supreme Court, 1877), at 733.
242 *Ex Parte Jackson*. 96 US 727 (Supreme Court, 1877), at 736.
Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the housetops.’

Technology enabled the eye to trespass without physical invasion into a person’s property, and forced privacy to extend to personal information. Rather than data versus metadata, Warren and Brandeis reframed the jurisprudential reasoning around the Justice Field’s first piece of legal logic – the secrecy or confidentiality of the communication itself – and uniquely attempted to attach a harms-violation to a person’s dignity rather than his property. This way of thinking closely mirrors the Roman honor or personalitas-based idea of a harms violation and diverges from a more Lockean root in private property.

Such a view failed to achieve immediate legal recognition when it came to governmental surveillance. In the 1928 Supreme Court Case on which Justice Brandies was serving, Olmstead v. United States, unwarranted communications procured from wiretapped conversations were declared legally admissible as evidence. But wiretapping at least was at least making its exit on the state-level. It had been declared illegal by over fifty percent of states as early as 1928, and the interception of telecommunications data had been outlawed by California as early as 1862. Nevertheless, whether Warren and Brandeis ever made it into the twenty-first century and the Internet is a far more dubious question. But some make the claim, and they do so by citing Katz

243 Warren and Brandeis, “The Right to Privacy,” 195. This does not sound much different from Tacitus’ comment in 117 AD: “Men were afraid to meet; afraid to talk…they even feared things dumb and inanimate, the roofs and the walls.”
244 Recall Lord Camden’s comment in Entick v. Carrington: “the eye cannot by the laws of England be guilty of a trespass.”
Katz v. United States: Privacy Peeks out of the Penumbra

*Katz v. United States* marks the legal transition of privacy to digital age. The advent of electronic surveillance gave third parties the ability to peek behind the moats and balustrades of man’s private “castle” (harkening back to *Semayne*) without physically scaling the walls. The *Katz* affair affirmed the idea written in Brandeis’ *Olmstead* dissent that man’s castle is more than just his home; some aspect of it travels with him wherever he goes. Charles Katz, who had “enclosed himself” in a glass, public phonebooth to discuss illegal gambling, was arrested by the FBI and incriminated based on this conversation, which had been wiretapped. The court found that even though he was using a public service, Katz had a “reasonable expectation of privacy” and therefore the government needed a warrant justified by probable cause prior to implementing the wiretap. The FBI, therefore, violated the fourth amendment.

*Katz* paves ground in many crucial ways. Most importantly, it established that electronic invasion paralleled physical invasion and allowed for fourth amendment protection. Law enforcement therefore needs probable cause and warranted approval by a judge in order to tap communications. This ruling also implies the illegality of bulk (or dragnet) surveillance: such collection defines no targets and thus cannot demonstrate probable cause, unless perhaps an entire telecommunications user base could be attributed to a nefarious deed.\(^{247}\) Second, Katz’s legacy mapped out a precedent for determining private versus public. “Reasonable expectation”

\(^{247}\) One might foreshadow that the NSA’s use of “selectors” could demonstrate probable cause even of bulk surveillance, but that jumps the historical gun quite a bit and will be discussed later.
of privacy derives from two sources. The first is a personal, subjective expectation: Katz, while technically in ‘public’, entered into an enclosed booth and used a service meant to be two-way and not a loudspeaker. Second, there must be an objective check by society that the subjective expectation is “reasonable.”

Yet within the Katz decision rests a critical distinction that will cause problems after 9/11. Namely, while it safeguards communications, it safeguards them strictly from law enforcement (as opposed to national security) purposes. In Justice White’s concurring opinion, he notes that if Katz had been plotting something more threatening to the state, then the unwarranted wiretap would have been legal:

There are circumstances in which it is reasonable to search without a warrant. In this connection…the Court points out that today's decision does not reach national security cases [of] Wiretapping to protect the security of the Nation…authorized by successive Presidents…We should not require the warrant procedure and the magistrate's judgment if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable.

The following years in the development of legal restrictions on government intrusion play out the ambiguities within Katz. Do people have a reasonable expectation of privacy in public, or to their metadata? What justifies “probable cause” for obtaining communications data? Finally, to what extent does national security wipe clean every individual’s privacy protection?

IV. Oversight and Out of Mind: American Surveillance (Un)Restricted

---

248 Katz v. United States, 389 U.S. 347 (1967). Justice Harlan’s concurring opinion, later called the “reasonable expectation” test and used in Smith v. Maryland in 1979. In other words, the plaintiff cannot be so deluded to claim he expected privacy in the middle of a public space.

The “national security” justification for communications surveillance whittled down *Katz* and *Ex Parte Jackson* into relative obsolescence. In a 1975 investigation into the operations of U.S. intelligence agencies, Senator Frank Church unearthed a program called Operation SHAMROCK, instituting precisely what Congress feared after the telegraph dragnet operation in the 1870s. Just like during the Civil War, the military placed censors at major telecommunications companies like RCA Global and Western Union (again) and never took them off. As a result, from 1945 to 1975 NSA agents had been reading and circulating over 150,000 messages per month, and covered up their tracks by refraining to report any details of the operation on any “traceable” document to Congress or even the president himself. While their purpose was to seek out foreign spies and saboteurs, they had to sift through American citizens’ information to do it.

Luckily for civil libertarians, democracy struck a fatal blow to Operation SHAMROCK. Congress determined that – at least out of wartime – the operation’s Fourth Amendment invasion outweighed the direness of the threat to national security. Also, thanks to the Watergate Scandal only a few years before, Congress feared that the surveillance would be abused for political rather than national security purposes. But Congress still recognized the state’s need to perform foreign intelligence surveillance to adequately provide security for its citizens in the age of spies and MAD. Thus birthed the Foreign Intelligence Surveillance Act (FISA).

*FISA*

Functionally, the text of FISA focuses chiefly on surveillance collection and oversight mechanisms. FISA legislators came in with two main objectives: make sure as few American

---

citizens are surveilled as possible, and make sure that someone watches the watchers. To safeguard American citizens, FISA required electronic surveillance to be solely directed at “the acquisition of the contents of communications…used exclusively between or among foreign powers.” On a macro level, the Attorney General now became responsible for ensuring that any unwarranted electronic surveillance met the following criteria: first, it had to be directed (at least in intent) at “foreign powers” and their “agents.” These “foreign powers” could be a “foreign government or any component thereof,” or a “foreign-based political organization, not substantially composed of United States persons.” An “agent of a foreign power” had to be “any person other than a United States person,” who engaged in spying or international terrorism. Alternatively, FISA allowed the targeting of agents spying for a “foreign power” or anyone suspected of engaging or being connected to international terrorism. After affirming these qualities of FISA targets, the Attorney General then had to ensure there would be “no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is party.” Finally, the entire operation had to undergo “minimization procedures” to prevent dissemination of “nonpublicly available information,” narrow the breadth of acquisition, and shorten retention times.

On a microscopic level, Federal officers would have to undergo a new series of procedural hoops to engage in warranted data collection. Attempting to codify a shift from bulk to targeted surveillance, FISA essentially required the Federal officer to justify probable cause by

identifying or describing the specific target of the surveillance.\textsuperscript{258} He also had to identify himself via signature on the warrant application, along with the Attorney general and a designated official from the executive branch.\textsuperscript{259}

Yet despite the procedural checks and balances, FISA still presented intrinsic technical opportunities for power abuses. This stems in part from FISA’s main objective: to separate domestic and foreign intelligence gathering by raising the requirements for the former and lowering the requirements for the latter. In legal terms, domestic surveillance warrants for law enforcement purposes are governed under a Title III warrant procedure; conversely, FISA warrants, procured for national security rather than law enforcement purposes, are governed more loosely and outside the Fourth Amendment and Title III procedure.\textsuperscript{260} Since requirements for procuring a FISA warrant were far lower and less stringent than normal warrant procedures for domestic surveillance, Congress feared that these disparities would lead law enforcement agencies to attempt to circumvent the traditional warrant procurement process for the ease of FISA. Congress also feared that the inherent secrecy to FISA would cause the same lack of oversight that existed in Operation SHAMROCK. Secrecy in surveillance was logical and indeed necessary in seeking out spies and mapping terrorist organizations; obviously surveillance would not be effective if the potential agent knew they were being watched.\textsuperscript{261}

To prevent these abuses, FISA created a judicial oversight mechanism, the Foreign Intelligence Surveillance Court (FISC). The FISC is a panel of seven (now eleven) district court

\textsuperscript{258} 50 U.S.C. § 1804 (a)(2).
\textsuperscript{259} 50 U.S.C. § 1804 (a)(d).
\textsuperscript{261} This differs from traditional Title III warrant procedure, which requires persons to be notified if they are under investigation.
judges elected by the Chief Justice of the Supreme Court.\textsuperscript{262} These judges determine whether there is indeed probable cause in each warrant application case. However, “probable cause” in FISA corresponds to the “belief that the target of the electronic surveillance is a foreign power or an agent of a foreign power.”\textsuperscript{263} As Peter Swire notes, this rendition of “probable cause” differs significantly from Title III “probable cause,” which looks for intent of crime rather than the identity of the target.\textsuperscript{264}

Either way, oversight beats no oversight, and FISA does in fact allow for congressional, executive and judicial watch over its watchers. In fact, such a mechanism of checks and balances to communications intelligence was and remains an unprecedented restriction on government surveillance, that upon creation was applauded by both civil libertarians and security hawks alike.\textsuperscript{265} Indisputably, the creation of the FISC filled some major gaps in surveillance restrictions to that point. Before FISA, the executive branch assumed the authority to surveil without judicial oversight, and no one was required to publish any information to the public.\textsuperscript{266} Before FISC, ordinary federal courts lacked the facilities and security clearances to deal with the classified information disclosed in intelligence agency hearings.\textsuperscript{267} By 2016, the cheers of 1978 innovations would (or should, perhaps) be gagged down rather significantly under a flurry of corrosive legislation. The “national security” justification was bolstered by an assortment of

\begin{itemize}
\item \textsuperscript{262} 50 U.S.C. § 1803.
\item \textsuperscript{263} 50 U.S.C. § 1805 (a)(3)(A).
\item \textsuperscript{265} Peter Swire, "The System of Foreign Intelligence Surveillance Law." 1320.
\item \textsuperscript{266} Now the Attorney General reports to the House and Senate Intelligence Committees every six months on the process and results of surveillance activities. These committees publicize the statistics such as the total number of FISA warrant applications granted, modified, or denied. See James Grimmelmann, Internet Law: Cases and Problems (Semaphore Press, 2015), p. 273.
\item \textsuperscript{267} Ibid.
\end{itemize}
antiquated judicial logic on Title III privacy (i.e. domestic law enforcement privacy), which eroded many of the principles originally espoused in FISA.

*Smith v. Maryland*

The first and perhaps most resounding blow to constitutional privacy in America began with a seemingly innocuous ruling on metadata. In 1976, Patricia McDonough was robbed and later harassed via telephone by an unknown assailant. The criminal was unmasked only after the police placed a “pen register,” which would record and relay all numbers called by a particular phone, on the suspect’s home phone and caught him calling McDonough’s phone number. Officials had no warrant and gave Smith no notice of the pen register installation, but the Supreme Court affirmed the legality of these actions because the metadata information made from his home was not “private.” The logic came from *Ex Parte Jackson*, which ruled that metadata of postal letters was not private and therefore required no warrant. As in letters so with phones: the telephone company records and publishes (as a business record) metadata in order to know how much to bill their clients, and Smith had already relinquished this information to a third-party.268 Using the “reasonable expectation of privacy” test from *Katz v. US*, the court ruled that the government violated no objective expectation of privacy by observing Smith’s phone bill.269

*Smith v. Maryland* should have no bearing on something like FISA, right? After all, it pertains to law enforcement and has nothing to do with national security or foreign agents. But that only makes the ruling more poignant because it began to once again flatten the boundaries between citizens and aliens, not two years after FISA was passed. Looking backwards, by the

time 9/11 hit and Congress pushed through the USA PATRIOT Act, judges would use this logic to absolve officials from walking through the procedural steps of warrant procurement for both law enforcement and foreign surveillance.

Privacy and Surveillance in the name of PATRIOT and FREEDOM

Now we have come full circle, from the world of upstream and downstream surveillance to the oversight mechanisms that govern them under the Janusian mantra of privacy and security. From 2001 to 2015, the American surveillance apparatus was governed by the USA PATRIOT Act. Its first chip out of FISA protections lowered the extent of probable cause needed by Federal officials when applying for a warrant. In FISA, foreign intelligence gathering had to be the primary purpose for search or surveillance; in PATRIOT, foreign intelligence had only to constitute “a significant purpose” for the investigation.270 Alberto Gonzales, Attorney General at the time, lauded the amendment as “bringing down the wall” that separated intelligence and law enforcement officials.271 To him, the re-blending of foreign intelligence and law enforcement officials would bolster the security of the nation and efficiency of the courts by “[eliminating] the need for courts to compare the relative weight of the ‘foreign intelligence’ and ‘law enforcement’ purposes of the surveillance or search, and [providing for] increased coordination and sharing of information between intelligence and law enforcement personnel.”272 With this increased coordination, PATRIOT also authorized both intelligence and law enforcement agencies to re-engage in bulk data collection, compel companies to turn over data to the

government, and seize tangible objects (books, papers, records, etc.) for any investigation “to protect against international terrorism.”\textsuperscript{273} The data of American citizens could be collected and processed as long as the investigation was not “conducted \textit{solely} on the basis of activities protected by the first amendment to the Constitution.”\textsuperscript{274}

These amendments seem historically regressive to say the least. Britain used similar justifications when it authorized the Townshend Acts: bulk surveillance and tangible seizures had to be instated to collect necessary taxes for the purpose (and recompense) of protecting the colonists from French invasion and Dutch subversive imperialism. The same circumstance happened when Congress reauthorized bulk surveillance on its own citizens after the Civil War and forced Western Union to turn over its telegraph communications. Now, after the 9/11 attacks and the omnipresent threat of terrorism, Congress and its constituents may be too scared to insist that privacy return from the penumbra and curb surveillance. Or perhaps in the age of porous borders and devastating cyber-threats, the populace has finally bought into the fear that had subsided in the American colonists or the Reconstruction Congress. Is their silence a sign of tacit assent, or is it merely the luxury of the panopticon’s invisibility in cyberspace?

After the Snowden revelations, there was a backlash against PATRIOT in the name of the FREEDOM Act. 2015 marked the year that many of the PATRIOT Act’s amendments were up for revision, and civil libertarians have made a few strides to curb some of the more purportedly egregious measures in the PATRIOT Act. Bulk data collection is (once again) prohibited, by (once again) requiring agents to justify warrants on the basis of a selector.\textsuperscript{275} From this selector (e.g. person, IP address, account, personal device), the NSA is allowed to apply for further data records within the first “hop” of the address. Hops refer to degrees of separation; if

\textsuperscript{274} USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272, Sec. 215 (emphasis added).
\textsuperscript{275} USA FREEDOM Act, H.R. 2048 (2015). See, in particular: Sec. I.103, II.201, and V.501.
my phone number is within the selected target’s contact list, then I am fair game to have my data searched. For the second hop (say, if the government wants to search the data of someone on my contact list), the government now needs to state “session identifying information” that affirms my connection with the suspected terrorist in some way. This “hop” requirement has also been expanded to the use of metadata loggers such as pen registers and trap-and-trace devices, forcing agents to justify their surveillance on the basis of “selection terms.”

The FREEDOM Act also focuses chiefly on transparency, and expands upon collection requirements by enforcing data processing limitations that were absent in PATRIOT. In both FISA and PATRIOT, companies were prohibited from publicizing when they received a subpoena to transfer data to NSA programs like PRISM. This decree, aptly called a ‘gag order,’ was rescinded and replaced with new permissions for private party reporting. Also, FREEDOM creates now requires the FISC to declassify all opinions, decisions and orders that include a “significant construction or interpretation of law.” Third, it provides the judges with a panel of *amicus curiae* that FISC may call upon for expert analysis during proceedings. This is an unambiguously valuable addition: FISC judges will be allowed to more fully understand the technical details and implications of the technologies in dispute, allowing them to move away from logic based on shaky analogues. Finally, government data storage programs like NUCLEON and PINWALE can no longer retain inappropriate data, and must “[promptly] destroy all call detail records” determined not to be foreign intelligence information.

---

276 H.R. 2048 (2015), Title II.
277 It is important to note that private entity disclosure is limited to quantitative data, such as the number of orders requested or customer selectors targeted. See Harley Geiger, "USA Freedom Act Summary & Analysis." *Center for Democracy & Technology* (2014), p. 2.
278 H.R. 2048 (2015), Sec. IV.402.
279 H.R. 2048 (2015), Sec. IV.401.
Taken as a whole, the FREEDOM Act’s surveillance limitations (or privacy ameliorations) could be seen as a hybrid between FISA and PATRIOT. PATRIOT broke down FISA’s wall between foreign intelligence and law enforcement agencies; FREEDOM turned it into a berm. FISA and PATRIOT targeted data collection standards, and FREEDOM extended its reach into limiting data processing and disclosure. Yet none of these Acts safeguard the data of non-US citizens, and many of their selection-centric safeguards fail to seal the cracks opened by anachronistic judicial interpretations of cyber-related processes. This final section examines these cracks, or “surveillance clusters” - areas where privacy fails to bound surveillance, which creates an asymmetric approach to surveillance much like the colonial Americans and Romans before them.

V. Clusters of Surveillance: Outcasts, Airports, and Aliens

Reflecting on surveillant assemblages such as PRISM and the like, one can see an odd beauty in the uniformity of modern surveillance. At least automated processes are not racist or discriminatory, right? They do not target philosophers over masons like in the Roman system, Bostonians over Britons like in colonial America, or blacks over whites like in modern anti-police polemic (Ferguson and the like). In its all-encompassing maw, surveillance is colorblind, race-blind, and xeno-apathetic. Is it?

Take the result of one of the data processing programs mentioned in Section I, called the “Watch List.” If my phone number shows up in the contact list of a known terrorist’s phone, or if my Google search hits a number of NSA selectors, then an NSA agent will likely put my name on a “Watch List.” Watch lists are controlled by an FBI-CIA joint department called the Terrorism Screening Center (TSC), and have different levels of severity: the “No Fly” list arrests you if you attempt to leave the country; the “Selectee” and the “Silent Hit” lists separate
individuals into other more ambiguous thematic baskets.\textsuperscript{281} There is little oversight or restrictions for the low-level agents who add names to the watch lists, which had already reached a size of 70,000 names by 2005.\textsuperscript{282}

Even though watch lists cannot have “single names” like Mohammed, they result in the arrests of a disproportionate amount of innocent Muslims with the same namesake. To name one of a thousand examples, a forty-four year-old Stanford PhD and mother of four, named Rahinah Ibrahim, was handcuffed and arrested by the San Francisco police on her way to Hawaii.\textsuperscript{283} Another case taken up by the ACLU and canonized by a croup of comedians peals:

They call me David Nelson and my name has been besmirched
When I fly across my country, I will always be strip-searched
Somewhere a David Nelson is allegedly quite mean
And the TSA ain't able to declare my person clean . . .
I missed my flight from Texas and I missed my flight to Spain
You'd think my second cousin was a Tikrit named Hussein
I'm scrutinized and sanitized by security and then
The next time that I fly, they have to do it all again.\textsuperscript{284}

Thirty-two million Americans report that they have been victims of racial profiling, and Muslims bear the brunt even with robotic surveillance. But ought we blame the racism of government surveillance or of ourselves? After the September 11 attacks, a Gallup poll showed that 58

\begin{itemize}
  \item \textsuperscript{281} The data on how people reach these latter two lists remain unreleased. The Department of Homeland Security, in 2009, released a primer called the “Role of the No Fly and Selectee Lists in Securing Commercial Aviation,” but the criteria for reaching each list was blacked out. See, Department of Homeland Security, “Role of the No Fly and Selectee Lists in Securing Commercial Aviation” (Washington: Office of Inspector General, July 2, 2009) pp. 9-14. A leaked internal memo on the selection process can be found in the Appendix, Figure
  \item \textsuperscript{282} Donohue, “Anglo-American Security and Privacy,” 1137.
  \item \textsuperscript{283} Raymond Bonner, “One Woman’s Case Proves It’s Basically Impossible to Get Off the ‘No-Fly List’” \textit{ProPublica} (2015).
  \item \textsuperscript{284} “Statement of David Nelson” (ACLU).
\end{itemize}
106

percent of Americans favored requiring “Arabs” (regardless of nationality or American
citizenship) to go through more intensive security checks at airports.285

Discriminatory surveillance in airports is doubly problematic due to their exceptional
legal status on the physical “frontier” – so to speak – of the national border. According to the so-called “special needs” doctrine of the Fourth Amendment, government searches in certain
contexts are exempt from the warrant requirement due to their extraordinary influence on
preserving public interests.286 This collectivist logic, similar to the national security exemption,
enables the suspicionless inspections of physical information and transportation networks (recall
Roman surveillance on the cursus publicus), including vehicular searches in highway
checkpoints and personal/baggage screening at airports. But when combined with unwarranted
Watch List arrests, physical screening in airports begins to bear rather existentially scarring
results. In Rahinah Ibrahim’s trial (she had sued the government to get her off the list), she cited
“shameful” abuses to her dignity as a citizen; others understandably say they feel personally
ostracized by their country and community.287 Claims of personality or honor infringements such
as these fall along the lines of Brandeisian, Talmudic, and Roman views of privacy rights.
However, they have yet to break judicial ground against American government surveillance,
whose internal trainings on how to track communications reference a character named
“Mohamed Badguy” as their archetype.288

This inherent discrimination does not favor the recent move towards more decentralized
forms of American surveillance. In 2002, Admiral Poindexter launched a program called

285 Mark Singer, “America’s Largest Arab Community in the Aftermath of September 11 (The New
Yorker, Oct. 15, 2001).
286 Jack Goldsmith, Cyberthreat, Government Networks, and the Fourth Amendment (Washington:
287 Bonner, “One Woman’s Case Proves It’s Basically Impossible to Get Off the ‘No-Fly List’”; Kari
Huus, “Muslim travelers say they’re still saddled with 9/11 baggage” (NBC News, September 13, 2011).
288 Amy Davidson, “The NSA’s Spying on Muslim Americans” (July 10, 2014).
Operation Terrorism Information and Prevention System (TIPS). Its function was to fill in the surveillance holes that automated surveillance failed to meet: namely, a national Citizens Corps of peer-to-peer surveillance. TIPS recruited “millions of American truckers, letter carriers, train conductors, ship captain, utility employees and others” as informants of any suspicious activity.\textsuperscript{289} As with the Roman *frumentarii* system, TIPS was destroyed by the press and Congress and prohibited. But just as the Romans disbanded the *frumentarii* and rose up the *agentes in rebus* in their wake, the American government decentralized the program into a number of smaller component parts. Now we have the Marine Watch, the Highway Watch (which employs over three million truck drivers for information-sharing purposes), and the Neighborhood Watch to assist in “national security and road safety.”\textsuperscript{290} The Volunteers in Police Service (VIPS) encourages community members to take photographs and utilize Twitter and Facebook to document the community’s activities – particularly suspicious activity – and look into people’s “Virtual Life.”\textsuperscript{291} Another VIPS document on “Alternative Citizen Patrol” encourages the adoption of volunteer citizen patrol groups to provide “extra eyes and ears to the community.”\textsuperscript{292} If all of these programs have anti-Muslim or anti-[feared or despised minority] citizen groups, discriminatory surveillance will leave the airports and easily pervade into local communities. Perhaps surveillance should have been left in the hands of Big Brother after all.

Fortunately, Big Brother still has many nearly invisible tools to play with in its law enforcement and national intelligence forms. Police can place unobtrusive “Q-Ball” GPS trackers on cars, use drones to monitor cities and towns from above, place hidden CCTV cameras in public places, and access national surveillance databases to find information about potential

---

\textsuperscript{289} Donohue, “Anglo-American Security and Privacy,” 1132.
\textsuperscript{290} Donohue, “Anglo-American Security and Privacy,” 1133.
\textsuperscript{291} Volunteers in Police Service, “Moving Your Volunteer Program Forward with Social Media,” (US Department of Justice), pp. 1-3.
suspects. With a warrant, they no longer need to search and seize computers to access their information thanks to programs like “Magic Lantern,” which infiltrates a computer through a disguised malware-infected email, and then “watches” users type in passwords to thereby access any document or email in the user’s network.293

But there must be Fourth Amendment protections for programs like Magic Lantern, drone-based monitoring, and the more racist aspects of asymmetrical surveillance, right? Privacy from government intrusions on the home and property must surely exist in the twenty-first century. Indeed, there remain protections in the Bill of Rights that protect against physical and (some forms of) electronic intrusions, searches and seizures, and even self-incrimination. The FREEDOM Act does prevent the processing and physical reading of data and metadata outside particular selectors and citizenships. Letters and emails still cannot be read without a warrant, and a man’s physical home does indeed remain his castle until probable cause shows that he intends to harm others in it. But legal rulings on disputes between citizens and government surveillance are beginning to shift the framework of our castles from stone to glass.

Meta-debating Metadata

Let us return to Mr. Glass, the victim of two Supreme Court rulings and a European Court backlash against the American security state. The original case that dealt with Glass’ vehicular monitoring, United States v. Jones, actually ruled against GPS surveillance by law enforcement. Scalia, delivering the majority opinion, harkened to a quote from Entick v. Carrington to support the logic behind his ruling:

---

“[O]ur law holds the property of every man so sacred, that no man can set his foot upon his neighbour’s close without his leave; if he does he is a trespasser, though he does no damage at all; if he will tread upon his neighbour’s ground, he must justify it by law.”

Scalia used *Entick* to argue Jones’ privacy based on his inherent Lockean right to private property. In essence, the fact that the policeman physically inserted a GPS tracker onto a vehicle without a warrant and then used the tracker to monitor Jones, which constituted a “search.”

Scalia went on to emphasize a difference between visual inspection of a vehicle in public and the attachment of the device to a car. While “[t]he exterior of a car…is thrust into the public eye…thus to examine it does not constitute a ‘search,’” the officers in this case did “more [sic] than conduct a visual inspection of the respondent’s vehicle.”

Unfortunately for Mr. Glass, Scalia’s logic and that of the three justices who concurred with him (without filing a concurring opinion) does not apply. Constant public surveillance by drone causes no harm or invasion to private property, nor does it violate a person’s objective expectation to privacy. Therefore, drone surveillance falls outside the protection of Scalia et al.’s interpretation of the Fourth Amendment in *Jones*.

Justice Sotomayor makes an admirable attempt to fill this hole by attempting to make two revisions to how we look at metadata and privacy in public. First, whereas *Smith v. Maryland* ruled that metadata gleaned from pen registers proffered insignificant data to claim “private,” an amalgam of that data could reveal immense insights into a person’s private life. Sotomayor says that even though people disclose metadata to third party carriers all the time, “I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a

---

list of every Web site they had visited in the last week, or month, or year.”

This marks a stark deviation from *Ex Parte Jackson* and *Smith v. Maryland* by distinguishing the actors involved when engaging in a “reasonable expectation of privacy” test. Just because a person allows their information to be seen and used by Google does not mean that the information has now lost all claims to privacy from the NSA. Privacy, in this light, is no longer a binary where the existence of a third party marks the end of privacy, or where privacy ends at the boundary of property. Rather, it is Nissenbaum’s contextual integrity model, where privacy is defined by the context around the relationship in which information is disclosed to other parties.

District Court Judge Richard Leon nearly dismantled the NSA’s entire metadata gathering program by applying Sotomayor’s analysis to bulk metadata surveillance. In *Klayman v. Obama* (2013), Leon argued that the “nature and quantity of the information contained in people’s telephony metadata [today] is much greater” than in 1979, and therefore metadata could not be regarded in the same blasé light as it was in *Smith v. Maryland*.

In his ruling, he noted that the FREEDOM Act did absolutely nothing to prevent bulk metadata collection and processing under Section 215 of the PATRIOT Act, and therefore violated the Fourth Amendment. His ruling nearly codified the elimination of dragnet surveillance as a whole and established an entirely new precedent for examining data in cyberspace; one that was based on the nature of data flows in cyberspace and the information processing capabilities of surveillance programs like PRISM and XKEYSCORE, not on letters, telegrams, or telephones.

Yet Leon and Sotomayor’s opinions were swiftly dispatched and metadata is still regarded in terms of *Smith v. Maryland* principles. FISC judge Rosemary Collyer rejected and

---

298 *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013). Leon, Memorandum Opinion, at 28: “When a person’s metadata is aggregated over time, in this case five years, it can be analyzed to reveal ‘embedded patterns and relationships, including personal details, habits and behaviors.’”
overturned Leon’s analysis in *Klayman v. Obama* (2013), ruling that Leon’s analysis was “unpersuasive” and further (in response to Sotomayor, perhaps) that *U.S. v. Jones* “provides no basis for departing from Smith with respect to the Government’s acquisition of non-content telephony metadata.” Her justification combines the “plain view” and “trespass” doctrines of Fourth Amendment jurisprudence used by Scalia in his majority opinion in *Jones* with *Smith v. Maryland* to explain that people have no reasonable expectation of privacy to information turned over to third parties. Collyer emphasized that “when a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities.”

This does not exactly bode well when the FREEDOM Act forces companies like Google, AT&T, or EYE2EYE to turn over data in bulk.

What does this capability actually mean for privacy from government surveillance? In Roman terms, it means that the *frumentarii* need not read the contents of your letter to know which baths you frequent, philosophers you talk to, or religion you secretly adhere to. In colonial American terms, it means that customs officers need not break down your doors to know which goods you have, where you procured them, and from whom. Today, it means that surveillance drones could follow your public activity for weeks without a warrant, mapping which buildings you enter and who you talk to in public, on the phone, or via email.

---


301 “The Court observed that it “consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” BR 14-01 (2014). Collyer, at 10.

CONCLUSION

He gazed up at the enormous face. Forty years it had taken him to learn what kind of smile was hidden beneath the dark moustache. O cruel, needless misunderstanding...But it was all right, everything was all right, the struggle was finished. He had won the victory over himself. He loved Big Brother.303

As we look into the past immersed in our world of big networks, big data, and Big Brother to stare back at us from our computer cameras and CCTV monitors, it is only natural to incline ourselves to think that surveillance could never have existed without x, y, or z. If Mr. Glass had existed in second-century Rome – shall we call him Magister Vitrum – would he be able to empathize with the unblinking eye of Magnus Frater? Lyon, Weber, and others say no. Clearly, one could not instill the non-deified paranoia of omniscience, omnipresence, and omnipotence without the technologies or bureaucratic administration that we have today. On the other side of the technological coin, Haggerty and Lyon claim that even Orwell’s model proves too primitive for understanding the purpose, hierarchies, actors, targets, and dynamics of the surveillance structures that we have today.304

In many ways such a claim would be correct. Mg. Vitrum would be unable to comprehend the concept of electricity much less the cameras and cables that followed. Obviously surveillance looks completely different now than it does before, but to what extent are these differences aesthetic mental contrivances as opposed to real qualitative differences in how surveillance operates over time? A great deal of this thesis has been devoted to responding to this question with an emphatic no.

304 Lyon, The Electronic Eye, 218.
First of all, surveillance theory’s separation of models into three chrono-thematic baskets is inherently flawed. Rome may not have had a centralized bureaucracy in the Weberian sense, but Roman surveillance by no means embodied the “irrational,” disorganized, and shallow attributes of “primitive surveillance.” In fact, it was centralized and decentralized, bureaucratic and capricious synoptic and panoptic and oligoptic. It created “docile bodies” of self-regulated communities within its boundaries, and used visibility (on the roads) and invisibility (in public spaces) to intimidate and exploit. Its communication networks spanned the entirety of the empire and indeed look incredibly similar to the backbone of America’s telecommunications network (see Appendix, Figures 10 and 11). These networks had unreliable third-party service providers, encrypted messages, and attempted totalitarian surveillance by the government to ensure no data was malicious. Rome melded elements of primitivism, panopticism, and post-panopticism in one glimpse. Classifying Rome as any one of these lenses leads to a myopic historical bastardization of the time period. The same goes for modern America. Its surveillance structures retain highly centralized elements through the singular programmatic Leviathans necessary to amass solitary petabyte-sized data banks. At the same time the surveillance apparatus could not function without the decentralized and harmonized agencies that perform upstream and downstream surveillance.

Moreover, even though their structures are two thousand years and two civilizations apart, American and Roman surveillance systems functioned in very similar ways that continue to conflate these theoretical models. Neither operates as purely Foucauldian oppressive models of power domination, but make national security the primary focus of their social contractual aim.\(^{305}\) Their actors – whether *agentes in rebus* or automated robots – monitor marginalized

\(^{305}\) Recall that Roman surveillance was used for military coordination and legal harmonization across provinces, neither of which directly oppressed or entrenched internal power hierarchies.
groups through tactics of communal self-regulation and mobilization, strong-man oppression, and heightened central surveillance. They cluster decentralized surveillance resources around frontiers, information networks, and potentially threatening communities. They outsource surveillance to the private sector (third party service providers, individual data carriers, or local communities) for the same reasons. They even use visibility and transparency of their operations for both intimidation (visibility) and subversion (invisibility). In the end, those who feel on the wrong side of the –opticon claim that they feel perpetually watched, heard, and monitored by the eyes, ears of the government’s invisible agents.

Of course the many nuances between the systems create large fissures to dissuade any further claim of parallelism. The Romans monitor marginalized groups by exiling Christians, killing political rivals, and jailing philosophers while the Americans do it by disproportionately tracking Muslims’ communications and peering into private life without barging into the home. These nuances are certainly important, but to claim that they fundamentally change the qualities of the surveillance apparatus and logic in their respective creations should be regarded as a point of contention, not a premise to create an entirely different theory.

Yet some discrepancies admittedly give pause to qualitative differences among the surveillance systems. The nature of the agents proves an immediately striking qualitative shift. Automated processing does not necessarily differ from human surveillance in its discrimination, but it does feel less of a visceral invasion to think of an apathetic and impersonal computer “looking” at my data. If automated data collection and processing does in fact alter how citizens feel about and interact with the structures surveilling them, then surveillance may indeed be able to push back the existential harms arguments of communities that view privacy like Julie Cohen and the Talmud.
This begs another qualitative question that opens up the can of worms to the other half of this thesis’ investigation: how did privacy function as a boundary of surveillance? This is a very difficult question to answer, in part because of the inherently hazy nature of the term and primary metrics used in picking it out of the penumbra. This thesis has in part pointed to the existence of privacy through instances of popular revolt against government surveillance. However, we have seen that these instances of revolt and surveillance rarely isolate privacy as their leading agent, and typically include perceptions of injustice, marginalization, and monetary exploitation. Would Romans have revolted against the *frumentarii* if they had not been corrupt and exploitative? Would Otis have spoken out against the *Writs of Assistance* if he had not seen British taxation as inherently unjust?

We can hardly make such a claim for ourselves, and much less make post hoc rationalizations of inherent rights in the psychologies of other societies. When we call for the abolishment of PRISM and PATRIOT, do we do it because we actually believe that the knowledge of deep and ubiquitous surveillance will harm our existential self-development? If so, then perhaps we should stop posting our intimate details on Facebook and LinkedIn. Alternatively, perhaps we have something incriminating to hide and simply fear that the government will find us out and throw us into jail. Or perhaps we fear tyrannical power due to a philosophical grounding in our country’s history, which would make sense because citizens of the United Kingdom for one allow far more CCTV cameras and condone equally invasive surveillance measures as we do without national backlash.\(^{306}\)

---

In the end though, even Roman and American revolts against government “privacy” invasions share many similarities that follow the structure of the social contract. For one, citizens will tend to accept and even vote in laws that restrict privacy to increase surveillance, but only on the occasion that there is a perceived national security threat. When this threat goes away, the populace will typically push to curb the strength of that surveillance provision. However, this poses a new problem in the age of dataveillance: soldiers are no longer barging into houses to conduct searches, or appropriating carriages and houses for their operations. The physicality of surveillance is dwindling, and with it our vigor in curbing typical infringements like bulk surveillance.

Perhaps the realm of cyberspace constitutes the largest qualitative change between Rome and America. Well-funded individuals can cause as much damage to nations as only armies could, and they can do it from their bedrooms. How can man’s home still be his castle in such a world? Maybe governments really do need the PRISMs and dragnets to preserve its socially contractual obligations in the information age, and perhaps we must allow the panopticon to turn our castles into glass houses. But whether or not we decide to abandon or love Big Brother, or welcome the panopticon as a model for our own self-imprisonment, we must bear in mind the qualities of surveillance and privacy that change and those that remain timelessly constant.
Figure 1: Bentham’s model of the pantheon
Figure 2: Architectural design of the Pantheon

Figure 3: Map of Roman Empire and Legion Distribution, AD 125
Figure 4: The NSA’s Upstream and Downstream Data Collection. Source: The Guardian

Figure 5: Global Fiber-optic Grid. Source: nsa.gov
Figure 6: North American Fiber-optic Network

Figure 7: T-Splitter. Source: “Redacted Declaration of J. Scott Marcus”
Figure 8: XKEYSCORE. Source: The Guardian
Figure 9: PRISM Collection Dataflow Chart. Source: The Guardian

Figure 10: U.S. Transmission Backbone.
Figure 11: Imperial Roman Road Network c. 117 AD. Source: University of North Carolina
BIBLIOGRAPHY

Primary Sources


Brown, Ian, interview by European Court of Human Rights. Witness Statement (September 27, 2013).


Epictetus. Dissertationes. Edited by Christopher Fuhrmann.


Ex Parte Jackson. 96.727 (The Supreme Court, 1877).


*Memorandum Opinion*. (b)(1),(b)(3) (Foreign Intelligence Surveillance Court, October 3, 2011).


*Olmstead v. United States*. 277 (438) (The Supreme Court, 1928).


*Semayne's Case*. 668 (Court of King's Bench, 1604).


*Smith v. Maryland*. 442.735 (The Supreme Court, 1979).


[http://avalon.law.yale.edu/18th_century/quartering_act_165.asp](http://avalon.law.yale.edu/18th_century/quartering_act_165.asp).


**Secondary Sources**


Elliot, Justin. "Does the NSA Tap That? What We Still Don't Know About the Agency's Internet Surveillance." ProPublica, July 22, 2013.


