A Rhetorical Hermeneutics of Danger: Leaks in the Digital Age.

A DISSERTATION
SUBMITTED TO THE FACULTY OF
UNIVERSITY OF MINNESOTA
BY

Daniel Ladislau Horvath

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

Advisor Ronald Walter Greene

May 2015

Acknowledgements

I would like to express the deepest appreciation to my mentor and advisor, Dr. Ronald Walter Greene. His truly inspiring work and his gentle soul have defined the trajectory of my entire academic career. I also want to thank my committee—Dr. Karlyn Kohrs Campbell, Dr. Arthur Walzer, Dr. Edward Schiappa—for their hard work and, above all, for their patience. Their attentive reading and thoughtful feedback have shaped the present argument, made me a better writer, and helped me become a more discerning thinker. I would also like to thank my writing and support group—Dr. Shannon Stevens, Erin Cole, and Dr. Dana Schowalter—for their unwavering support. My appreciation goes to the larger UMN family as well—professors, friends, colleagues—as integral parts of the universe that made this project possible. I also want to mention all my professors at UNLV who encouraged me to pursue my studies, none more adamantly so than my MA advisor Dr. Donovan Conley.

On a personal note, my sister, Edith, my brother in law, Robert, and my niece, Petra, have provided a home far from home. I would not have survived let alone thrived in the U.S. without their love and support. I am also grateful for my parents' patience. Silvia and Vasile paid the steepest price for my success: not being able to see their son in person for the last 10 years. Finally, I owe a debt that can never be repaid to my partner, Dr. Shannon Stevens, who has provided the very "conditions of possibility" for something like this to exist.

Dedication

This dissertation is dedicated to those whose lives are interwoven in the texture of this project: Shannon, Betty, Ziggy, and Muggsey.

Abstract

For the past 10 years, unauthorized disclosures of classified information have become a permanent fixture of our political landscape. Their frequency, magnitude, and commonality have engendered competing discourses that rhetorically articulate the act of disclosure to transparency and accountable governance or, respectively, to threat and national security. Through an analysis of the legislative history of FOIA, internal documents from various state institutions aiming to deter such disclosures, and public statements from people indicted of leaking classified information, this dissertation investigates how truth of and about government becomes problematized, how its accessibility, its subjects authorized to speak, and its threatening others are shaped, defined, and put into political play. This dissertation traces through this legislative history the "will to truth in politics" and "national security" as distinct logics of organizing truth of and about government whose dialectic results in a "multilayered architecture of access" by which the discursive field is controlled through divisions between licit and illicit objects of discourse, lawful and unlawful circuits of discursive flow, as well as authorized and unauthorized subjects. This structured access is complemented by an "insider threat apparatus" that defines potential leakers as "insider threats," as individuals with a propensity to commit a crime and thus as targets of surveillance and intervention. The counter-discourse, to these institutional attempts to conflate leaking and treason, links a *parrhesiastic* irruption of truth to the most important ideals of the democratic imaginary: transparency, accountability, and informed citizenry. The "rhetoric of *parrhesia*," however, is not so much a counter-discourse as it is the dialectical other of

the “rhetorical hermeneutics of dangerousness.” Both are deployed as technologies of interpretation that distribute discourses, institutions, and populations onto a political field of action structured by the issue of access to information. In the end, this study illuminates how Foucauldian Rhetoric is less of a rhetorical hermeneutics to uncover the power of discourse but a way to investigate how a rhetorical hermeneutics is put into operation by an apparatus to uncover problems and threats.

Table of Contents

Chapter I:

Unauthorized Disclosures and Rhetoric *via* Foucault

> I have never tried to analyze anything whatsoever from the point of view of politics, but always to ask politics what it had to say about the problems with which it was confronted.[1]

"Please turn off and stow all electronic devices"

"I genuinely believe that the story that's the biggest one—that will make the biggest impact and will shape how the events of the last 10 months are viewed by history—is the story on which we're currently working," claimed Glenn Greenwald, the famous journalist that broke the Edward Snowden story, in an 2014 interview with Stephen Colbert.[2] Whether we choose to accept the label "the biggest one" or simply read this quote as a common journalistic teaser announcing the next story is less relevant than the seemingly inevitable fact of its occurrence. *Disclosures are now common*. With documents from only one source, in this case Snowden, news of the existence of a global surveillance machine with all its manifold incarnations, with studied pace, has steadily become part of the public knowledge for over a year now. We live in, what we might be inclined to call, the digital leaks era.

While leaks to the press are nothing new, the provisional origin point of this era of digital leaks can be set with the release in 2010 of the "Collateral Murder" video of an apache helicopter killing two Reuters' reporters, among others, and the subsequent Wikileaks disclosures and scandals of the last 4 years. This is an era marred by massive

revelations in terms of their relevance, in terms of their quantity, as well as in terms of the virulent government reaction against those perpetrating the leaks, a reaction leading to the unflattering label "war on whistleblowers." Each side, meaning that of the government and that of the supporters of these revelations, similarly appeal to privacy (for themselves) and transparency (for the other party). Each of these demands, for publicity and respectively for secrecy, rests on and activates a certain understanding of the world. On one hand, the specter of Oceania, the fictional land described by Orwell in his seminal novel *1984*, where total ideological control over the population is exercised via absolute surveillance and indoctrination, takes an active rhetorical role in the discourses surrounding the Snowden revelations. Snowden himself references Orwell in a short Christmas video message claiming that the technological advances make NSA's collection of data and surveillance capability dwarfing that of the fictional Big Brother. On the other hand, the trauma of 9/11, as the event that never should have happened and should not happen ever again, as well as the subsequent war on terror against Al Qaeda as the enemy par excellence, authorizes a perpetual war and ever increasing systems of surveillance and intervention. In one world we are threatened by totalitarian control, in the other by annihilation; in one, the government becomes inimical to democracy, in the other, we are surrounded by countless enemies.

One vision is animated by the fantasy of an end state of democracy, where things can be known, where things can be disseminated to all, where this publicity can discipline the elected officials to work on behalf of the people rather than on behalf of private interests, and where informed consent can finally legitimize the representative in

"representative democracy." The other is animated by the dream at the heart of governance, of total control of the social field, of being able to govern with the consent of the governed in their interests according to expertise, to defend society of any and all enemies both foreign and domestic, by clearly identifying and defining problems and threats, by knowing, surveilling, analyzing, and ultimately by targeted intervening.

Chelsea Manning's 30-year sentence, Aaron Swartz's suicide allegedly caused by the threat of a 30-year prison sentence for sharing academic articles at no cost, and Edward Snowden's attempt to gain political asylum yield the only three subject positions available to those who speak out of turn: the *prisoner*, the *martyr*, and the *exile*. The survivor—Daniel Ellsberg—might turn out to be a unique subject position. All these cases raise important questions about truth, about sharing information, about ownership of knowledge and ultimately about truth of and about governance. The emperor's new clothes story captures so eloquently both the irruption of truth in the political arena and the plasticity of power structures. While the story builds to the moment of truth, the climactic scene where the child reveals that the emperor is naked, in fact the imperial procession continues despite these revelations. Embarrassment aside, the structures of power do not collapse completely. This is the context, the milieu of the study as well as its object domain.

To follow the motto opening this dissertation, the goal is to analyze what "politics" has to say about the problem of disclosures, with which it is confronted at an unprecedented level today. In this respect, I am interested in tracing the discourses that articulate these "entities"—"government" and "the people"—in rapport to these

disclosures and their relationship with truth in the context of an increasingly permeable digital world. My first goal is to make sense of these competing narratives as well as the way these narratives are articulated into political demands and into institutionalized modes of intervention. My second objective is to situate these discourses in the larger discursive formations articulating truth to transparency and security. My third goal is to make sense of the political subjectivities that emerge from these scandals by charting the emergence and political relevance of the whistleblower and the insider threat as the subjectivities par excellence of the digital leaks era. Lastly, I aim to show the continued relevance for rhetorical studies of the Foucauldian corpus. With this last goal in mind, I will proceed next to detailing my theoretical and methodological commitments that bind together the different analyses unfolding in this project.

Foucauldian Rhetoric as Critical Sensitivity

> But there is a negative work to be carried out first: we must rid ourselves of a whole mass of notions, each of which, in its own way, diversifies the theme of continuity.[3]

I use Foucauldian Rhetoric as a shorthand for a rhetorical studies approach enriched by the encounter with the work of French "historian of thought" Michel Foucault. The concerns of this project, as previously mentioned, are directed at the discourses that flourish in the wake of these disclosure scandals, the discourses that articulate differently institutions and citizens to truth in politics. Who better to serve such analysis than Foucault himself whose main theoretical concern was to chart the regimes of games of truth wherein the analysis is directed not so much at what is true as it is

directed to what is accepted as truth in a particular society, in a particular discipline. What rhetoricians actually do in practice with his help does recommend Foucault as a prime resource for rhetorical criticism. Indeed our theoretical engagement with Foucault, ebbing and flowing with each new book and published seminar, is now at least three decades old. Between 1965, the year of the first English translation of the *History of Madness*—the abridged version titled *Madness and Civilization: A History of Insanity in the Age of Reason* —and 2015, the English speaking world saw a steady stream of Foucauldian scholarship. Up until 1985, all Foucault's major works had been translated and published in English. After a lull, between 1985 and 2000, the last decade saw the publication of almost all of Foucault's lectures at College De France from *Society Must Be Defended* to *The Courage of Truth*—the last lecture given before he died—and currently (2014) *Wrong-Doing, Truth-Telling. The Function of Avowal in Justice.* Like clockwork, every two years, and now with increased frequency, we have a new published seminar, a new glimpse into his work. There is a new Foucault book every year and there are still more books translated and published. This abundance of scholarship is matched by an equally vast list of rhetorical criticism articles that engage Foucault at every stage.

On the matter of how rhetorical scholars are approaching the Foucauldian corpus, the critical orientation of the scholarship employing Foucauldian concepts to make distinctly rhetorical arguments, a brief survey of scholarship yields a useful taxonomy that allows us to interrogate Foucault's uptake in rhetoric. The articles cluster in three main categories: theoretical engagements, practical applications, and disciplinary problematizations. The first category, what I would label, "Rhetoric *and* Foucault,"

contains primarily theoretical engagements having the difficult task of introducing the Foucauldian ideas to our discipline. These articles try to show the compatibility between rhetoric and Foucault, bridging the gap between rhetorical theory and concepts and those of Foucault. The second cluster of articles can be grouped together under the banner "Rhetoric *with* Foucault." These are practical applications making use of specific concepts from the Foucauldian panoply in the act of rhetorical criticism. "Rhetoric via or *through* Foucault," points to a smaller number of articles showcasing ways of doing criticism that seem transformed by the encounter with Foucault problematizing some of the foundational principles of rhetorical criticism, emphasizing circulation over hermeneutics, and being concerned with the interplay of power, knowledge, and subjectivity. These articles are performing what I would call a Foucauldian rhetoric, an elusive term that defines an orientation, a way of doing, a critical sensitivity rather than a method proper.

This brief review of a 30-year history of scholarship popularizing, appealing to, and, in some cases, being transformed by the encounter with Foucault's work allows me to speak of a distinct theoretical and methodological sensibility that articulates rhetoric's traditional concern—the role of discourse in human affairs, broadly construed— and elements—speaker, speech, audience, and situation—to larger issues clustered around philosophical questions of knowledge, power, and subjectivity. Although some of our discipline's theoretical breakthroughs—epistemic, critical, ideological, or constitutive—that overtly turn our disciplinary gaze toward these questions are either made possible by, or done with the express help of, Foucault, it bears repeating that these are not new to

rhetoric and do not emerge in rhetorical studies solely or even primarily as a result of this theoretical encounter. Nonetheless, I argue, Foucault allows us to bring together these distinct and disparate—already rhetoric's—concerns manifested in *turns*—as in "significant theoretical and methodological shifts in direction," i.e., *epistemic turn*, as well as in "one at a time," i.e., *taking turns*—in a loosely linked ensemble amounting to a perspective or a sensibility. My attempt to sketch the inner workings of this sensibility are not so much a matter of policing the proper understanding of Foucault in rhetorical studies as much as it is a way to clarify and lay bare the assumptions that buttress and guide my own rhetorical approach to the discourses surrounding the unauthorized disclosures of classified materials.

What I can trace through decades of scholarship is the intersection between a highly influential body of theory and our own rhetorical studies tradition. Specifically, this disciplinary history looks at how rhetorical critics have picked up and used Foucauldian concepts to do rhetoric, hence, literally, "Foucauldian rhetoric." Furthermore, in answering Barbara Biesecker's question—*if our field were to affirm his [Foucault] statements, how would its tactics be transformed and the territory modified?*—I argue, we are compelled to ponder not how rhetoric can appropriate Foucauldian concepts into its theoretical and methodological matrix while continuing to study persuasion "in roughly the same old way,"[4] but to consider what is or should be the result of this encounter and what are the productive transformations through which rhetorical studies should go. Therefore, if we avoid the temptation of becoming simply Foucauldian as well as the temptation of metabolizing solely those concepts which are

benign to our fundamental theoretical and methodological assumptions and thus allowing us, as Biesecker notes once more, "to integrate our discipline among the postmodern humanities" while in fact remaining the same, we must contend that the resulting critical perspective is neither simply Foucauldian nor simply rhetoric, but something new, a Foucauldian rhetoric.

It is in this articulation of concepts and methods from rhetorical studies and Foucauldian work that I find a productive way of looking at discourse. In order to trace the assumptions behind Foucauldian rhetoric, I will begin with asserting and defining a series of characteristics—the theoretical horizon and methodological makeup of this critical sensitivity. This is as much a definition of this critical sensitivity as it is a literature review, as each characteristic rests on a germinal essay in rhetorical criticism.

Foucauldian rhetoric (1) is archival, spans great vistas of discourse and begins with problematizations; (2) its own conceptual logic is that of bricolage (the toolbox approach); (3) is posthumanist; (4) is articulatory, taking articulation as its logic, as its organizing principle linking the elements of the rhetorical situation, and (5) is sensitive to the subtle relations between subjectivities, powers, and knowledges allowing the mapping of apparatuses and thus a better understanding of the role rhetoric plays in relation to power knowledge and subjectivities.

Foucauldian rhetoric (1) is archival, spans great vistas of discourse and begins with problematizations. In other words, it lends itself with ease rather to explorations of a greater magnitude than precise analyses of smaller units of discourse such as a speech or a film. That is not to say that is better than or that it displaces such analyses but that its

sensitivity is calibrated to the larger tectonic movements of discursive formations. In other words, it is simultaneously synchronic and diachronic, covering as much terrain and extending over as much time as it needs to in order to make visible the contingency of specific practices. An apt example is John M. Sloop's excellent study on discourses about prisons and prisoners that spans popular articles about prisoners (over 600 hundred) from 1950 to 1993.[5]

To put it differently, Foucauldian rhetoric is a rhetorical exploration of discourse that maintains the essential impulses of Foucault's dual methodological movements of Archeology and Genealogy. Archaeology, as defined by Foucault, points to the analysis of facts of discourses and discourses "as an event or as a set of events." This is a tactical decision to disregard the critical impulses to see in what we look at, what we already know. As Foucault eloquently pleas, we need to clear our minds of all the "unquestioned continuities by which we organize, in advance, the discourse that we are to analyze"[6] from tradition, influence, development, evolution, sprit to book, oeuvre, and author. This is a conscious attempt to let a new way of linking statements emerge from their strange and unexpected juxtapositions. Foucault reads with equal interest philosophical works, such as Bentham's panopticon, as well a detailed list of chores at a school or a 1775 news clipping about a public execution. These diverse texts, as Roger Deacon contends, are not looked at "merely as 'literature' (and, as such, largely devoid of truth), 'philosophy' (accurately reflecting reality), or 'law' (delimiting practice), but as both conditions and effects of the period in question."[7] This dual role of conditions and effects, makes any text or practice potentially meaningful for a rhetorical analysis. I am not suggesting a

wholesale rejection of our critical vocabulary or mimicking Foucault's methods. Foucauldian rhetoric is a critical orientation rather than a method proper; what I want to define is an impulse, a way to approach rhetorical objects, an approach that perhaps also constitutes these objects in the process. Foucault's insight into receiving "every moment of discourse in its sudden irruption"[8] is valuable particularly when what we are after are the intricate interplays between power, knowledge, and subjectivities that inform our present. In the concern for the present, genealogy becomes relevant.

Genealogy as "both the reason and the target of the analysis of discourses as events" traces how the discursive events have determined in particular ways our present and our subjectivities. "Genealogy," concludes Foucault, is "the aim" of the analysis while Archaeology is "the material and methodological framework."[9] Thus archeology is not displaced as much as "widened" by the genealogical approach, which seeks to investigate "how people are constituted and recognized as subjects."[10] This is a dual task, of looking back (archeology) in order to trace the lines of emergence of particular practices (genealogy). "In each apparatus [dispositif]," contends Deleuze, "it is necessary to distinguish what we are (what we are already no longer), and what we are in the process of becoming: *the historical part and the current part.* History is the archive, the drawing of what we are and what we are ceasing to be, whilst the current is the sketch of what we are becoming."[11]

Foucauldian rhetoric also begins with a concern for the present, with problematizations. For Foucault himself, problematization "doesn't mean representation of a pre-existing object, nor the creation by discourse of an object that doesn't exist. It is

the totality of discursive or non-discursive practices that introduces something into the play of true and false, and constitutes it as an object for thought (whether in the form of moral reflection, scientific knowledge, political analysis, etc.)."[12] Problems and solutions become a way to carve out the issues we are interested in; "why?" and "how?" something becomes visible, becomes a problem. The present and its problematizations become a way to trace the emergence and transformations of cultural practices that engender our current conjectures. In other words, "how and why, at specific times and under particular circumstances, certain phenomena are questioned, analyzed, classified, and regulated, while others are not."[13] Problems emerge. As Foucault notes, "for a domain of action, a behavior, to enter the field of thought, it is necessary for a certain number of factors to have made it uncertain, to have made it lose its familiarity, or to have provoked a certain number of difficulties around it."[14] Consequently, for Foucault, the task of the history of thought is to rediscover at the root of all the solutions

> The general form of problematization that has made them possible … or what has made possible the transformation of the difficulties and obstacles of a practice into a general problem for which one proposes diverse practical solutions. It is problematization that responds to these difficulties, but by doing something quite other than expressing them or manifesting them: in connection with them, *it develops the conditions in which possible responses can be given*; it defines the elements that will constitute what the different solutions attempt to respond to. This development of a given into a question, this transformation of a group of obstacles and difficulties into problems to which the diverse solutions will attempt to produce a response, this is what constitutes the point of problematization and the specific work of thought. [15]

Problematization can be understood in another, complementary way. Problematization is also a way to characterize the critical act. The critical act is a way to problematize to bring something before thought, to make something visible. Indeed, as Foucault contends, "thought is not what inhabits a certain conduct and gives it its meaning; rather, it is what allows one to step back from this way of acting or reacting, to present it to oneself as an object of thought and to question it as to its meaning, its conditions, and its goals." [16] "Thought is freedom" proclaims Foucault "in relation to what one does, the motion by which one detaches from it, establishes it as an object, and reflects on it as a problem." [17] In other words, problematization refers both to "the way in which specific historical practices give rise to our condition the emergence of objects of analysis … themselves … an amalgam of experiences …. discourses …. practices …. and institutions" and to "the ways in which genealogy and genealogists are able to transform a 'given' into a question and, in so doing, require the rethinking of politics, philosophy, and ethics."[18]

For this project, then, the point of departure is the emergence of unauthorized information sharing—as in disclosures/leaks—as a problem in our digital present. Truth-telling, whistle-blowing, treason, terrorism, government, corporations, consumers, surveillance, "freedom fighters," technologies and digital practices all intersect into the emergence of an old problem—transparency in governing—with a new twist brought about by the unruliness and permeability of the digital systems and the accessibility of information. Politics is confronted now with the permeability of truth. Despite the "digital" in all of this, the narrative is a familiar one –governments, surveillance,

discipline and control, versus transparency, democracy, and the informed consent of the people. To put it simply, we are in the midst of a *problematization of truth, in a digital world*. Institutions, practices, discourses, technologies, and mode of subjectivation intersect. The permeability of the digital systems that allows a greater access to information is a revolving door; the nebulous legal framework unable to catch up with the technological evolution allows a greater access to information about citizens than ever before and leaves governments and their secrets vulnerable to disclosures. The project indeed spans great vistas of discourses, spread across a hundred years, and across genres from legal discourses to internal documents to interviews and statements. This selection is also animated by archeological impulses. The documents assemble into formations that rest on their existence and circulation rather than on their meaning and their origin (authors/speakers). Ultimately, to speak of genealogy, I try to chart these formations with an eye towards figuring out how these discourses deal with the present problematization of truth in relation to governance.

(2) Foucauldian Rhetoric's own conceptual logic is that of bricolage. In other words, it is a contingent and eclectic assemblage of concepts from rhetorical studies and Foucault's own work. This is the reason why I speak of a critical sensitivity or orientation rather than a method proper. The conceptual logic of bricolage was "authorized" by Foucault himself in the oft cited excerpt about a conceptual *toolbox*. Thus Foucault states,

> I would like my books to be a kind of tool-box which others can rummage through to find a tool which they can use however they wish in their own area... I would like the little volume that I want to write on disciplinary systems to be

> useful to an educator, a warden, a magistrate, a conscientious objector. I don't write for an audience, I write for users, not readers.[19]

It is this logic that connects all the analysis unfolding in the subsequent chapters. Chapter Two charts the emergence and traces the genealogy of the current debates about truth in and about governance through 100 years of legal discourse, sketching the seemingly competing discursive logics of a "will to truth in politics" and "national security" using the conceptual apparatus detailed in Foucault's famous *Discourse on Language*. This theoretical text, an overview of future avenues of research, and thus bereft of evidentiary support, provides us nonetheless with a comprehensive list of concepts, some undeveloped by Foucault himself, that have the potential to be reactivated in a rhetorical analysis/genealogy of how we have come to argue in these ways about the current scandals revolving around unauthorized disclosures. Chapter Three assembles a different set of concepts to chart the logic rhetorically articulated in the development of the government's "insider threat" program implemented throughout all government agencies and redesigned to include the leakers alongside the spies. Here, it is *Discipline and Punish* that provides the background theoretical and methodological text against which the government's attempt to define the insider threat and devise a system of surveillance and intervention begins to make sense. Particularly, I isolate the figure of the delinquent and the shift that Foucault describes in the procedures of punishment from crime to criminal, from the author of the crime to the individual with the propensity to commit a crime as the new target of intervention. And finally, Chapter Four moves forward in time to Foucault's last seminars, his "greco-latin trip" as he himself dubbed it, whereby the

intersection between rhetorical studies' concerns and Foucauldian ones are overtly the closest: the interrogation of the ancient concept and practice of *parrhesia* as the courage to speak the truth. As we can see, the toolbox approach, or obeying the conceptual logic of bricolage, provides the methodological freedom and enhances the ability of the critic to adapt to the shifting rhetorical patterns in a large mass of documents.

(3) Foucauldian Rhetoric is posthumanist. Joshua Gunn and Dana Cloud provide a useful taxonomy that allows us to navigate the contentious issue of rhetorical agency.[20] The authors cluster rhetorical criticism scholarship around three distinct perspectives on agency: (a) the humanist tradition centered on the rhetor as the origin or discourse, thus possessing agency; (b) the post-humanist paradigm that starts with the deconstruction of this conscious autonomous agent and attends to the agency of structures (institutions, language, etc.); and (c) the dialectical perspective which offers a way out of this dichotomy by positing agency as the interaction between agent and structures.

Foucauldian rhetoric works thus from within the posthumanist tradition as Foucault's work has been associated primarily with the posthumanist tradition in rhetorical studies. Chris Lundberg and Joshua Gunn provide a short yet comprehensive excursus through the theories of three philosophers most often associated with post-humanism: Derrida, Lacan, and Foucault.[21] What the works of these particular authors do, according to Lundberg and Gunn is to point to the radical contingency of the subject, its fragmentary qualities, and its dependence on structures and systems beyond the individual consciousness. However, as the authors rightly point out, even the great "masters of suspicion" credited with pronouncing the death of the autonomous/rational

subject, do not deny the subject a certain social effectivity; indeed, "few would deny agency exists." As Gunn and Cloud contend, a perspective that claims as its theoretical background the post humanist turn is based on decentering the all-powerful, choice driven, radically free subject and attends to large forces at play, with structural, material and discursive formations that limit or constitute the subject.[22]

Dilip Parameshwar Gaonkar is among the first critics to unpack Foucault's concept of discourse for what we would inclusively call the communication studies field. He sums up the lessons we need to learn from Foucault, lessons that very much inform this critical sensitivity. Gaonkar defines three of rhetoric's temptations problematized by the encounter with Foucault: the *egological*—the humanistic temptation par excellence through which by establishing the sovereignty of the subject we discover "behind what is said the intention of those who said it;"[23] the *teleological*— "the source of our obsession with continuities and of our fear of unfilled discursive spaces" which means denying the singularity of the events; and the *hermeneutic* temptation—which "promises the inexhaustible presence of the logos."[24] These, as Gaonkar notes, are remarkably resilient for "they promise the illusion of identity in the face of difference, the illusion of order in the face of chance, the illusion of unified self in the face of its dispersion."[25] As my narrative goes, we need to think of how rhetoric is transformed by this encounter, not simply what is compatible and what is not compatible with rhetoric. For Gaonkar, against the hermeneutic temptation, Foucault proposes to "substitute the notion that discourses are limited practical domains which· have their boundaries, their rules of formation."[26] In the space "vacated" by the teleological temptation, Gaonkar points to Foucault's analysis

of the play of discontinuities and differences. Finally, the space vacated by the founding subject is, for Gaonkar populated now by "'discoursing' subjects."[27]

This reading of the transformative encounter between rhetorical studies and Foucault establishes the initial coordinates of the posthumanist impetus in Foucauldian rhetoric: first a decentering of the subject – replacing it with "discoursing subjects" – which means that, at the very least, a Foucauldian rhetoric speaks of subject positions; second, a more sensitive orientation toward discursive events as events–bypassing the host of concepts that organize the field before our encounter with the object; and third, sensitive to circulation of discourse, institutional uptakes, formations – as opposed to the hidden meaning. These propensities, part of Foucauldian Rhetoric as a critical sensitivity, are translated into the critical act in this project as an interrogation of themes, of articulations between concepts and practices, rather than interrogating meaning and motives, situations or speakers. This project charts vast domains of discourse from a hundred years of legal documents defining freedom of information and secrecy, to internal documents across stage agencies defining the insider threat, to interviews and statements by two of the most prominent names at the heart of these scandals, Manning and Snowden. While certainly speakers and authors populate these pages, the theoretical explanations and the methodological inquiries make use less of intentionality and the act of speaking than they do of the existence of statements and the circulation and span of discourses across times and domains (hence, posthumanist.)

(4) Foucauldian Rhetoric sheds the logic of influence for the logic of articulation. Traditionally, the constitutive elements of rhetoric have been the speaker, the speech, the

audience, and the occasion. Thus, rhetoric as a practice (oratory) is seen as an exchange of influence from speaker via speech to the audience, a sort of quantum of energy traveling though language representations to induce movement. The speaker's intention to sway people one way or another (forensics), to move them to action (deliberative) or to inspire them (epideictic), materializes into speech which, depending on the ability of the speaker to find "the best available means of persuasion", achieves its goal or not. As Biesecker notes, "this long-held conception of the rhetorical situation as an exchange of influence defines the text as an object that mediates between subjects (speaker and audience) whose identity is constituted in a terrain different from and external to the particular rhetorical situation."[28] The speaker and the audience are presupposed to be fully constituted subject with a fixed identity, meaning "stable subjects whose relationship is mediated by language."[29] Thus, beside the linear model of persuasion undergirding the logic of influence, this perspective on rhetoric also implies a commitment to an untenable conception of subjectivity. As Biesecker further points out, "if any symbolic act is no more than an event that links distinct and already constituted subjects, then rhetorical discourse bumps up against the impenetrable and unalterable space of the subject."[30] Such an essentialist view of subjectivity, contends Ronald Greene, "figures the subject as possessing a substance outside of history, a substance that is always already present, no matter the contingent rhythms of political, cultural and economic history."[31] If we are dealing with unalterable substances (as in stable subjects) the result can only be cooperation or coercion, "cooperation if the two substances are working toward a similar goal, and coercion if the two are working at cross purposes." [32]

Thus, on one hand, we have Lloyd Bitzer's seminal essay "The Rhetorical Situation," in which he argues that rhetoric is situational in that "rhetorical discourse comes into existence as a response to situation" and a situation is rhetorical "insofar as it needs and invites discourse capable of participating with situation and thereby altering its reality."[33] As Biesecker notes, rhetorical discourse becomes an "effect structure" whereby its coming into existence "is determined by and takes its character from the situation that engenders it."[34] On the other hand we have Richard Vatz's response that turns Bitzer's thesis on its head. For Vatz "rhetoric is a cause not an effect of meaning" and consequently discourse names/defines and makes salient the situation and not vice versa. However critics position themselves in relation to this debate, Biesecker contends, all presume "a causal relation between the constituent elements comprising the event as a whole."[35]

Biesecker shows that the dichotomy between realists (real existing situations determining their own appropriate rhetorical responses) and social constructivists (it is in the act of naming that situations becomes salient) is an unproductive one. With the help of Derrida's concept of *differance* Biesecker transcends this dichotomy and questions influence as the governing logic of the rhetorical situation by destabilizing the notion of an autonomous subject. If *differance* marks a difference between all the elements of a system as well as a temporal deferral within each element, that means that from text to identities, we have instead of an origin, an empty space and a relationship between elements rather than an element, which is covered up. Speaker and audience become immanent to the rhetorical situation; they are elements of the rhetorical situation that are

at the same time effects constituted in the very interplay between the elements of the rhetorical situation. Their identity does not preexist the rhetorical situation, for "once we take the identity of audience as an effect-structure, we become obliged to read every 'fixed' identity as the provisional and practical outcome of a symbolic engagement between speaker and audience."[36] As Biesecker intimates, "the deconstructive displacement of questions of origin into questions of process frees rhetorical theorists and critics from reading rhetorical discourses and their 'founding principles' as either the determined outcome of an objectively identifiable and discrete situation or an interpreting and intending subject."[37]

Articulation is a way to understand complex phenomena without appealing to causality but focusing rather on the ways in which things contingently connect to each other. In her deconstructive reading of the rhetorical situation Biesecker argues that "the rhetorical event may be seen as an incident that produces and reproduces the identities of subjects and constructs and reconstructs linkages between them."[38] Taking his cue from Laclau and Mouffe, DeLuca advocates for a wholehearted embrace of articulation theory as it provides "contingent grounds for a fundamentally rhetorical understanding of the postmodern world."[39] Thus, through importing Laclau and Mouffe, articulation is any practice establishing a relation among elements, relationship that changes the identity of the elements. Elements do not have an essential meaning. Thus, for DeLuca "the linking of elements into a temporary unity is not necessary, but rather is contingent and particular and is the result of a political and historical struggle." [40] Grossberg contends that articulation is "the production of identity on top of differences, of unities out of

fragments, of structures across practices. Articulation links this practice to that effect, this text to that meaning, this meaning to that reality, this experience to those politics."[41] The sovereign subject with its motives and intentions, its skills and performance no longer explains the relationship between the elements of a rhetorical situation. DeLuca contends that "in a world without foundations, without a transcendental signified, without given meanings, the concept of articulation is a means to understanding the struggle to fix meaning and define reality temporarily"[42] Speaker, speech, audience, situation are all in flux, contingently linking to each other in different way, in different historical contexts, with different outcomes.

Articulation is scalable from how meaning is created to "the role of discourse in the constitution of the social world" and to how elements in an apparatus of government relate to each other. Greene proposes a new materialist understanding of rhetoric by appealing in part to the shift from a logic of influence to a logic of articulation. Of particular interest here is Greene's Foucauldian inflected use of articulation. Foucault identifies four types of technologies, "each a matrix of practical reason: (1) technologies of production, which permit us to produce, transform, or manipulate things; (2) technologies of sign systems, which permit us to use signs, meanings, symbols, or signification; (3) technologies of power, which determine the conduct of individuals and submit them to certain ends or domination, an objectivizing of the subject; (4) technologies of the self, which permit individuals to effect by their own means, or with the help of others, a certain number of operations on their own bodies and souls, thoughts, conduct, and way of being, so as to transform themselves in order to attain a

certain state of happiness, purity, wisdom, perfection, or immortality."[43] If we associated rhetoric with technologies of sign systems and if "these four types of technologies hardly ever function separately," [44] rhetoric becomes part of a larger network of interactions between discursive and nondiscursive elements. Greene thus theorizes the governing apparatus as an "ensemble of human technologies dedicated to improving the welfare of a population."[45] Rhetoric does not mediate between stable subjects (speaker and audience) but links elements together; it links problems and solutions, institutions and populations, and so on.

For the purpose of my project, then, understanding what a text means is less relevant from this perspective than charting the text's articulations with nondiscursive practices within social apparatuses. Thus, Foucauldian rhetoric is less interested in decoding representations. In this respect, there are roughly three ways in which we can read a text. First, what could be called, a hermeneutic approach wherein we read and decode meanings and intents, hidden meanings and manipulations, or the actual said behind the said—to use Foucauldian speak. Second, what I would call symptomatic. The best analogy for this approach is psychoanalysis. Here the text is a symptom of a deeper, unknown condition. The intents and motives of the speaking subject become irrelevant for the act of reading for the actual meaning is unknown to those who utter the words as well; the critic, as analyst, sees the workings of ideology, of capitalism, of patriarchy, of institutional racism in the most innocuous words and images—to use the famous Lacanian statement about the unconscious, "in you more than you." Third, a way of reading we could call articulatory. If the first two are representational as in, the texts

represent something else, or *reading the unsaid behind the said*, as Foucault would critically put it, an articulatory reading attends to surface, to circulation of text, to their articulation to apparatuses, to practices, to their institutional uptake; it doesn't look at the origins of texts (intents, motives) nor to their effects (what this or that text cause to happen in the world) but how they link up with nondiscursive practices, with structures of power, with modes of knowledge, and with modes of subjectivity.

Greene's discussion of YMCA movies is an eloquent example of an articulatory reading for it is less important what the Y movies are portraying—as there is no analysis of their content—but how the movies circulate, how they unfold in practice, what is the institutional site for their display, how do the YMCA secretaries' voices interact with the movie to educate the new immigrant working class, what are the effects of linking these movies, in these sites, with these audiences, in these times.[46] It is a similar impulse that guides my reading of these documents, to see how rhetoric travels, how systems of surveillance feed off of behavioral science, how they justify post facto their implantation and how their functioning engenders new avenues of research. Ultimately, I read in the assemblage of these texts the horizon of the thinkable and the sayable in relation to the democratic desire for access to information and right to speak as well as in relation to the governmental rational of secrecy and national security.

(5) Foucauldian Rhetoric is sensitive to the subtle relations between subjectivities, powers, and knowledges allowing the mapping of apparatuses and thus a better understanding of the role rhetoric plays in relation to these elements. So, what is an apparatus? Foucault defines the term comprehensively in an interview as:

> firstly, a thoroughly heterogeneous ensemble consisting of discourses, institutions, architectural forms, regulatory decisions, laws, administrative measures, scientific statements, philosophical, moral and philanthropic propositions - in short, the said as much as the unsaid … the apparatus itself is the system of relations that can be established between these elements … Secondly, what I am trying to identify in this apparatus is precisely the nature of the connection that can exist between these heterogeneous elements … Thirdly … a formation which has as its major function at a given historical moment that of responding to an *urgent need.* The apparatus thus has a dominant strategic function."[47]

We have, thus, a heterogeneous ensemble of elements, an ensemble of elements fulfilling a specific function, of which rhetoric is but one, an ensemble that connects in different ways, an ensemble that comes together to make sense, to control, to solve an issue. Therefore, we have complex interactions between discursive and nondiscursive elements. Foucault reliance on the word technology via the ancient Greek *tekhne* as "a practical rationality governed by a conscious goal," might explain the logic governing the interactions between all these elements. We should not reify this logic however and conceptualize it as able to control the interaction or originating from one agent, but more in a vague manner as "makes sense" to do "this" now in order to solve "this" issue. Thus, if at first the apparatus comes together under the "prevalent influence of a strategic objective" and next it is "constituted and enabled to continue in existence insofar as it is the site of a double process …. a process of *functional overdetermination,* because each effect-positive or negative, intentional or unintentional- enters into resonance or contradiction with the others and thereby calls for a readjustment or a re-working of the

heterogeneous elements that surface at various points. On the other hand, there is a perpetual process of *strategic elaboration."*[48] In a strange way, this rationality and goal do not preexist the apparatus but emerge historically alongside with it. In other words, this "making sense," this strategic objective, this goal that acts as a loose logic of articulation between all these elements is also in a sense thrown back into the mix, becomes part of the interactions, it morphs, it evolves, it changes with the relations while at the same time, at no point being able to fully control the connections. Foucault gives the example of the prison system as one such dispositif/ apparatus that comes into existence for a specific purpose and unexpectedly creates the delinquent milieu, leading paradoxically to the professionalization of the criminals.

There are thus two elements that we need to focus on: (1) the complex interaction between the discursive and nondiscursive and (2) the practical rationality governing these interactions. For Foucault, thus, the *strategic* nature means that this is "a matter of a certain manipulation of relations of forces, either developing them in a particular direction, blocking them, stabilizing them, utilizing them" and thus "always inscribed in a play of power" as well as "always linked to certain coordinates of knowledge which issue from it but, to an equal degree, condition it." The dispositif (apparatus) thus consists of "strategies of relations of forces supporting, and supported by, types of knowledge." [49]

The problem of leaks is certainly one of *the* problems of our political present. The frequency and the importance of the revelations brought about by leaks is something that cannot be ignored. Orwell, for those inclined to use fictional analogies, and Nixon, for those who use the past as prologue, become shorthand for the current government

infringement on the rights of the people. Indeed, leaks have become an integral part of political strategies. On one hand, the content of these disclosures becomes an overt part and justification for political demands—for privacy, for transparency, for limiting the government's ability to use national security as a blanket permission to curtail rights. On the other hand, the government itself strategically uses leaks to engender a favorable political milieu for itself. Both the Bush and the Obama administrations have been accused of being surprisingly restrained in prosecuting leaks that shed a positive light on their activities (the Valerie Plame scandal or leaks about Al-Qaida plots revealed in part by NSA surveillance in the midst of the scandals about the NSA surveillance.) Nonetheless, leaks are overtly considered a problem by government and thus engender the emergence of apparatuses designed to deal with them. Particularly in Chapter Two, an insider threat apparatus emerges as a heterogeneous ensemble of discourses, institutions, scientific statements, and so on, responding to the urgent need of anticipating leaks before they happen. This dominant strategic function then assembles discourses, knowledges, and systems of surveillance and intervention. Next, I will detail the arguments unfolding in each chapter.

"The Map is not the Territory"

The successive scandals related to the unauthorized disclosures of classified materials of the past 10 years have reanimated the debate of what we can and should know about our own governance. While these scandals certainly breathe new life into these disputes about information—the right to access it, the freedom to convey it, and its democratic significance—these debates are certainly not new. Chapter Two, titled "'The

Fellowship of Discourse:' Secrecy, Disclosures, and Dangerous Discourse in US Jurisprudence and Legal Practice" situates the current scandals in the long and contentious history of truth of and about government. For a hundred years now, with the emergence of laws governing military secrets in time of war—*Defense Secrets Act of 1911*—public discourse begins to reflect a tension in relation to truth of and about government. I trace this tension through an eclectic group of objects raging from legal acts—such as the *Freedom of Information Act* (FOIA), Executive Orders on National Security, Whistleblower Protection Act, and The *Espionage Act*, with their attendant historical developments—all the way to Nixon's secret tapes, Manning's sentence and the Pentagon study on the damage caused by Snowden's revelations. Foucault's assumption in *Discourse on Language* that discourse is never allowed to flow freely and that it is controlled, selected, organized, and redistributed though society, provides the theoretical lens through which these documents are scrutinized.

The chapter traces this tension between two distinct logics organizing the understanding of the relationship between the governed and the governing: the "will to truth in politics," animating our ideas of transparency and accountability, of freedom of speech and of information, and thus, ultimately, of consent of the governed, and "national security" articulating the themes of a dangerous world to secrecy and security. Ultimately, despite the differential awareness of their prohibiting effects, I argue, both the will to truth in politics and national security work as rarefaction strategies resulting in a multilayered architecture of access to information that operates a division of the discursive field of and about government into licit and illicit objects of discourse, licit

and illicit circuits of discursive flow, and authorized and unauthorized subjects. The next two chapters explore the split along this line of tension in regards to the speaking subject. If the whistleblower is the subject personifying the *will to truth in politics*, the insider threat is the corresponding speaking subject of *national security*. The first is celebrated for discoursing, the other prosecuted for the same act. However, as these disclosures scandals have shown, these two distinct legal subjects tend to overlap.

Thus Chapter III, titled "The New Delinquent of the Digital Age: The Whistleblower as 'Insider Threat,'" explores the institutional rhetoric pertaining to subjects speaking out of turn. It is in the government institutions, at the intersection of power and knowledge where causal links are posited between behaviors and the potential to do harm, where the sketch of the potential leaker emerges. The attempt to isolate this figure is anchored is the Executive Order 13587 October 7, 2011, the presidential act that sets in motion a series of institutional attempts to define and ultimately contain the insider threat. Mirroring the shift Foucault described in *Discipline and Punish*—from punishing the crime to knowing the criminal—I trace through several government documents the emergence of the leaker as insider threat that must be known, must be put under surveillance, and must treated or excised before the disclosure happens. The result is an "insider threat apparatus," an assemblage of problems (disclosures), of methods of inquiry, of techniques of surveillance, of discourses and authorities, whose logic of functioning is metonymical. This translates into extracting behavioral patterns and psychological predispositions from apprehended insiders (spies and saboteurs) and transforming them into signifiers of delinquency. This is what I call a new *semiotics of*

dangerousness that becomes materialized in new systems of surveillance and intervention.

In Chapter Four, titled "'But what of the Man?' From Manning to Snowden, the Leaker as Parrhesiastes," I explore how (in)famous leakers think and speak of themselves and of their actions. Public statements and interviews by two of the most prominent leakers, Chelsea Manning and Edward Snowden, make up the texture of this chapter. The concept of *parrhesia*, as theorized in rhetorical studies and by Foucault himself, provide the theoretical guide through these texts. The focus is not so much to determine if these specific speakers are indeed *parrhesiastes* as it is on sketching how the leakers construct themselves in relation to something akin to courageous truth telling. Through these highly publicized cases, we can see thrown back into political and rhetorical play the ancient concept of *parrhesia* as the courage to speak truth to power in public.

Leakers rhetorically situate themselves in the gap between an Orwellian world built upon economic, military, and technological might, and the vision of a transparent society built around the public good and reliant on informed citizenry. In their discursive self-portrayals, the disclosures function in a similar way to *parrhesia* in Ancient Greece: it is predicated upon exposing corruption and it has the same formal characteristics—duty, it exposes one to danger and thus requires courage, and it is done in the interest of the people. As such disclosures are posited to function as a counterbalance to the official communique, to the media spin. The leakers, thus, translate their actions within the logic of a will to truth in politics.

Chapter II

"The Fellowship of Discourse:" Secrecy, Disclosures, and Dangerous Discourse in US Jurisprudence and Legal Practice.

> I am supposing that in every society the production of discourse is at once controlled, selected, organized and redistributed according to a certain number of procedures, whose role is to avert its powers and its dangers, to cope with chance events, to evade its ponderous, awesome materiality.[50]

Foucault's generalized pronouncement on discourse translates, in this chapter, into a rhetorical and critical perspective on the issue of unauthorized disclosures of classified material. I want to focus here on politics as a discursive domain and the issue of truth in politics, as it becomes problematized by these disclosures (meaning "leaks"), as a specific object. I consider the problem of disclosures, exacerbated in a digital milieu, as an issue of truth and truth-telling. In an epistemological sense, as an equivalence between words and things, the leaked documents can be said to be "true." Their veracity is not questioned by the government as they are generally considered to accurately reflect the invisible, and sometimes controversial, operations of the government apparatus. While the truth (accuracy) of these documents might not be contested, its disclosure to the public (truth-telling), however, is contested. The leaks of classified documents bring to the surface the tension between transparency, as the democratic desire for accountable power structures, and confidentiality, as a principle of governance. To put this tension in pop-culture terms, the intrepid FBI agent Fox Mulder of the infamous "X-files" on one

hand, the conceited Colonel Nathan R. Jessup from the military courtroom drama "A Few Good Men," on the other. Two characters giving rise to two of the most popular one liners about truth. On one hand we know "*the truth is out there*," on the other we are told we "*can't handle the truth*." First, the quintessential "democratic" attitude—holding power under perpetual suspicion, finding in its own frustrated attempts its *raison d'etre*—second, the patriarchal/paternal care of state institutions—designed to shield citizens/children from the necessarily obscene underside of a functioning democracy, finding in its own failures via exposure the confirmation of its necessity.

Despite what appears to make these two positions radically different, both, I claim, are powered by the same conviction. Whether we think of the Watergate scandal with its attendant collapse of a US presidency, or the alleged loss of US life, prestige, and ability to defend itself as a result of unauthorized disclosures, whether we think of *parrhesia* or treasons, whistleblowers or spies, whether it needs to be revealed and/or protected, whether it needs to burst into consciousness as the "innocent" cry about the emperor's new clothes, whether its flow must be controlled and its unfolding meticulously choreographed, one thing is clear: *truth is powerful, truth is dangerous; its presence in the public sphere is never inconsequential*. So, if we agree that the issue of unauthorized disclosures brings to the surface the varied ways in which discourse of and about the functioning of state institutions is controlled, and that both the attempt to make it public and the adamant efforts to keep it secret function based on the same presumption of dangerousness, we can conclude that there is no better critical lens for this issue than Foucault, as eloquently stated at the beginning of this chapter.

Disclosures bring into the political fray not only issues of access to information and freedom of speech, they also problematize the citizen-subject in relation to information pertaining to its own governance. Who can know the truth and who can speak the truth? With what effect and what consequences can truth be spoken? What are the predetermined licit and illicit pathways through which truth circulates, can circulate and/ or must be prevented from circulating? Who can know, speak, and/or listen to the truth? Illegal disclosures bring to the surface the contested ground of how information circulates and how citizens are distributed as speaking, listening, and knowing subjects in relation to truth in a democracy. Who can and cannot speak , who is authorized to address and who is barred from addressing the public on matters of national interest and security, like the double helix, dance around each other, in mutual determination, in an upward spiral through US history, through policies, laws and executive orders, though supreme court decisions and media spectacles. In order to chart this contested ground, where *speech is powerful and dangerou*s, I will trace in US jurisprudence and legal practice several threads concerning the prohibition of objects of discourse (what can be known, under what circumstances, through which procedures) and the rarefaction of speaking subjects in relation to truth of and about government (who can be in the know and who can speak, and what consequences are reserved for those who speak out of turn).

Foucault's assumption, hinted in the opening quote, is that discourse is never allowed to flow freely, that discourse is controlled, selected, organized, and redistributed though society. So how precisely is discourse controlled? What are, in Foucault's terminology, principles of rarefaction? Foucault speaks of sets of procedures: the first, is

what he calls "systems of exclusion," exterior to discourse attempting to control its production from the outside (*prohibition, the divisions between madness and reason*, and the *will to truth*) concerning "that part of discourse which deals with *power* and *desire*"; the second is what he dubs "internal rules" where "discourse exercises its own control" concerned with "mastery of another dimension of discourse: that of *events* and *chance*"[51] (*commentary*; the *author*; and the *disciplines*); and the third group of rules controlling discourse, is what he calls "rules for the subjection of discourse" (*ritual, fellowship of discourse, doctrine, and education*.)

These sets of rules provide the guiding methodological lens though which I will endeavor to do a genealogy of truth in and of governance. What I want to draw out, using this Foucauldian perspective, is how true discourse of and about government is controlled, what are the procedures put in place for its containment, as well as the legal attempts to define the subject who can know and speak (the whistleblower) and the punishment reserved for the subject who breaks these rules (the spy/criminal). Thus, I will talk first about institutions, laws and policies forming a complex system of access to information, particularly as exemplified by the legislative evolution of the *Freedom of Information Act*, a veritable manifestation of what I call, in a ludic dialogue with Foucault's notion of the will to truth, a "will to truth in politics." Second, I will scrutinize the laws that define the subject and the rituals of benign disclosures, such as the Whistleblower Protection Act. Third, I will explore laws that define the subject and the rituals of punishment for unauthorized disclosures, particularly in respect to the 1917 Espionage law that, even today, is the default legal act invoked in the prosecution of

national security whistleblowers. Finally, I will deal with a varied set of objects, from secret White House tapes to indictment documents on the public prosecution of recent cases of whistleblowers, as show trials, as public rituals of punishment of disclosures that, together showcase the notion of dangerous discourse.

Controlling Discourse

Before we proceed with the analysis of these legal acts, a more developed understanding of the critical tools, inspired by Foucault's vision for the study of discourse, is in order. At the heart of the existence of all the systems of control described by Foucault is the idea that discourse introduces something new and perhaps unruly into the world that we need to cope with. It is along these lines that I follow Foucault when dealing with disclosures of confidential information and the legislative web that develops around the issue of truth in the public sphere. Foucault's theoretical musings in *Discourse on Language* allow me to interrogate 100 years of legislative history and practice about what can be known regarding the inner workings of government, who can speak that knowledge, and with what effects.

As briefly mentioned above, Foucault talks about three groups of rules that control the production of discourse, regulate its proliferation, and control its social distribution. The first set of rules, under the label, exclusion, are of course *prohibition*, the *division between reason and madness*, and what he calls a *will to truth*. Particularly, for my project, I am interested in prohibitions and the will to truth. When it comes to prohibitions, to put it simply, not everyone can talk about everything, everywhere, all the time. Foucault contends that there are three types of prohibitions: covering objects (what

can we speak about, as in categories of information in FOIA), how can we speak about these things (or what Foucault calls "rituals with its surrounding circumstances" – as in legislation detailing the rituals of legally disclosing information), and those pertaining to the speaking subjects, granting "the privileged or exclusive right to speak of a particular subject" (only some people have access—closed sessions and committees—and only some can claim the label whistleblowers.)[52]

Prohibitions refer to objects, times, places and speaking subjects and these prohibitions "interrelate, reinforce and complement each other, forming a complex web, continually subject to modification."[53] For Foucault, politics and sexuality are the areas "where this web is most tightly woven today, where the danger spots are most numerous." Indeed, contends Foucault, "psychoanalysis has already shown us that speech is not merely the medium which manifests—or dissembles—desire; it is also the object of desire" and "historians have constantly impressed upon us that speech is no mere verbalization of conflicts and systems of domination, but that it is the very object of man's conflicts."[54] This is particularly true when it comes to unauthorized disclosures. These acts contest the government based on the content of these leaks (surveillance, etc.) but they also throw into political play the very act of knowing these things, the very act of speaking these things. Beyond their content, disclosures reveal the disputed ground of what can be known and who can speak.

The second group of rules, are those label "internal" where discourse "exercises its own control," rules "concerned with the principles of classification, ordering and distribution" pertaining to "the mastery of another dimension of discourse: that of events

and chance."[55] Here Foucault points to commentary, the ever-expanding and incessant derivative discourse emerging from an "originary text," the author, as the unifying principle of a group of statements whose post facto existence colonizes our interpretation, and the disciplines, as coherent branches of knowledge that define the coordinates of being "in the true" when making a statement. These conceptual categories, while less relevant for the analysis as direct methodological tools, nonetheless inform my larger posthumanist critical sensitivity employed here.

The third group of rules, designed to control discourse, are those that operate a rarefaction among speaking subjects, a group of rules Foucault dubs of "subjection of discourse." If the first two sets—systems of exclusions and internal rules—are, in Foucault's take, designed to deal with the power of discourse and the "hazards of its appearance," this set refers to speaking subjects. Here, Foucault contends, we are concerned with "determining the conditions, under which it may be employed, of imposing a certain number of rules upon those individuals who employ it thus denying access to everyone else."[56] This, argues Foucault, "amounts to a rarefaction among speaking subjects." Not all "may enter into discourse" on all subjects unless being authorized to do so, in a manner of speaking. Among these system of rarefaction Foucault counts the "ritual," "fellowships of discourse," "doctrine," and "social appropriation," as education.

Thus, the prohibition of objects of discourse, rituals (as the pageantry that must accompany discourses), the rarefaction of speaking subjects, and the fellowship of discourse are the critical vocabulary that allow me to explore, through legislative acts and

debates, and through contentious litigations, what can be known by the public, how it can be known and circulated, who are the subjects authorized to know, who is allowed to hear it, and, in the case of transgressions, what are the consequences for those who mishandle this dangerous speech. These concepts allow me to look at legislation where discourse itself is the overt object of contention, of strategic calculations.

In the light of these concepts, I look at truth of and about government as the contested ground where we can trace a will to truth in politics and a more overt rarefaction strategy labeled "national security." These two strategies are locked in a perpetual struggle to define the overall logic of public discourse on and about government, to define its objects, to trace its pathways of circulation, and to authorize its subjects. Both these logics/strategies are buttressed by several tactics enshrined into law: (1) *prohibition of objects* of discourse; (2) *ritualized access* to information; and (3) *the rarefaction of speaking subjects*, notable in the above mentioned legal acts as well as in those laws defining, protecting and/prosecuting whistleblowers and spies. Traversing both the will to truth as well as the national security strategy is the theme of *dangerous speech*. It is difficult to separate these threads of thought (objects to be known and subjects allowed to be in the know from the notion of dangerous speech) in the legal documents themselves, but I will attempt to use different types of legal documents (FOIA, Whistleblower Protection Act, the Espionage Law, as well as legal proceedings pertaining to the prosecution of famous whistleblowers) to speak in turn of the *will to truth in politics*, of *prohibited objects*, *privileged subjects*, *transgressions*, and finally about *dangerous discourse*.

(1) To Be "In the Know": The *Freedom of Information Act* as Will to Truth in Politics

The *Freedom of Information Act* (FOIA) is a law which "gives you the right to access information from the federal government" and is "often described," as FOIA's own website touts, "as the law that keeps citizens in the know about their government."[57] First, we might muse on the delightful similarity between Canguilhem's "in the true," which Foucault takes as a shorthand for how statements make sense within the complex web of the disciplines, and the Government's own "in the know." Within the third set of internal rules controlling discourses, Foucault talks about, with emphasis added, "*not sciences,* but 'disciplines.'" Disciplines are "defined by groups of objects, methods, their corpus of propositions considered to be true, the interplay of rules and definitions, of techniques and tools: all these constitute a sort of anonymous system, freely available to whoever wishes, or whoever is able to make use of them."[58] It is about the role of formation of new statements. As Foucault notes, "for a discipline to exist, there must be the possibility of formulating—and of doing so ad infinitum— fresh propositions." Propositions must reference a specific range of objects, use accepted concepts and techniques, and fit into a theoretical field,[59] or, to put it simply, "a proposition must fulfil some onerous and complex conditions before it can be admitted within a discipline; before it can be pronounced true or false it must be, as Monsieur Canguilhem might say, 'within the true'."[60] "It is always possible one could speak the truth in a void" continues Foucault, "one would only be in the true, however, if one obeyed the rules of some discursive 'policy' which would have to be reactivated every time one spoke." I endeavor

to treat "in the know" about the government as a *critical synonymy* to "in the true." As I will show, to be "in the know" is a similarly complicated process that must pass through a tightly woven web of authorities, definitions, exceptions, procedures, and so on. To be in the know means to be a certain subject, to look at certain discursive objects, to follow specific procedures, and to live in the carefully choreographed temporality of authorized disclosures.

The *Freedom of Information Act* is a way to talk about institutions, laws and policies classifying information with varying degrees of secrecy that categorize both what kind of information can be known by the public and when. I am not interested in uncovering the hidden meaning of these texts, nor do I assume either an enlightened or maleficent rhetorical motive behind the letter of the law. In Foucauldian manner, I am working in a post humanist tradition, whereby individual speakers, their motives and their rhetorical skills are less relevant as critical explanatory factors as are the act of making statements, how these statements link up to one another forming webs of topologies, classifications, and distributions of discourses. I am also not interested in mapping the ideological fault line that lies at the heart of this debate. As we will see, the expansion and contractions of FOIA sometimes follow the predictable political cycles where conservatives and liberals alternate. Beyond the ideological clashes, this contentious ground can also be mapped as a struggle between the three branches of government where laws, executive orders, and court decisions vie for the ultimate codification of the issue of truth of and about the government. While both are certainly worthy endeavors, I am less interested in the overt disagreements and more so about how the system itself

works. Despite is chronological feel, this section is not so much an attempt to detail a legislative evolution as it is an effort to map the contentious ebb and flow of varied understandings of what it means to be "in the know" about government. Freedom and information are pulled apart or stitched back together as democratic accountability, as a manifestation of the will to truth in politics, and national security, as a rarefaction strategy, alternately gain rhetorical and political prominence. Therefore, instead of talking about ideology, I will talk about rhetorical topoi animating the legislative changes, for these topoi traverse all time periods belonging to this meandering movement of our need to be "in the know" affected by these magnetic poles (democratic accountability and national security.)

So first, what is the will to truth? Foucault talks about a "will to truth" that characterizes Western thought and society. "It is perhaps a little risky" admits Foucault "to speak of the opposition between true and false as a third system of exclusion."[61] Foucault proceeds to tell a beautiful story, to recount the history of a tendency toward truth in history that begins with the division between Hesiod and Plato "separating true discourse from false" leading to the "routing" of the Sophists, continues with the 16th century and the scientific will to knowledge which "sketched out a schema of possible, observable, measurable and classifiable objects … imposed upon the knowing subject … a certain position, a certain viewpoint, and a certain function …"[62] It is as if, suggests Foucault, "the will to truth had its own history, which is not at all that of the constraining truths: the history of a range of subjects to be learned, the history of the functions of the

knowing subject, the history of material, technical and instrumental investment in knowledge."[63] However, as Foucault notes, this will to truth

> like the other systems of exclusion, relies on institutional support: it is both reinforced and accompanied by whole strata of practices such as pedagogy—naturally—the booksystem, publishing, libraries, such as the learned societies in the past, and laboratories today. But it is probably even more profoundly accompanied by the manner in which knowledge is employed in a society, the way in which it is exploited, divided and, in some ways, attributed.[64]

It is this reliance on institutional support that, argues Foucault, "tends to exercise a sort of pressure, a power of constraint upon other forms of discourse."[65] We are thus "unaware of the prodigious machinery of the will to truth, with its vocation of exclusion."[66]

I want to translate this general will to truth into the specific concept, namely a "will to truth in politics." I would briefly define this concept as the tendency to make political demands and lobby for legislation that codifies government transparency as a sine qua non of democracy. For now, I would trace a brief line between Jeremy Bentham and Jürgen Habermas. As Bentham argued, "before entering into the detail of the operations of the assembly, let us place at the head of its regulations the fittest law for securing the public confidence, and causing it constantly to advance towards the end of its institution. This law is that of publicity."[67] We find in Bentham the distrust of government officials is being countered by their permanent surveillance and perpetual recording of everything produced in public. Similarly, for Habermas two crucial elements for a strong and healthy public sphere are transparency and access to media. "Regulations demanding that certain proceedings be public" argues Habermas, "are also

related to this function of public opinion."[68] In his description of the devolution from the process of making things public "intended to subject persons or affairs to public reason, and to make political decisions subject to appeal before the court of public opinion" to the current state of affairs where the process of making public "simply serves the arcane policies of special interests," we note the importance of transparency.[69] The need for transparency or, to translate in my own conceptual apparatus, the need to know the truth about how we are being governed, is a political demand with a long tradition and constant presence in our thinking about democracy. Bentham and Habermas provide here nothing more than two anchoring points for this grand claim about the existence of a will to truth in politics.

(1)(a) Will to truth in politics

The language employed by FOIA in defining its scope and the reason for its own existence, allows me to begin to theorize this *will to truth in politics*. Thus, in 1967, a short two-page law amends section *552 Title 5 of US Code* to allow public access to certain categories of information pertaining to government functioning. Any person gains as a result the right to obtain access to records kept by government agencies, thus "each agency" proclaims the act will "make available to the public" information pertaining to their functioning, provided they do not fall under a list of exemptions.[70] *The Privacy Act of 1974* amended FOIA by adding substantial access, protection, and control to and over one's own information.[71] This addition comes with a clear rhetorical articulation of its foundation. Here privacy is declared a fundamental right protected by the US Constitution. As a result, the collection, maintenance, use, and dissemination of personal

information must be regulated. "The Congress finds that (1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies" and that the digitization of data "(2) has greatly magnified the harm to individual privacy that can occur" and that "(3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems."[72] This act gives increased access to one's own information kept by the government by permitting individuals to determine what records are collected, kept, disseminated, prevent records to be kept without consent; allow individuals access and the right to correct or amend those records; and allow exceptions only if there is an important public policy need. This language hints at the imbalance of power between government and citizens and the potential for abuse as the byproduct of this imbalance. This theme—of the power imbalance and potential for abuse that would certainly follow—is a staple of this will to truth in politics, that stems from and reinforces the long US tradition valuating discourse (freedom of speech) and demonizing government.

The *Government in the Sunshine Act,*[73] amending FOIA by opening state agencies' meetings to scrutiny, articulates both the ideal impetus of FOIA—the *will to truth in politics*—and the tension it tries to balance between democratic accountability and national security. Thus, according to this act, "it is hereby declared to be the policy of the United States that the public *is entitled to the fullest practicable information* regarding the decision-making processes of the Federal Government" and that "the purpose of this Act is to provide the public with such information while protecting the

rights of individuals and the ability of the Government to carry out its responsibilities."[74] The ability of the government to conduct its affairs is counter-posed to the privacy of the individuals and their right to access information. Thus, access to information and individual privacy, on one hand, and the government's ability to function, on the other, become part of a political equation that must be balanced.

The Electronic Freedom of Information Act Amendments of 1996[75] adds to this reasoning, by returning to the original FOIA and defining its overall function as requiring agencies of the Federal Government "to make certain agency information available for public inspection and copying and to establish and enable enforcement of the right of any person to obtain access to the records of such agencies, subject to statutory exemptions, for any public or private purpose."[76] Furthermore, this act also touts some of the most relevant categories of information and issues where FOIA fulfilled its democratic purpose via transparency. "Since the enactment … the *Freedom of Information Act* has been a valuable means through which any person can learn how the Federal Government operates" and has led "to the disclosure of waste, fraud, abuse, and wrongdoing in the Federal Government" as well as "to the identification of unsafe consumer products, harmful drugs, and serious health hazards."[77] At the same time, responding to the digital revolution, the electronic FOIA defines its own purpose in accordance with this vision of transparency and democratic success. Given that agencies "increasingly use computers to conduct agency business and to store publicly valuable agency records," agencies should use this new technology "to enhance public access to agency records and information." Specifically, this act rhetorically articulates its purpose directly onto democratic ideals of

transparency. “The purpose of this act” touts EFOIA are to “(1) foster democracy by ensuring public access to agency records and information; (2) improve public access to agency records and information; (3) ensure agency compliance with statutory time limits; and (4) maximize the usefulness of agency records and information collected, maintained, used, retained, and disseminated by the Federal Government.”[78] Thus, fostering democracy means transparency, means more efficient and direct access to information.

The *Openness Promotes Effectiveness in our National Government Act of 2007*[79] in its findings prefacing the act itself, states that FOIA was signed into law “because the American people believe that (A) our constitutional democracy, our system of self-government, and our commitment to popular sovereignty depends [sic] upon the consent of the governed.” Government does not draw its legitimacy simply from consent – it must be an informed one. Indeed, “such consent is not meaningful unless it is informed consent.” Quoting Justice Black, the authors put forth that “the effective functioning of a free government like ours depends largely on the force of an informed public opinion.”[80] The American people, the authors maintain, “firmly believe [sic] that our system of government must itself be governed by a presumption of openness.”[81] The US Supreme Court is quoted that FOIA “establishes a ‘strong presumption in favor of disclosure’” and that this presumption “applies to all agencies governed by that Act.”[82] The emphasis privileges openness as this act quotes the Supreme Court once more as stating that “disclosure, not secrecy, is the dominant objective of the Act.”[83] What is relevant here is that beyond the stated purpose and the list of FOIA successes, as in the case of E-FOIA,

the Open Government Act situates itself within an intensely litigious evolution towards openness. This is the rhetorical topos of democratic accountability and the presumption of government secrecy as concealing not only legitimately sensitive information but also violations of the law, or fraud and abuse. Tying consent of the governed to access to information speaks to this *will to truth in politics* animating legislation such as FOIA, the First Amendment or the Whistleblower protection laws. In all these examples, access to information, the ability to freely criticize the government, and the ability to expose information are all buttressed by the presumption that government secrecy is always prone to abuse and thus must be kept in check.

Moreover, the act concedes FOIA's failures and thus its character as a perpetual democratic project. Indeed "in practice, the Freedom of Information Act has not always lived up to the ideals of that Act."[84] As such, "Congress should regularly review section 552 … in order to determine whether further changes and improvements are necessary to ensure that the Government remains open and accessible to the American people and is always based not upon the 'need to know' but upon the fundamental 'right to know'."[85] Quoting Supreme Court cases where the decisions favored disclosure over appeals to exceptions, the act places the Congress and the courts as representatives of the people and the government as the authority that must be challenged. The "need to know" and the "right to know" are at war through all these legal acts, though the evolving and amended list of exceptions, through executive orders that limit or expand the division between permitted and prohibited objects of discourse.

This *will to truth in politics* can be discerned in the last version of FOIA, a House bill designed to amend it that has yet to pass the Senate, and thus not quite law yet.[86] The very title of the bill—"to amend section 552 … to provide for greater public access to information"—situates the act once more in this historical process of a continued struggle for transparency on behest of the people. Notable additions that speak to this *will to truth in politics* are new paragraphs that discuss increased disclosures. Thus the paragraph titled "disclosure of information for increased public understanding of the government" tasks agencies to review their records to determine whether their disclosure would be in the public interest "because it is likely to contribute significantly to public understanding of the operations or activities of the Government."[87] We need not only to know what the government does but we also need to understand. This is not simply informed consent but comprehensively knowledgeable consent. The bill also ends with the establishment of an independent "Open Government Advisory Committee" tasked with making recommendation "for improving Government transparency."[88]

A different story is predictably told in the case of the successive executive orders defining national security and its attendant systems of classification. We find here, defined in its short introductions, national security as a rarefaction strategy. This is not the first executive order to deal with this issue, so the beginning of this data set is somewhat arbitrary. That being said, in 1978, Jimmy Carter spoke of what has been labeled the "balancing test." Thus "in order to balance the public's interest in access to Government information with the need to protect certain national security information from disclosure,"[89] the order defines classification types, authorities, expectations, and

procedures pertaining to national security information. Once again, access to truth and national security are placed in the zero sum political equation. The balancing test is an interesting rhetorical topos as it was the subject of subsequent removal from national security executive orders as putting undue burden on the government's need to classify information. Indeed, in Carter's case, the balance tips still in favor of public interest. In his statement accompanying this order, Carter argues that "the public is entitled to know as much as possible about the Government's activities" and that "the Government classifies too much information, classifies it too highly and for too long." The government's tendencies for over-classification "violate the public's right to know, impose unnecessary costs, and weaken protection for truly sensitive information by undermining respect for all classification." In Carter's own words, this order "will increase openness in Government by limiting classification and accelerating declassification" as well as "improve protection for information that needs to be kept secret." Furthermore, argues Carter, "no document is to be classified unless its release reasonably could be expected to cause identifiable damage to the national security."[90] "Identifiable damage" is another rhetorical topos that was eliminated in subsequent order as placing an undue litigious burden on the government. The tension between the democratic accountability—as a manifestation of the will to truth in politics—and national security—as a manifestation of national security as rarefactions strategy—is visible in these lines, with Carter attempting to solve this dilemma in the public's interest.

The language and tenor of the national security information changes with President Ronald Reagan and the executive order 12356. Lacking a signing statement, the

short justification prefacing the order gives us a glimpse into the change of direction in terms of national security. Reagan states that this order "recognizes that it is essential that the public be informed concerning the activities of its Government, *but* that the interests of the United States and its citizens require that certain information concerning the national defense and foreign relations be protected against unauthorized disclosure."[91] With President William J. Clinton, we have another reversal, bringing the act closer to Carter's, and tipping the balance once again in favor of the public interest. Thus, Clinton purports,

> Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information. Nevertheless, throughout our history, the national interest has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, and our participation within the community of nations. Protecting information critical to our Nation's security remains a priority. In recent years, however, dramatic changes have altered, although not eliminated, the national security threats that we confront. These changes provide a greater opportunity to emphasize our commitment to open Government.[92]

The need to be informed tied to democratic principles opens the paragraph. While acknowledging the need to protect information, Clinton contends that the historical circumstances that lead to a restrictive system of classification are dissipating. Over-classification here is considered a historically contingent affair, tied perhaps to the cold war era. Thus, the balance is tipped in the favor of openness and toward public interest once more.

George W. Bush revokes Clinton's order replacing it with his own vision of national security. As stated in the introduction of the order

> Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information. Nevertheless, throughout our history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations. Protecting information critical to our Nation's security remains a priority.[93]

The most notable change from the previous order is the elimination of the changing historical circumstances and the ending that once more tips the balance towards classification and secrecy. From "emphasize our commitment to open Government" we go to "Protecting information critical to our Nation's security remains a priority." Democratic accountability becomes subservient to the need for protecting national security.

The last order to modify the system of classification is Barack H. Obama's order 13526. Obama makes a slight modification to the opening paragraph, stating that

> Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information both within the Government and to the American people. Nevertheless, throughout our history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations. Protecting information critical to our Nation's security and demonstrating our commitment to open Government through accurate and

> accountable application of classification standards and routine, secure, and effective declassification are equally important priorities.[94]

The flow of information is defined here as both within government and to the public. The most notable change is the attempt to achieve a perfect balance between the two. If Carter and Clinton tried to favor public interest and Reagan and Bush preferred an empowered government with tighter control over information, Obama declares "protecting information critical to our Nation's security" and "demonstrating our commitment to open Government" as "equally important priorities." Democratic accountability and national security are valued equally and kept in precarious rhetorical balance.

FOIA, as we have seen, attempts to materialize this "will to truth in politics," but in the case of executive orders, the tension between this will to truth and national security as a rarefaction strategy is negotiated overtly. This tension and its solutions, somewhat predictably split alongside ideological/party lines, with Democratic presidents trying to favor limits of classification and resolving doubt in favor of lesser classification, and Republican presidents trying to empower the government as much as possible to control the flow of information. However, I am not interested in this false dilemma between a repressive hypothesis, as Foucault called it, where power is seen as always prohibiting, and freedom/liberation seen as always allowing. Although different presidents try to solve the political equation in different ways, the idea of a zero sum game cuts across all attempts.

The *need to know* and *right to know* are not in a simple opposition with FOIA, on one hand, perpetually evolving toward greater transparency, and executive orders, on the

other hand, expanding the list of exceptions as the direct prohibition,. As Foucault himself notes, the will to truth itself is a mode of rarefaction, a historically contingent principle of exclusion alongside prohibited words and the division between madness and reason. This will to truth in politics alongside the national security as a strategy of rarefaction, via FOIA and the successive executive orders on national security, construct a multilayered architecture of access, where *truth of and about government* is directed to flow through certain circuits, where the subjects "*in the know*" are clearly defined and identified through legal categories, and timelines for disclosures, while intensely debated ideologically, regardless of the resolution of this ideological debate, tie the public's awareness to a certain historical hindsight. Next, I will chart how FOIA and its correspondent executive orders work to divide the political discursive field into licit and illicit objects of discourse, procedures, and subjects.

(1)(b) Licit and Illicit Objects of Discourse

The rarefaction of discursive objects is evident not only in the act of limiting the categories of information pertaining to national security, of course, but also in the act of naming the categories that are opened for access. It is Foucault's call to critically operate under the principle of reversal that allows to see both in direct prohibitions and in overt acts of opening ways to control discourse. Within the mass proliferation of discourse, Foucault sees a logophobia, "a sort of dumb fear of these events, of this mass of spoken things, of everything that could possibly be violent, discontinuous, querulous, disordered even and perilous in it, of the incessant, disorderly buzzing of discourse."[95] In order to deal with this fear, Foucault proposes three decisions "which our current thinking rather

tends to resist," namely question the will to truth, restore to discourse its character as an event, and abolish the sovereignty of the signifier.[96] These three decisions lead to four critical principles: reversal, discontinuity, specificity, and exteriority. By *reversal* Foucault invites us to see in the principles behind the flourishing of discourse—author, discipline, or the will to truth—"the negative activity of the cutting-out and rarefaction of discourse."[97] Thus, in the original FOIA, there is in one sense an opening up of government and, in another sense, a closing down. These two support each other, that government discourse of which we can be "in the know" is parceled out, divided. A veritable *multilayered architecture of access* is born that controls access to truth about the government.

This is not to say that under the guise of opening, under the pretense of access to information, a purposeful prohibition is nefariously smuggled in. Through the principle of *specificity*, Foucault further elaborates the notion of discourse as a phenomenon not as an epiphenomenon. Indeed, "a particular discourse cannot be resolved by a prior system of significations."[98] Discourse is not the "legible face" of the world, but "violence that we do to things, or, at all events, as a practice we impose upon them."[99] I do not imply that in the list of exceptions there are nefarious motives, nor do I challenge the reasoning behind these exceptions, nor do I operate with an alternative in mind, against which this one reveals its ideological underpinnings. There is no prior system of signification (rhetorical and or/ideological) that allows me to explain these exceptions. What I am interested in is the very existence of these categories of exceptions as well as the division between licit and illicit objects within our public debates about access to information.

Furthermore, the act that in theory allows more people to be in the know about the government limits this activity through a set of exceptions, through clear procedures, and according to predetermined timelines. Here Foucault's concept of *exteriority* becomes useful to map this architecture. Exteriority means that our endeavor to understand discourse must not proceed as an inward movement; we need not "burrow to the hidden core of discourse" but look for its "external conditions of existence."[100] It is precisely this set of exceptions that become the contentious ground occupied alternatively by the topoi of democratic accountability and that of national security setting up the very coordinates within which these debates take place. I am not interested as much in divining the motives or ideology animating discourse as I am in mapping its existence its circulation and material consequences. Based on these principles, Foucault defined his future analysis as falling into two groups—the critical and the genealogical—with the former working with the principal of reversal (seeing rarefaction where we would be tempted to see flourishing) and the latter bringing the other principles into play to chart "how series of discourse are formed, through, in spite of, or with the aid of these systems of constraint."[101] Although these two groups are for Foucault somewhat distinct projects, in my project the critical and genealogical perspectives work in conjunction.

What I am interested in the case of FOIA is what the public can know and what the exceptions to disclosures are, or what the public cannot know. I am not interested as much in debating this distinction and argue that what is licit should not be and vice versa, as I am in the existence of the distinction itself and its operation, the contested ground of licit and illicit discursive objects as classified in relation to disclosure to the public.

FOIA as it is in effect at this time (2014) begins by defining the kinds of information that should be made available to the public. First, each agency will

> publish in the Federal Register for the guidance of the public (A) descriptions of its central and field organization and the established places at which, the employees (and in the case of a uniformed service, the members) from whom, and the methods whereby, the public may obtain information, make submittals or requests, or obtain decisions; (B) statements of the general course and method by which its functions are channeled and determined, including the nature and requirements of all formal and informal procedures available; (C) rules of procedure, descriptions of forms available or the places at which forms may be obtained, and instructions as to the scope and contents of all papers, reports, or examinations; (D) substantive rules of general applicability adopted as authorized by law, and statements of general policy or interpretations of general applicability formulated and adopted by the agency; and (E) each amendment, revision, or repeal of the foregoing."[102]

Each agency will also

> make available for public inspection and copying A) final opinions, including concurring and dissenting opinions, as well as orders, made in the adjudication of cases; (B) those statements of policy and interpretations which have been adopted by the agency and are not published in the Federal Register; (C) administrative staff manuals and instructions to staff that affect a member of the public; (D) copies of all records, regardless of form or format, which have been released to any person under paragraph (3) and which, because of the nature of their subject matter, the agency determines have become or are likely to become the subject of subsequent requests for substantially the same records; and (E) a general index of the records referred to under subparagraph (D);"[103]

And last, alongside the information mentioned above, "each agency upon any request for records which (i) reasonably describes such records and (ii) is made in accordance with

published rules stating the time, place, fees (if any), and procedures to be followed, shall make the records promptly available to any person."[104] The act divides that information and thus its flows, circuits, and accessibility procedures in (1) information that needs to be published by default, (2) information that must be made available, and (3) information that must be requested in order to be made available. Aside from the information that is made public by default, and the information made available, there needs to be a demand, one needs to ask.

There is a problem in conceptualizing the licit object of discourse solely as the pouring out of discourse and illicit object (national security exemptions) as prohibited discourse. Indeed, the idea of informed consent, tied to unbridled access to information, conceals its illusory nature. As we have seen with Cablegate (a quarter of a million of diplomatic cables leaked), and before that with the Iraq and Afghan War logs (together summing up about half a million documents), having access to documents does not really translate into informed consent. The incalculable mass of documents produced by the government makes the idea of keeping everything under scrutiny, ludicrous. Thus this will to truth in politics animating a need for transparency rivaling Bentham's vision meets a bureaucracy capable of producing a quantity of paperwork sufficient to drown the most adamant supporter of transparency, reminiscent of Henry Tuttle's end in Terry Gilliam's *Brazil*, where the character played by Robert DeNiro dematerializes under a vortex of documents and paperwork. Access does not solve this impossible tension any more than prohibition amplifies it.

The first exception of FOIA is, evidently, that pertaining to invasion of privacy. Thus "to prevent a clearly unwarranted invasion of personal privacy, an agency may delete identifying details" with the caveat that the explanation for the deletion must be also given in writing.[105] The comprehensive list of exceptions, is

> (1)(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order; (2) related solely to the internal personnel rules and practices of an agency; (3) specifically exempted from disclosure by statute (other than section 552b of this title), if that statute—(A)(i) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue; or (ii) establishes particular criteria for withholding or refers to particular types of matters to be withheld; and (B) if enacted after the date of enactment of the OPEN FOIA Act of 2009, specifically cites to this paragraph. (4) trade secrets and commercial or financial information obtained from a person and privileged or confidential; (5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency; (6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy; (7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by criminal law enforcement authority in the course of a criminal investigation or by

> an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual; (8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or (9) geological and geophysical information and data, including maps, concerning wells.[106]

This list of exceptions opens up a contentious (at times litigious) terrain of interpretation. All these exceptions, at times phrased in vague language, ultimately empower authorities to make decisions and draw the line between licit and illicit objects, as evidenced by the lawsuits challenging these invoked exceptions.

For a better understanding of prohibited objects of discourse, I turn to the executive order pertaining to classified information. Here, the attempt to prohibit access is overt. Here, the list includes information that must be "expected to cause identifiable or describable damage to the national security" if disclosed improperly and it pertains to the following categories:

> (a) military plans, weapons systems, or operations; (b) foreign government information; (c) intelligence activities (including covert action), intelligence sources or methods, or cryptology; (d) foreign relations or foreign activities of the United States, including confidential sources; (e) scientific, technological, or economic matters relating to the national security; (f) United States Government programs for safeguarding nuclear materials or facilities; (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection

services relating to the national security; or (h) the development, production, or use of weapons of mass destruction.[107]

So we have on one hand the main categories of information, or licit objects, and on the other the list of prohibited categories, or the illicit objects of discourse. It is not one category or the other that are of interest but the space between them. These categories, both licit and illicit, are contested; their very definitions are argued. The prohibited objects give birth to an entire system of appeals, of litigiousness, of contestation; courts are authorized to deal with these issues, and arguments are produced around these exceptions. We might not know what the secret is but around it there is an explosion of legal discourse, a tremendous amount of energy and information being expended. Prohibitions are not definitive. Between categories of information for the public and exceptions there emerges a contestation ground upon which denials, appeals, resolution and court cases (with around 47 cases disputing these exemptions reaching the Supreme Court) take on the issue of truth.[108]

(1)(c) "Truth, Delayed:" Licit and Illicit Circuits of Discursive Flow

Alongside this division between licit and illicit objects of discourse we also have a system of procedures of access from identifying the agency, making the demand, setting up a system of fees, to provisions for appeal to denied requests, litigious procedures and so on. Thus, "in order to carry out the provisions of this section, each agency shall promulgate regulations … specifying the schedule of fees applicable" and that these fees "shall be limited to reasonable standard charges for document search, duplication, and review," and even provided for free "if disclosure of the information is

in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester."[109] The reasonable nature of these current provisions might conceal the struggle that led to them. Indeed deceptive procedures and exorbitant fees have been and are still used as a disruptive tactic in relation to FOIA requests. For example, the report of the House Committee on Government Operations 1972 pointed to major problems in the implementation of FOIA such as "bureaucratic delay in responding to an individual's request," "abuses in fee schedules by some agencies for searching and copying of documents or records requested by individuals … an effective bureaucratic tool in denying information to individual requestors."[110] No later than 2013, Associated Press, in an investigation to uncover the use of secret government email accounts by top Obama appointees to conduct official business, was initially asked by The Labor Department to pay fees in excess of $1 million dollars for the list of email addresses.[111] Both the use of secret emails and the use of fees are noteworthy.

Similarly, the act provides for specific rules regarding litigation. Thus, "on complaint, the district court of the United States … has jurisdiction to enjoin the agency from withholding agency records and to order the production of any agency records improperly withheld from the complainant."[112] The new rules even provide for litigation costs. Thus "the court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this section in which the complainant has substantially prevailed."[113] As in the case of fees, litigation also has a

chilling effect. The same House Report also lists among the major problems "the cumbersome and costly legal remedy under the act when persons denied information by an agency choose to invoke the injunctive procedures to obtain access" where "the time it takes, the investment of many thousands of dollars in attorney fees and court costs, and the advantages to the Government in such cases makes litigation under the act less than feasible in many situations."[114]

What all this procedures of access, fees, appeals, and litigation procedures do is set up *licit circuits of discursive flow*. We end up with a bureaucracy whose inherent intricacies have been used through FOIA's history to hinder access to truth, obey national security as overt rarefaction strategy, of have been smoothed over, as a result of the tendencies pertaining to this overarching will to truth in politics. I am charting how such a bureaucracy, even when obeying this will to truth, creates complex circuits of information flow. Thus, the ability to make demands for information, to read the legal jargon, to foot the bill, to engage in lengthy appeals processes, even when all these procedures are set up to facilitate access, can still be considered, taken together as forming *a complex architecture of access* whose very existence is a way to slow down access, to carefully control it, to direct it through established circuits. If we add this to the idea that informed consent based on absolute government transparency is a desire that must never reach its conclusion (seeing that we cannot possible process all the paperwork produced by governments), we see that the demand for freedom of information is an incessant demand that can never be fulfilled, as actual access to all the information would drown it. In a sense, it is the rarefaction itself that seems to sustain this demand. Thus,

the will to truth in politics, like Mulder's conviction that aliens exist, can only survive if we constantly encounter barriers.

Aside from this architecture of access, another interesting aspect is the timeline associated with the disclosures of classified information. When it comes to FOIA, the request for information must be honored in a timely fashion. For this purpose *kairos*, as rhetorical timing, becomes a useful way to unpack the temporality of disclosures. "Each agency, upon any request for records … must determine within 20 days … after the receipt of any such request whether to comply with such request and shall immediately notify the person."[115] In terms of requests, the timelines, even though are sometimes used as delaying tactics, are, at this point, fairly short (20 days, with specific exceptions). But beyond the requests via FOIA that pertain to information we are allowed to get, we have the duration of classifications. This issue pertains to the illicit objects, to the documents that we not allowed to see, to read, to use in the political fray, provided enough time has passed. Particularly, I am interested in the declassification process. The division between licit and illicit objects of discourse in this case is not permanent, although that is still a debated topic as we will see. Thus, the moment when secrets are revealed, and more precisely the procedures and the timelines associated with the process of declassification allow me to talk about the antagonistic moment of truth irruption in the two distinct circuits of information flow: licit declassification and illicit "leaks."

Carter's Order 12065 sets up the duration for classification. Thus "each original classification authority shall set a date or event for automatic declassification no more than six years later." In exceptional cases, in which classification is required beyond the

original 6, the "date or event shall be as early as national security permits and shall be no more than twenty years after original classification." Evidently, this 20 year term comes with its own exceptions, such as for foreign government information where "the date or event may be up to thirty years after original classification."[116] In terms of declassification policy, for Carter "3-401. Classified information constituting permanently valuable records of the Government … shall be reviewed for declassification as it becomes twenty years old."[117] "When classification is extended beyond twenty years, a date no more than ten years later shall be set for declassification or for the next review … subsequent reviews for declassification shall be set at no more than ten year intervals" [118]

In Reagan's EO 12356 nothing of these established and clearly defined timelines, with their exceptions in tow, survives. The 6 year limit, the 20 year maximum limit, and so on are replaced by "1.4.a. Information shall be classified as long as required by national security considerations" and "*when it can be determined*, a specific date or event for declassification shall be set."[119] With Clinton's EO 12958, we get another reversal. Timelines are resorted to the classification and declassification processes. Thus, without a date or event set, "information shall be marked for declassification 10 years from the date of the original decision" that can be extended "for successive periods not to exceed 10 years at a time." All these timelines have an accompanying list of exceptions usually pertaining to revealing sources, methods, or procedures for weapons of mass destruction. Furthermore, "3.4.a. within 5 years from the date of this order, all classified information contained in records that (1) are more than 25 years old, and (2) have been determined to

have permanent historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed."[120]

George W Bush's EO 13292 once again backtracks. Although it maintains some of the timelines associated with classification and declassification, it empowers the classifying authorities to classify beyond 10 years and even beyond 25 years. Indeed, "an original classification authority may extend the duration of classification, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information under this order are followed."[121] And lastly, Obama's EO 13526, now in effect, stabilizes these timelines as follows: Upon reaching the date or event, the information shall be automatically declassified. … If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, unless the original classification authority otherwise determines that the sensitivity of the information requires that it be marked for declassification for up to 25 years from the date of the original decision. (c) An original classification authority may extend the duration of classification up to 25 years from the date of origin of the document, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information under this order are followed.[122] "No information" proclaims the order "may remain classified indefinitely." In terms of automatic declassification, the order speaks of the same type of information—more than 25 years old, and having permanent historical value. It further specifies, as opposed to

previous orders, timelines for the exception to the automatic declassification, extending to no more than 50 years and even 75 years for the exceptions to the exceptions.

While the timelines align with ideological differences, their variations are less relevant for my analysis than their very existence. The classification and declassification processes define the kinds of information that should be secret but can be eventually known. It is a system of classification and differentiation of information, of marking/tagging that information with different labels and stamps that create certain circuits of circulation within society. But these circuits not only have spatial coordinates but temporal ones as well. These legal acts associate information and its wide distribution with particular timelines.

A useful way to think rhetorically about this distinction is to bring into the discussion rhetorical time and timing. *Kairos* , as a rhetorical concept, complementing the Foucauldian conceptual apparatus, is defined as "the principle of timing or opportunity in rhetoric … calls attention to the nature of discourse as event rather than object; it shows us how discourse is related to a historical moment; it alerts us to the constantly changing quality of appropriateness."[123] However, seeing distinct temporalities at odds in licit and illicit disclosures, a more useful way to think about this topic is to bring the concept of *chronos* alongside that of *kairos*, as well as their differences, to attend to the problem of truth and timing. Carolyn R. Miller offers a useful conceptualization that can help us think of disclosures and their attendant temporality. In her discussion about the rhetoric of science, Miller contrasts *chronos*, the quantitative term, as "as duration, measurable time, the background that *kairos* presupposes" and *kairos*, the qualitative term, as "a

critical occasion for decision or action."[124] Miller notes the ambiguity of the term *kairos,* emerging from the objective or subjective understanding of the rhetorical situation. Lloyd Bitzer and Richard E Vatz, in their infamous debate, as well as Scott Consigny's resolution, provide the narrative structure to flesh out this ambiguity. On one side, an objective situation, independent of the rhetor, with its own exigencies where "*kairos* presents itself at a distinct point in time, manifesting its own requirements and making demands on the rhetor, which the rhetor must discern in order to succeed," and on the other, a postmodern situation, where the rhetors create the situation; thus, "any moment in time has a *kairos,* a unique potential that a rhetor can grasp and make something of, defining (at least in part) the terms for his or her success. [125] Miller aligns her own understanding of *kairos* with Consigny's famous "both are right" approach. Thus, situations have both objective and subjective characteristics and *kairos* "permits this interplay by including both objective and subjective dimensions of a moment in time."[126]

The temporality of the licit flow of information through carefully designed system of circulation is precisely calculated and drawn. *Chronos*, as objective time, animates the licit disclosures. Declassification will be made, in Carter's Executive Order "as early as national security considerations permit" and the decisions pertaining to declassification "shall be based on the loss of the information's sensitivity with the passage of time or on the occurrence of a declassification event."[127] It is the passage of time and the decreasing relevance of the information that lead to declassification. As this truth's timeliness expires, the truth is revealed. Indeed, the consecutive Executive Orders erase or resurrect the sentence, "At the time of original classification, the original classification authority

shall establish a specific date or event for declassification based on the duration of the national security sensitivity of the information."[128] Implicit in this sentence is the notion that there is a proper time, an appropriate moment for disclosures that either an event or the passage of a measurable amount of time can bring forth. Also implicit is the suggestion that any disclosure prior to this predetermined moment or passage of time is inappropriate, that it risks introducing an unknown variable in the proper circulation of discourse.

Unauthorized disclosures interfere with this delayed temporality that relegates important information about the present to a disengaged historical analysis of the past. *Kairos*, as the interplay between subjective and objective characteristics, which enacts its own possibility, helps us think of illicit disclosures as opportune moments that one does not wait for, that are not inscribed in the inexorable passage of time, but that can and should be brought to bear within the present. The kairotic nature of unauthorized disclosures disturbs the classification procedures and its attendant political reasoning of secrecy, of carefully postponed disclosures, of truth deferred.

Miller also notes that in *kairos* there are two aspects of meaning, "two metaphors embedded in it, a temporal one and a spatial one." The spatial component refers to something like opportunity, an opening, which "we should remember …. can be constructed as well as discovered."[129] Thus,

> *Kairos* as spatial opening is thus central to the rhetoric of the scientific article, and again, the work that it does is to obliterate the distinction between objective and subjective: the opening must be one into which the writer can successfully place his or her own conception of what has been done and, at the same time (and

> place), one that readers will agree exists. *Kairos* as opening is actively constructed by writers and readers and is simultaneously accepted as really existing (or not) in a way that matters for subsequent actions.[130]

On one hand, as we have seen, the temporality of licit disclosures that operates to allow delayed access also tends to make the relevance of the material, as a way to intervene in the political present, somewhat irrelevant; the potential effectiveness of discourse to affect the present is hindered; truth becomes a matter of history and not of the present. Only when discourse is no longer consequential for the people involved, for the political issues as stake, only then it can become available. In other words, being "in the know" is a historically delayed act of political gratification; it disarms the political valance to that particular truth. Being in the know is very much a retrospective process, which means being in the know about the previous administration, about decrepit and forgotten scandals and abuses. *Chronos* —as the temporality of the EOs—as a delayed and foreseeable opportune moment, closes down the discursive field by controlling the irruption of discourse in the public sphere. On the other hand, illicit disclosures create on opening, create their own opportune timing. To every illicit disclosure, the authorities will always respond with the biblical wisdom of "there is a time for …" The "*kairos"* of leaks is set against the "*chronos* /*kairos"* of the tactics pertaining to government's concept of "being in the know." As Foucault notes on *parrhesia*, "it is a truth-telling, an irruptive truth telling which creates a fracture and opens up the risk: a possibility, a field of dangers, or at any rate, an undefined eventuality."[131] The leaks claims the dangerousness and kairotic nature of *parrhesia*, of the irruption of truth during the debate, clamoring for attention and political relevancy.

We can contrast, as an appropriate illustration of this distinction between *chronos* and *kairos,* the effect of the Pentagon Papers on the political climate of its day with the declassification of the Nixon tapes 30 years later. The tapes certainly have historical value but not much relevance in terms of their usefulness as a political tool of intervention in the present. On one hand, delayed flow, assigned to a deferred opportune moment, on the other, a disruptive, unpredictable leak, creating its own timing, its own opening; creating the space for itself as well as the debate, where there was none. These different temporalities clash, the first associated with the delayed release of truth of and about government and the second with the sudden uncontrolled irruption of truth via leaks.

"Putting together the two metaphoric dimensions of *kairos,"* continues Miller, "we might come up with a definition much like that of Eric Charles White, who portrays *kairos* as 'a passing instant when an opening appears which must be driven through with force if success is to be achieved.'" "This formulation," concludes Miller, "allows for both objective and subjective dimensions, so long as we permit the appearance of the opening and the terms of success themselves to be matters of rhetorical negotiation."[132] Through licit disclosures we have an attempt to control discourse by controlling its circulation and its release. *Chronos* /*kairos* functions as "objective" timing within the logic of the national security rarefaction strategy by relegating the safe disclosures to the future. There is a time for truth but its time must be precisely calculated, its release prudently prepared; it must always come in small doses, always delayed, always after the "event." This temporality is ultimately an attempt that aims at stabilizing the meaning of

governance and preserves the authority of institutional structures by shielding them from having their inner workings exposed during their actual functioning. Through illicit disclosures, we have an opening up of the discursive field, a sabotage of the normal flow of time, a kairotic opening that questions the seemingly stabile sovereign structures, an opening that entails all manners of dangers—to the structures themselves (whether as a vote of no confidence or by truly weakening national security, as the authorities maintain) as well as to the speaker—an opening that brings its own opportune timing with it. One thus ties *chronos* /*kairos* to disclosures as exact time, precisely measured and delayed, timing as prophesized, timing as a future event to come; the other creates the kairotic opening, the irruption, the very uncontrollable pouring forth of discourse that sparks the fear of a system collapse of institutions.

(1)(d) "The Fellowship of Discourse:" On the Community "in the Know"

At the same time, this is a system that limits the number of actors authorized to handle this information, to know and speak this truth behind closed doors. For example, in terms of the authority to classify, the last National Security EO lists "1.3.a. the President and the Vice President … agency heads and officials designated by the President; and United States Government officials delegated this authority." All original classification authorities, continues the order "must receive training in proper classification (including the avoidance of over-classification) and declassification."[133] In terms of declassification, the order lists (if they are still serving and having original classification authority) "3.1..b. the official who authorized the original classification … the originator's current successor in function … supervisory official of either the

originator or his or her successor in function …. officials delegated declassification authority in writing by the agency head or the senior agency official of the originating agency … Director of National Intelligence (or, if delegated by the Director of National Intelligence, the Principal Deputy Director of National Intelligence) may, with respect to the Intelligence Community, after consultation with the head of the originating Intelligence Community element or department, declassify, downgrade, or direct the declassification or downgrading of information or intelligence relating to intelligence sources, methods, or activities."[134]

Another way to think about this is to use Foucault's notion of "the fellowship of discourse" the function of which "is to preserve or to reproduce discourse, but in order that it should circulate within a closed community, according to strict regulations, without those in possession being dispossessed by this very distribution."[135] "Fellowships of discourse" point to a seemingly forgotten mode of knowledge, meaning that of secret societies, of apprenticeship, of ritualized recitations, where the goal is preserving and reproducing discourse within closed communities, bound by rules. Nonetheless, Foucault contends, "such 'fellowships of discourse' remain, with their ambiguous interplay of secrecy and disclosure." Foucault points to rhapsodists as an archaic model of this fellowship of discourse where the knowledge of recitation was preserved within a small group where "the roles of speaking and listening were not interchangeable." Indeed the distribution of subjects that are in the know, that can read, speak, and transmit information pertaining to national security is scarce. But there are many other such fellowships, argues Foucault, "functioning according to entirely different schemas of

exclusivity and disclosure." "One has to think," ads Foucault, "of technical and scientific secrets, of the forms of diffusion and circulation in medical discourse, of those who have appropriated economic or political discourse."[136]

The sad case of Arron Swartz, the internet activist who committed suicide as a result of being threatened with a 35-year prison sentences for downloading and distributing freely via web sharing sites over 4 million academic articles, speaks to this limitation of access to certain discourses. In Swartz's own words, resonating with Foucault's take on the control exercised over discourse via narrow access points, "The world's entire scientific and cultural heritage, published over centuries in books and journals, is increasingly being digitized and locked up by a handful of private corporations."[137] Similarly, I argue, the intelligence community, the states, the governmental apparatus, these are all, in a sense, fellowships of discourse as Foucault defines them. The justification is always that speech is dangerous, that its distribution outside these circuits can spin out of control whether it is the diplomatic cables, the Iraq and Afghan war logs, or the documents detailing the vast surveillance machine built by NSA. Only people already in the know, only authorized subjects, vetted through institutional procedures, can access and communicate this information.

Whatever the model we use, when it comes to the fellowship of discourse, Foucault argues, "the number of speakers were, if not fixed, at least limited, and it was among this number that discourse was allowed to circulate and be transmitted."[138] Indeed, Steven Garfinkel, director of the General Services Administration's Information Security Oversight Office estimates, in support of Reagan's National Security EO, that this order

"keeps the number of classifiers at its present total of approximately 7,000 persons worldwide, down 900 percent from just a decade ago."[139] While the number seems to vary, it gives us a sense of scale of this rarefaction of speaking subjects or knowing subjects that are the only ones invested with the power to read and make this determination for decades to come. So it is both the small number and the drastic reduction (900%) that are worthy of attention. As Foucault would put it

> this amounts to a rarefaction among speaking subjects: none may enter into discourse on a specific subject unless he has satisfied certain conditions or if he is not, from the outset, qualified to do so. More exactly, not all areas of discourse are equally open and penetrable; some are forbidden territory (differentiated and differentiating) while others are virtually open to the winds and stand, without any prior restrictions, open to all."[140]

These authorities of classification are privileged subjects, in charge of this information, who have the legal authority to change its classification status, to deny its flow through public circuits. This is the process of rarefaction of knowing and "speaking" subjects, of subjects that can handle, know, and make decisions on the sensitivity of information and the duration appropriate to its declassification of subjects "in the know." Furthermore, this authority to classify or declassify is not granted indefinitely. One is not the knowing subject in all and forever. Even among this secret fellowship of discourse, "membership" can be given and taken away, granted for specific tasks, categories of information, of lengths of time.

(1)(e) Freedom and Information

Concluding the section on FOIA, I claim that the Freedom of Information Act manifests in legal terms a *will to truth in politics*. The need for transparency and government accountability translate this will to truth in concrete political demands. The resulting legal framework constructs a *multilayered architecture of access* with clearly defined yet shifting and disputed *division between licit and illicit objects of discourse*, between *authorized and unauthorized circuits for discursive flow*, complete with schedules of fees, modes of access, rules for litigation and resolution, and with a precise temporal flow. This is a legal system that enshrines any modification into circuits of jurisprudence that have a limited number of players, rarefied subjects, capable of modifying its rules. The contentious legislative history of FOIA shows that this ebb and flow can quickly drown certain categories requiring grand legislative efforts that imply extensive collations to reverse directly prohibiting trends. However, the partisan lines that divide these categories are less relevant for my project than charting the rarefaction of objects and subjects and the delaying of truth. Next, I will address the twin subjectivities haunting the scandals of unauthorized disclosures: the whistleblower and the spy.

(2) "Rare Subjects:" On Whistleblowers and Spies

> Not just anyone, finally, may speak of just anything.[141]

As we have seen, the democratic subject of the Freedom of Information Act demands, pays, and litigates for its access to truth released years later according to its own temporal logic. While in practice it is hardly so, in theory anyone of us can inhabit this subject position. The whistleblower, on the other hand, is a knowing and speaking subject, one who always-already has access to this knowledge, and while it is allowed to

speak, it does so out of turn. The whistleblower is the subject allowed to break the rules and intervene in the present, to bypass the objective temporality (*chronos)* of the licit circuits of information flow and create the moment of revelation (*kairos*), to open up the space for debate. There is plenty of evidence that this figure, inhabiting our legal reasoning animated by the will to truth in politics, can rarely be seen in real life, particularly in regard to the issue of national security. The whistleblower is the rarest of subjects, made so by a web of legal definitions, procedures, exceptions, and intense prosecutions. Nonetheless, this subjective figure animates our current debate on the unauthorized mass/digital disclosures of classified information. With the same passion that the supporters of transparency award this title to Chelsea Manning or Edward Snowden, the establishment denies it, replacing it, via legal challenges, with that of the spy. The spy is the shadowy double haunting the whistleblower; it has nefarious purposes, questionable allegiances, and its actions weaken national security. If the corresponding subject to the will to truth in politics is the whistleblower, the corresponding subject to the national security as rarefaction strategy is the spy. Beyond the partisan framing, these twin figures organize the contentious relationships to truth of and about government.

The whistleblower thus is a paradoxical creature: allowed to speak outside the licit channels, protected from retaliation, and yet disruptive, intervening in the present, using sensitive information that opens up institutions and agencies to public scrutiny in way that are out of their control, denying the temporality and the licit discursive flow

established elsewhere. No wonder that the litigations show great confusion when it comes to deciding who is and who is not a whistleblower.

For Foucault "exchange and communication are positive forces at play within complex but restrictive systems" of which "the most superficial and obvious …. is constituted by what we collectively refer to as *ritual*."[142] Ritual refers to

> the qualifications required of the speaker (of who in dialogue, interrogation or recitation, should occupy which position and formulate which type of utterance; it lays down gestures to be made, behavior, circumstances and the whole range of signs that must accompany discourse; finally, it lays down the supposed, or imposed significance of the words used, their effect upon those to whom they are addressed, the limitations of their constraining validity.[143]

Foucault points to religious, juridical, therapeutic, and even political discourse as examples of ritualized discourses. We already have seen how rituals of disclosures, under FOIA or declassification under EOs, involves a bureaucracy of access—request, processing fees, processes of appeals, authorities and procedures of litigation, each with their own allowances and prohibitions—that contributes to a rarefaction of objects of discourse as well as of knowing and speaking subjects. The same rituals of disclosures, as codified in the Whistleblower Protection Act, operate a rarefaction among the always-already knowing subjects of national security. I take Foucault's understanding of ritualized discourse and interpret it to accommodate the whistleblowers laws. What we are dealing with here is a particular ritual, a protected one, enshrined into law, defining the rules of how to break the rules, the procedures to follow, the restricted, restricting and restrictive audience that is allowed to hear these dangerous words.

Despite these disruptive behaviors, the whistleblower is allowed to break the rules by following the rules of how to break the rules. To blow the whistle is a very well codified act of disruption; an act that can be named as such only if a series of conditions, each with their own long lists of exceptions, are fulfilled. So what are these rituals of disclosures Foucault speaks of, in the case of the Whistleblower Protection Act? For a person to be protected under the WPA, the case must have all of the following elements: a *protected disclosure*, a *covered employee*, and a *personnel action*.

So what it's a "protected disclosure"? According to USC Title 5 2301, lawful disclosures are disclosures of information which the employees "(2301(b)(9)) reasonably believe evidences— (A) a violation of any law, rule, or regulation, or (B) mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety."[144] The act is designed precisely to defend employees against reprisal for such disclosures. Also protected are any disclosures "2302(b)(8)(B) to the Special Counsel, or to the Inspector General of an agency or another employee designated by the head of the agency to receive such disclosures" information similarly pointing to violation or abuse.[145] Similarly protected are disclosures to Congress; thus "5 U.S.C. § 2302(b) this subsection shall not be construed to authorize the withholding of information from the Congress or the taking of any personnel action against an employee who discloses information to the Congress."[146] Also protected are activities related to whistleblowing such as "2302(b)(9) (A) the exercise of any appeal, complaint, or grievance right granted by any law, rule, or regulation; (B) testifying for or otherwise lawfully assisting any individual in the exercise of any right referred to in

subparagraph (A); (C) cooperating with or disclosing information to the Inspector General of an agency, or the Special Counsel, in accordance with applicable provisions of law; or (D) for refusing to obey an order that would require the individual to violate a law."[147] Exceptions, or unprotected disclosures, reference disclosures "not specifically prohibited by law and if such information is not specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs."[148] The employee thus is granted a certain discretion in determining what counts as ethical violation. What is required is to make a determination based on a reasonable belief of violation of the law or abuse. Second, in terms of how the audience for such disclosures, what we immediately notice is that the public is never mentioned. These disclosures are always internal, following predetermined circuits for information flow. Hierarchy is bypassed only to be reinforced by appealing to a higher authority. Third, predictably the exceptions refer to classified information and the overarching label national security.

The second condition for the Whistleblower Protection Act (WPA) defense is that the disclosures is made by a covered employee. A covered employee, or, more precisely, a covered position, refers to "2302(a)(2)(B) any position in the competitive service, a career appointee position in the Senior Executive Service, or a position in the excepted service."[149] Exceptions to this provisions refer to positions "2302(a)(2)(B)(i) excepted from the competitive service because of its confidential, policy-determining, policy-making, or policy-advocating character" as well as "2302(a)(2)(B)(ii) excluded from the coverage of this section by the President based on a determination by the President that it is necessary and warranted by conditions of good administration."[150] Indeed, a state

agency is defined as "2302(a)(2)(C) an Executive agency and the Government Printing Office, but does not include—(i) a Government corporation, except in the case of an alleged prohibited personnel practice described under subsection (b)(8); (ii) the Federal Bureau of Investigation, the Central Intelligence Agency, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Security Agency, and, as determined by the President, any Executive agency or unit thereof the principal function of which is the conduct of foreign intelligence or counterintelligence activities; or (iii) the Government Accountability Office."[151] Not all positions are covered and national security, as a strategy of rarefaction, cuts across the discursive field regarding violation and abuse, allowing certain agencies and topics while disallowing others. With Presidential Policy Directive 19 (2012) the ability for federal employees working in the intelligence community to report fraud and abuse is ameliorated.

The third and final condition for the WPA protection to be triggered, is a personnel action. Here, the law takes into account retaliation on the part of the institution for the act of disclosure. Thus a prohibited personnel action is defined as "take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment" where personnel action can be "2302(a)(2)(A) (i) an appointment; (ii) a promotion; (iii) an action under chapter 75 of this title or other disciplinary or corrective action; (iv) a detail, transfer, or reassignment; (v) a reinstatement; (vi) a restoration; (vii) a reemployment; (viii) a performance evaluation under chapter 43 of this title; (ix) a decision concerning pay, benefits, or awards, or concerning education or training if the education or training may reasonably be expected

to lead to an appointment, promotion, performance evaluation, or other action described in this subparagraph; (x) a decision to order psychiatric testing or examination; and (xi) any other significant change in duties, responsibilities, or working conditions."[152] The venues of appeal and litigation under WPA are the Merit Systems Protection Board (MSPB), Office of Special Counsel (OSC), individual rights of action. However, "An aggrieved employee affected by a prohibited personnel action is precluded from choosing more than one of the above remedies."[153]

This is, in short, the system put in place to protect those rare subjects that disclose information about violation of the law and abuse. It defines the types of disclosures, the covered (subject) positions, and the type of retaliation that triggers the operation of this cumbersome and reluctant system. In the Senate report in preparation for the amendment of the WPA, via the "The Whistleblower Protection Enhancement Act of 2012," this reluctance and cumbersomeness are laid bare. Thus, according to the report "Unfortunately, federal whistleblowers have seen their protections diminish in recent years, largely as a result of a series of decisions by the United States Court of Appeals for the Federal Circuit"[154] among which giving a narrow definition to the type of disclosure that qualifies under WPA. The Report list a series of decisions— *Horton v. Department of the Navy*, *Willis v. Department of Agriculture*, and *Meuwissen v. Department of Interior*—where the court ruled that "disclosures to the alleged wrongdoer are not protected, because the disclosures are not made to persons in a position to remedy wrongdoing," that disclosure made "as part of an employee's normal job duties" is not protected, and, respectively, that disclosures of information "already known are not

protected."[155] According to the report, these decision are "contrary to congressional intent for the WPA." The reason, goes the report, is that the focus was on whether the disclosures were protected "instead of applying the very broad protection required by the plain language of the WPA." The merits of these cases, maintains the report, "should have turned on the factual question of whether personnel action at issue in the case occurred 'because of' the protected disclosure."[156]

Apart from this restriction, the report points out "the lack of remedies under current law for most whistleblowers in the intelligence community and for whistleblowers who face retaliation in the form of withdrawal of the employee's security clearance leaves unprotected those who are in a position to disclose wrongdoing that directly affects our national security."[157] In what the report calls "a troubling decision" the MSPB held that "in delegating certain intelligence functions to an agency, the President had implicitly excluded that agency and its employees from WPA protection." The use of exception for direct prohibition is one of the tactics of the overall national security rarefaction strategy. The overall goal is to reduce the number of objects of discourse, to make the subjects allowed to access and handle that information, rare, and to define and tightly control the circuits of discursive flow. The Report evidently obeys the logic of the will to truth in politics that animates much of our discourse over freedom of speech, of information, and our demands for government accountability. The report thus states that providing avenues for redress to the employees of the intelligence community as opposed to exclude them "would encourage the intelligence community whistleblowers to come forward." Indeed, ", protecting disclosures that are made

according to a specified, protected channel would likely better protect national security information … by removing the incentive to leak information publicly."[158] Leaks are not opposed to secrecy here but to lawful disclosures to the right people.

Reading these laws and their amendments, clearly one is not a whistleblower simply by disclosing some manner of wrong-doing; one must have his or her actions reflected in this interpretable web of categories and exceptions, and must prove him or herself through litigious, contentious, and sometimes lengthy processes. For example, the Supreme Court listened on May 2014 the case involving an air marshal who disclosed in 2003 that TSA stopped posting air marshals on overnight flights from Las Vegas to media outlet MSNBC and was subsequently dismissed. According to the *Wall Street Journal* he tried to raise the alarm through "regular channels," but he failed to do so. As a result of the disclosure Congress exerted pressure and the TSA reversed its decision. Thus "sensitive security information" is pitted against "a substantial and specific danger to public health or safety." According to WSJ, the U.S. Court of Appeals for the Federal Circuit "sided with Mr. MacLean," but the Obama administration made an appeal to the Supreme Court stating that "the Federal Circuit had made 'a serious legal mistake' that will 'embolden further disclosures' by federal employees and 'could put lives at risk.'"[159] The motive behind the government's actions is to chill the impetus behind disclosures, particularly those to the public, via media. On January 21, 2015, the Supreme Court favored the air marshal in a 7-2 decision.[160]

So on one hand, there is the legal system itself, operating at the intersection of this will to truth in politics and national security, struggling to define its categories beyond

interpretation (a rarefaction effect). On the other hand, we have the courts and boards with their own hermeneutic matrix that cannot be controlled but through grand legislative efforts every decade or two (a chilling/prohibiting effect). Contrasting the letter of the law and its interpretation in courts is meant to show how these interpretative matrixes and hermeneutic authorities function by default under the logic of prohibition/rarefaction. Thus, Foucault's concept of "ritual" helps us think of this web of procedures as the *ritual of licit disclosures* where one would need to fulfil certain conditions, be recognized as a particular subject, follow clearly defined pathways of circulation, and fail to trigger retaliation through litigation.

Ultimately, the whistleblower is a disloyal subject even if s/he is allowed to be so inside clearly defined parameters. The whistleblower replaces the institutional code of conduct and ethics with her/his own, placing the latter above the former. By appealing to the higher authority of the people, the whistleblower defies established hierarchies. The whistleblower is, in the end, a transgressive subject. Thus legal layers upon layers of conditions, procedures, and intense litigations are overlaid on top of it to quiet its defiance. Perhaps it is this very transgressive nature that makes it so easy for one to shift from whistleblower to spy as a legal category.

The spy is the ultimate disloyal subject of the polity; the spy speaks out of turn, it hijacks the truth of one government, and sells it to another. So what it means to speak out of turn and what are the laws that define the subject and the rituals of punishment for unauthorized disclosures? As President Woodrow Wilson stated in his address to Congress in 1915:

> I am sorry to say that the gravest threats against our national peace and safety have been uttered within our own borders … There are citizens of the United States, I blush to admit, born under other flags but welcomed under our generous naturalization laws to the full freedom and opportunity of America, who have poured the poison of disloyalty into the very arteries of our national life; who have sought to bring the authority and good name of our Government into contempt, to destroy our industries wherever they thought it effective for their vindictive purposes to strike at them, and to debase our politics to the uses of foreign intrigue … Their number is not great … but it is great enough to have brought deep disgrace upon us and to have made it necessary that we should promptly make use of processes of law by which we may be purged of their corrupt distempers. … A little while ago such a thing would have seemed incredible. Because it was incredible we made no preparation for it. … But the ugly and incredible thing has actually come about and we are without adequate federal laws to deal with it. I urge you to enact such laws at the earliest possible moment and feel that in doing so I am urging you to do nothing less than save the honor and self-respect of the nation. Such creatures of passion, disloyalty, and anarchy must be crushed out.[161]

In this address we see Wilson define the threat as internal, a threat for which the country is unprepared, a threat "uttered" inside the borders, an "other" that becomes self only to become an other/threat once more. The spy is both an outsider and an insider making his or her betrayal more difficult to deal with, his or her presence more difficult to detect. In this address we see Wilson urging Congress to take action against the enemy within. At the time of Wilson's address there was already a law on the books protecting state secrets: "An Act to Prevent the Disclosure of National Defense Secrets" of 1911. The very short law criminalized the disclosures of government information pertaining to

national defense to unauthorized persons.[162] The Secrets Act however offers minimal details and reduced sentences, ranging between 1 year (for disclosures) and 10 year (for disclosures to foreign governments). The *Espionage Act* of 1917, while retaining some of the language of the secret Act of 1911, completely rewrites the legal framework of espionage.

The *Espionage Act* of 1917 punishes, among other provisions, in section1(a) people that enter government facilities for obtaining information "respecting national defense with intent or reason to believe that the information to be obtained is to be used to the injury of the United States, or to the advantage of any foreign nation"; (b) the people who obtain/take/copy information related to national defense, "for the purpose aforesaid, and with like intent or reason to believe"; (c) people who "for the purpose aforesaid," receive or incite other to obtain information that "has been or will be obtained, taken, made or disposed of by any person contrary to the provisions of this title"; (d) the person who has authorized access and "willfully communicates or transmits or attempts to communicate or transmit the same to any person not entitle to receive it" or fails to communicate it to a proper authority; and (e) who have authorized access and "through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed." In other words, these are people who obtain, induce others to obtain, copy, transmit, or lose information pertaining to national defense with bad intent. The punishment reserved for the last category of individuals (the negligent ones) is a "fine of not more than $10,000, or by imprisonment for not more than two years, or both." For the

rest, who have malicious intent, punishment is "imprisonment for not more than twenty years." During war, however, the same offenses "shall be punished by death or by imprisonment for not more than thirty years."[163]

To these offenses of obtaining, copying, and transmitting information pertaining to national defense with malicious intent, the Act also adds, in section 3 (later made infamous by the addition of the sedition provision) people who "willfully make or convey false reports or false statements with intent to interfere with the operation or success of the military or naval forces of the United States or to promote the success of its enemies and whoever, when the United States is at war, shall willfully cause or attempt to cause insubordination, disloyalty, mutiny, or refusal of duty, in the military or naval forces of the United States, or shall willfully obstruct the recruiting or enlistment service of the United States, to the injury of the service or of the United States." The punishment here is "more than $10,000 or imprisonment for not more than twenty years, or both."[164] Section one with all its categories seems to speak about the spy, section 3 criminalizes speech against the war effort in any form it might take.

Indeed, with the Sedition Act of 1918, an amendment to the *Espionage Act* of 1917, dangerous speech is targeted. This new addition is worth rendering in full:

> whoever, when the United States is at war, shall willfully cause or attempt to cause, or incite or attempt to incite, insubordination, disloyalty, mutiny, or refusal of duty, in the military or naval forces of the United States, or shall willfully obstruct or attempt to obstruct the recruiting or enlistment service of the United States, and whoever, when the United States is at war, shall willfully utter, print, write, or publish any disloyal, profane, scurrilous, or abusive language about the

> form of government of the United States, or the Constitution of the United States, or the military or naval forces of the United States, or the flag of the United States, or the uniform' of the Army or Navy of the-United States, or any language intended to bring the form of government of the United States, or the Constitution of the United States, or the military or naval forces of the United States … into contempt, scorn, contumely, or disrepute, or shall willfully utter, print, write, or publish any language intended to incite, provoke, or encourage resistance to the United States, or to promote the cause of its enemies, or shall willfully display the flag of- any foreign enemy, or shall willfully by utterance, writing, printing, publication, or language spoken, urge, incite, or advocate any curtailment of production in this country of any thing or things, product or products, necessary or essential to the prosecution of the war in which the United States may be engaged, with intent by such curtailment to cripple or hinder the United States in the prosecution of the war, and whoever shall willfully advocate, teach, defend, or suggest the doing of any of the acts or things in this section enumerated, and whoever shall by word or act support or favor the cause of any country 'with which the United States is at war or by word or act oppose the cause of the United States therein, shall be punished by a fine of not more than $10,000 or imprisonment for not more than twenty years, or both.[165]

What we see here is no longer the sin of aiding the enemy as an agent in said enemy's employ, but expressions contrary to the official doctrine. People who cause/incite or attempt to incite insubordination, disloyalty, mutiny, or refusal of duty; people who interfere with the recruiting process; uttering, printing, writing, or publishing disloyal, profane, scurrilous, or abusive language directed to the war effort, the US Constitution, or the military, ultimately expression of dissent, become crimes; expression in any form that encourage resistance to the US or support the cause of the enemies of the US, or that are designed to interfere with the production side of the war effort as well as advocating,

teaching, defending, or suggesting to others doing any of the acts referred in this act, is also a punishable offense by a 10,000 dollar fine and no more than 20 years in prison.

A brief overview in *Freedom of Speech in the United States* points to over a thousand prosecutions under the *Espionage Act* and the Sedition Amendment "with almost any antiwar comment being a potential source of government suspicion." Thus "it became a crime to criticize the war bond effort, describe the draft as unconstitutional, or state and that it was in opposition to Christ." Among the examples are a citizen who opposed to the war and was convicted for stating in a personal letter. "I am for the people and the government is for the profiteers," while others "were punished for criticizing the Red Cross of the YMCA." Similarly, a German American "who had not purchased Liberty bonds and who justified his action by explaining that he did not support either side in the war was arrested for the remark."[166] To this mundane application of these laws, add the famous Supreme Court cases of the 1919 when convictions based on the *Espionage Act*, used to quell dissent, where upheld: Schenck v. United States (1919), where the distributing of leaflets against the draft was construed as a criminal offense;[167] Frohwerk V. United States (1919) where criticism by a newspaper of US involvement in the war was also construed as violating the *Espionage Act*;[168] Debs v. United States (1919) where a speaker was convicted for giving an anti-war speech;[169] and Abrams v. United States (1919) when the sentence for urging interference with war production was upheld.[170] For now, the individual details of all these cases are less relevant than the story told by their rapid succession on the page.

It is easy to add to this story the startling fact that only 11 people in US history of have been charged under this act for leaking classified national security information and that 8 of those (Tomas Drake, Stephen Jin-Woo Kim, James Hitselberger, Shami K. Leibowitz, John Kiriakou, Bradley Manning, Jeffrey Sterling, and Edward Snowden)[171] have been prosecuted under the Obama administration. Navy civilian analyst Samuel Loring Morison was prosecuted under the Reagan administration and Defense Department analyst Lawrence A. Franklin was prosecuted under the George W. Bush administration. It is also easy to elevate the entire group by mentioning Daniel Ellsberg, prosecuted under the Nixon administration, considered "the most dangerous man in America" and arguably the most famous and successful whistleblower, as being one of those 11.

My focus is pointing out that the *Espionage Act* has always been part of an overall tactic to manage dangerous speech and discipline the speaking subject. Evidently the *Espionage Act* is designed to deal with the very real existence of spies, who, for personal gain or for ideological reasons, sell information to foreign governments. But in its broad applications and its all-encompassing language, the act also can be, and has been, used to discipline the speaking subject. To put it simply, the limits of the thinkable in terms of the betrayal of an insider allows for the potential, which can be reactivated at any time, to criminalize speech, speakers, and whistleblowers. What brings together the post WWI landmark cases of the Supreme Court with the current prosecutions under the *Espionage Act* is precisely this ability to reactivate this potential despite any changes in the law, such as the repeal of the Sedition Act. Thus, apart from arguments that can be made about

continuity of overt purpose, or the opposite, the humanization of the law via successive amendments, I claim that the *Espionage Act* has a dormant potential to manage dangerous speech and the subjects who utter it.

Thus, from its inception, the *Espionage Act* had the potential to deal not only with individuals who betray secrets to the enemy, but also with dissent, with dangerous speech, with transgressive discourse, and with speaking subjects. It is this potential that can always be activated as long as the speaking subject is within the same legal space as the spy. As I will argue in the next chapter, these two figures—the whistleblower and the spy—kept apart in legal jargon, are nonetheless slowly being superimposed on one another and not just in the high profile cases that make the Obama administration (in)famous—more whistleblowers charged under the espionage law than all other presidents combined—but also in internal documents from state agencies defining the "insider threat" as on object of surveillance and intervention. This proximity, I claim, might have something to do with the fact that speech by and about government is dangerous. Next I will attempt to briefly sketch this idea of dangerousness I have been relying on throughout this chapter, a theme traversing both the will to truth and national security as purposeful rarefaction strategy.

(3) Of Dangerous Speech

> What is so perilous, then, in the fact that people speak, and that their speech proliferates? Where is the danger in that?[172]

Animating both the *will to truth in politics* and *national security* is the idea that true discourse of and about government is dangerous because it can bring down or

strengthen our democratic republic. Thus, on one side, for the advocates of freedom of speech and information, the concealment of these truths is dangerous for democracies and their revelation is dangerous for oppressive regimes. One the other side, discourse of and about government, escaping the predetermined and tightly regulated licit circuits of information flow, is dangerous as it exposes the interworking of the security state apparatus and thus weakens national security as well as putting real lives in danger.

So how precisely is discourse of and about government dangerous? First, as the complex web of laws, executive orders, and court decisions has shown, discourse flowing outside predetermined and well-guarded circuits can have dire consequences for the security of the entire nation. Second, as the legislation obeying what I have called "the will to truth in politics" has shown, discourse is powerful and dangerous for its potential to expose government fraud and abuse and, ultimately make the republic stronger, even if there is a temporary injury to national security. And third, and perhaps the most important, discourse is dangerous for those who utter it, for the transgressive subjects who favor the will to truth in politics to national security as the organizing logic of a democratic system. To speak to all these three, I will meander between different texts, from different genres and different eras—from executive orders and Nixon's secret tapes to Manning's court decision and the Pentagon report documenting the harm done by Snowden's revelations—performing a *bricolage* of sorts about dangerousness. What I hope becomes clear across all these diverse texts is the dispersion of the theme of dangerous discourse reactivated every time disclosures happen.

All executive orders, regardless of their ideological bent, link the level of classification of the documents based on their ability to do harm if disclosed. Thus, *top secret* "shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe;" *secret* "shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage;" and *confidential* will be applied "to information, the unauthorized disclosure of which reasonably could be expected to cause damage."[173] In other words, the level of confidentiality depends on the potential harm that the flow of this information through illicit circuits can cause to national security. The unit of measurement of a document is harm. Distinct levels of harm—from damage, to serious damage, and to exceptionally grave damage—justify increased level of classification. The level of confidentiality therefore is not linked to content but the relation between content and unknown, unauthorized, and presumed hostile subjects. Truth is dangerous; discourse, outside authorized circuits, handled by unknown subjects, can cause differing levels of damage to the nation. Therefore, its circulation must be controlled, the subjects that are privileged to make these determinations and handle the information must be few, vetted, and trained, and the transgressions must be punished. Information is power and when mishandled, it can be deadly.

The pouring forth of state secrets into the public's consciousness, the government's failed efforts to prosecute the newspapers or Daniel Ellsberg, and the intense turmoil evidenced by President Nixon's tapes, make the "pentagon papers"

moment the best suited to be woven next into this tapestry of dangerousness. While this is not a part of the digital leaks era per se, its echoes and invocation in the current scandals make this moment relevant for this discussion. At first Nixon seems to be unaware of the pentagon report; he is informed once the first article is printed in *The New York Times*. In various conversations, Nixon and his aids muse about the usefulness of the leak as it damages the reputation of the Democrats. Nixon also seems reluctant at first to prosecute The New York Times being focused more on finding and prosecuting the source. Nixon is also engaged in orchestrating the rhetorical framing of the situation. He inquires and coordinates the dissemination in mass media of certain messages; he is focused on providing specific frames via language. Indeed, he is most adamant to call the pentagon papers, "the Kennedy-Johnson papers." Particularly, I am interested in his strategic reframing of the disclosures and less so in the more dramatic statements—"Get the S.O.B." or the infamous "tie him to some communists"—on Ellsberg.

In a conversation with Charles Colson, special counsel to the President and, incidentally, one of the Watergate Seven who pleaded guilty to obstruction of justice for "devising a scheme to get and disseminate derogatory information about Pentagon Papers Defendant Daniel Ellsberg in 1971,"[174] Nixon articulates both his views on the dangers associated with disclosures as well as the rhetorical strategy to deal with it:

> President Nixon: In fact, I'm going to, as long as I am where I am, the New York Times will never, never, never have another opportunity to have any stolen goods, I'll tell you that.
> Colson: In my opinion, Mr. President, you need--"

> President Nixon: Yeah. They chose to take this on, and now we'll do it. Now, it isn't just the Times, but it goes beyond that. It goes to all of the disloyal people in government who do--"who are tempted to get out and peddle a paper here and there.
>
> …
>
> President Nixon: It goes also to the integrity of government. It's far beyond the war. This is a terrible thing.
>
> Colson: Well, imperiling people's lives.
>
> President Nixon: But I think--"I think the Times--"imperiling lives, imperiling our sources, imperiling our lines of communication, imperiling the President's right to have honest advice from his advisers.
>
> Colson: That's right.
>
> President Nixon: Why, it destroys it all.[175]

We see the familiar themes of the integrity and good functioning of government and the theme of disclosures endangering human lives coming together in the president's reasoning on the issue of the Pentagon Papers. We also glimpse the firm decision to fight these disclosures to the end. But beyond his own feeling about the publication of the Pentagon Papers, Nixon was also cognizant of the need to rhetorically frame the issue in the best possible terms. "Why don't you get this line … The *Times* is guilty of publishing . . . of knowingly publishing stolen goods" asks the president in the same conversation with Colson. The next segment, rendered in full, to sample both the process and the flavor of the conversation, is an apt example for this rhetorical reframing as well as bringing evidence to support the kind of reasoning that traverses (speakers, genres, and eras) any defense of national security:

President Nixon: Knowingly publishing stolen goods. Now, I want you to get that line.

Colson: Yes, sir.

President Nixon: Used. I want it used. Get it to ten senators and congressmen this afternoon, will you?

Colson: Yes, sir. I'll do it.

President Nixon: "Knowingly published." Get somebody to get it out on television. Now, that's the kind of thing. Get somebody to put in an editorial.

Colson: Well, that's the kind of thing people.

President Nixon: And then mail that around the country. Put it … put it … get it on some sort of print and mail it to a hundred thousand people. Knowingly publishing stolen goods.

Colson: Mm-hmm.

President Nixon: Why … why … why aren't they guilty of something?

Colson: That … that reduces it to something that is simple enough for pub …

President Nixon: Yeah.

Colson: for the people to understand.

President Nixon: Knowingly publishing stolen goods. And endangering the security of Americans.

Colson: Right.

President Nixon: Enda … that's the second line: Endangering the security of Americans.

Colson: Yes, sir.

President Nixon: Third, well, people don't care about the presidency and all that sort of thing, but nevertheless, the "endangering the security of Americans."

Colson: Ehrlichman is working on some very good lines for you tomorrow and of course, I think that will, if you choose to use them at Rochester, is a marvelous opportunity.

We see the familiar themes of theft, of endangering American lives, of endangering the security of the nation, as well as the overt attempt to sway public opinion and change the terms of the conversation revolving around the Pentagon Papers. Nixon's tapes here serve as another point of support that caries through and amplifies the long history of the dangerousness associated with truth of and about government. Nixon is relevant precisely because it represent the aberrant moment where the fear of this dangerousness leads the government and the office of the president of a democracy to its most embarrassing and damaging failures from that of preventing its secrets to be leaked, to that of stopping their publications, or to successfully prosecuting the source of the leaks, not to mention the loss of trust in the government for decades to come.

While PFC Bradley Manning's trial is too vast in its discursive bounty to metabolize effectively in this section, I want to anchor the argument about dangerous discourse in two documents: the initial charge sheet and the final sentence. Initial charge sheet has three charges with 22 specifications, detailing explicit charges under the broader categories. The categories are:

1. Knowingly giving intelligence to the enemy
2. Wrongfully and wantonly cause to be published on the internet intelligence belonging to the U.S. government, having knowledge that intelligence published on the internet is accessible to the enemy, such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon armed forces.
3. Charges related to unauthorized use of secure networks.[176]

As we know, Manning was not found guilty of the first charge, of aiding the enemy, which carries the death penalty, but was found guilty of everything else. What I am interested here is the definitions that the Court explicitly used to define these charges. First, the enemy. According to the verdict issues with special *enemy* "includes not only organized opposing forces in time of war but also any other hostile body that our forces may be opposing and includes civilians as well members of military organizations."[177] The broad definition extends the notion of enemy to anything that can be labeled as such by the government. Furthermore, when discussing the charges that fall under the *Espionage Act*, particularly if the information can be used to injure the U.S or to the advantage of a foreign nation, the court states that "the country to whose advantage the information could be used need not necessarily be an enemy of the United States. The statute does not distinguish between friend and enemy."[178] To this broad definition of enemy, we add a broader understanding of the danger of losing information by erasing the distinction between friend and enemy.

Also, dangerousness as knowing. The verdict sheet defines "knowledge" as requiring that "PFC Manning acted with actual knowledge that intelligence published on the internet was accessible to the enemy. The Court may not find the accused guilty of this offense if the Court finds PFC Manning should have known, but did not actually know this fact. Knowledge, like any other fact, may be proved by circumstantial evidence, including PFC Manning's training, experience, and military occupational specialty."[179] Additionally, "reason to believe" is explained as PFC Manning knew facts from which he concluded or reasonably should have concluded that the information could

be used for the prohibited purposes" adding "the fact-finder need not determine that PFC Manning had reason to believe that the information would be used against the United States, only that it could be so used."[180] This definition of *knowing* and *reason to believe*, in their broad applications, explain the textbook syllogism unfolding in specifications: "having knowledge that intelligence published on the internet is accessible to the enemy … at the time of the charged offense, al Qaeda and al Qaeda in the Arabian Peninsula were enemies of the United States … PFC Manning knew that al Qaeda was an enemy of the United States … PFC Manning had knowledge that intelligence published on the internet was accessible to al Qaeda …. PFC Manning's conduct was of a heedless nature that made it actually and imminently dangerous to others.[181]

In other words, anything anyone says about anything secret that can be retransmitted via any form of mass communication and reach anybody, and knowing that to potently be the case, is ultimately a punishable offense. Simply insert foe/friend in the syllogism and guilt is the unavoidable logical conclusion. Thus we have a broad definition of "enemy," a broader definition of injury and advantage of foreign nations that no longer separate between friend and foe, and guilt by having knowledge, in the broad sense as potentially knowing that some has access to anything disclosed in public. While the Executive Orders spoke at times of balancing harm to national security and national interest, where the latter sometimes suppressed the former and an acceptable level of harm to national security were considered tolerable if it serves the public, these decision, in their broad strokes, erase any possibility of that.

Edward Snowden was indicted as well under the *Espionage Act*. According to the official criminal complaint, Snowden is accused of theft of government property as well as, under the *Espionage Act*, of unauthorized communication of national defense information and willful communication of classified communications intelligence information to an authorized person.[182] Thus, certainly, speaking out on these classified issues entails a grave risk to the speaker. Perhaps the best evidence for an argument about dangerousness as being inextricably linked to discourse of and about government is the newly released (May 22, 2014) Pentagon study on the damage caused by Snowden's revelations. Apart from indicating the bureaucratic machine put in motion to assess the impact of the leaks, this document is also a performance of my argument in that it was released as a result of a FOIA request (a manifestation of the will to truth in politics), with 12 pages out of 39 made public, it is redacted to the point of its release being borderline meaningless (prohibitions of objects of discourse, rare subjects in the know), and featured prominently among redactions is the floating idea of dangerousness punctuated from time to time with statements such as the commission "assess with high confidence that the information compromise by a former NSA contractor (redacted) and will have a GRAVE impact on U.S. national defense" or "the scope of the compromised knowledge related to U.S. intelligence capabilities is staggering."[183]

Perhaps the best evidence for an argument about dangerousness as being inextricably linked to discourse of and about government is the newly released (May 22, 2014) Pentagon study on the damage caused by Snowden's revelations. Apart from indicating the bureaucratic machine put in motion to assess the impact of the leaks, this

document aptly illustrates my entire argument: (1) it was released as a result of a FOIA request (a manifestation of the will to truth in politics); (2) with the 12 pages, out of 39, redacted to the point of its release being borderline meaningless (prohibitions of objects of discourse, rare subjects in the know); (3) and featured prominently among redactions is the floating idea of dangerousness punctuated from time to time with statements such as the commission "assess with high confidence that the information compromise by a former NSA contractor (redacted) and will have a GRAVE impact on U.S. national defense" or "the scope of the compromised knowledge related to U.S. intelligence capabilities is staggering."[184]

The details are evidently scarce. Julian Sanchez writes for *The Guardian* that the Pentagon's report on "grave' threat is gravely overblown'" and that the harms touted by US "may be largely hypothetical – an attempt to scare spy-loving legislators with the phantoms of lost capability."[185] The report is limited as it deals with everything but the material made public—the non-NSA Defense material—and pertains more to information compromised. Nonetheless, the journalistic fervor in pointing out the hollowness of the government argument about the harm being done, that it fails to prove what it maintains, perhaps misses the larger rhetorical and philosophical point. It is because it is hollow, it is because the evidence for the claim of harm always comes in the form of a fully redacted page, that it can never be refuted. While the journalist is quick to point out that the danger is hypothetical, as if that disqualifies the government's argument, its hypothetical nature is precisely the feature that speaks to my argument. The dangerousness of discourse is always virtual, never actual, and thus all the more potent.

In a debate between Daniel Ellsberg and Ben Wizner (Legal Adviser to Edward Snowden & Attorney, ACLU) on one side and Ambassador R. James Woolsey (Former Director of the CIA) and Andrew C. McCarthy (former Federal Prosecutor) on the other side, Wolsey maintains that

> What he did was release -- steal and release -- material that went to, among others, Hezbollah, al-Qaeda, Hamas, Pyongyang, Tehran and so on. In the real world, you can't have a principle that it is really important to release material, but you're only going to release it to nice people; you're not going to let terrorists and dictators peruse it and use it. But that's what they do, and that's what they are doing, because Mr. Snowden decided to let them do that.[186]

This is the logic that governs the licit circuits of discourse. As we have seen, both in Manning's case as well as in Snowden's, the public sphere is always and forever contaminated with the presence of enemies. The public sphere is an uncontrollable surface on which discourse spins out of control, harming in varied and redacted ways the security of the people. That is why all these circuits must be created—whether to conceal it, or for its revelation—illicit disclosures introduce an unknown variable in the circulation of dangerous speech: the public, a multitudinous subject that cannot be rarified, that cannot be vetted, authorized, monitored, and controlled.

(4) Logophobia

> There is undoubtedly in our society … a profound logophobia, a sort of dumb fear of these events… of the incessant, disorderly buzzing of discourse.[187]

True discourse of and about governance, as information about the inner workings of institutions, is controlled via a web of legal acts, procedures, and litigations. We have,

evidently, direct prohibitions, under the logic of national security as overt rarefaction strategy. We also have *a multilayered architecture of access* in which *truth of and about government* flows through predefined circuits, where subjects "*in the know*" are clearly defined, and truth is delayed becoming a matter of historical hindsight. This architecture obeys what I have called *a will to truth in politics*. A particular discursive dynamic distributes subjects and arguments along this fault line. At heart of this fault line separating the will to truth in politics from national security are questions such as: who can know the truth, who can speak it publicly, and with what consequences.

While these two rhetorical logics differ in their awareness of their prohibiting effects, both are nonetheless rarefaction strategies. Working in conjunction, the result is a division of the discursive field of and about government into *licit and illicit object of discourse, licit and illicit circuits of discursive flow,* and *authorized and unauthorized subjects.* However, as evidenced by the contentious legislative history of the legislation discussed here as well as by the recent spate of high profile cases tried in the courts and the public outrage that accompanied them as well as the renewed push to enact some form of change, this apparatus is not successful at encompassing the field of discourse over which it intends to exert its control.

Traversing both these rarefaction strategies is the idea of truth of and about government as being powerful and dangerous. It is dangerous for the government, it is dangerous for the people, it is dangerous for those who work for the people, and it is dangerous for those who speak it in the marketplace without being authorized to do so. The digital revolution makes the borders between licit and illicit circuits much more

permeable than ever before. Ellsberg took three months to copy 4000 pages of the Pentagon Papers, while Snowden is accused of spiriting away over 1,7 million documents on a flash drive. The fear of this permeability might explain in part the zealous nature of prosecutions under the Obama administration and yield the unflattering sentence about the prosecution of more whistleblowers "than all the other presidents combined." This permeability might also explain the inability of the state apparatus to distinguish between the whistleblower and the spy. In the next chapter, I will interrogate documents designed for implementing an "insider threat" program in state institutions, a program that emerged as a reaction to these massive leaks of classified documents. While these laws try to keep the whistleblower and the spy apart, the recent prosecutions and the insider threat program betray the attempt to bring them closer together.

Chapter III

The New Delinquent of the Digital Age: The Whistleblower as "Insider Threat"

> Colbert: Are we still in danger?
> Philip Mudd: I think we are. If you look at 'homegrowns' – people who sit and look at a computer, and look at images from places like Gaza, Iraq, Afghanistan. Those kids are inspired by emotion to say 'I want to do something about that.' And now they have an ideology they attach themselves to and that's called Al-Qaeda-ism.[188]

Introduction

Philip Mudd's characterization of how people become subversive in the digital age links a simplified understanding of persuasion, as identification and affect, with the radicalization process in the context of a perpetual war. We might be inclined to label his exposition a caricature, a "media transmitted (ideological) disease" (MTD) infecting affect via mediated images of human suffering, but given Mudd's employment history as

the former director of the CIA's counter-terrorist center and senior intelligence advisor at the FBI, this intervention raises sobering questions on the way state institutions think of and understand the process by which a "trusted insider" becomes a an "insider threat." My interest, however, lies not in empirical questions such as "is this truly how the process through which one becomes involved in the subversion of one's country works?" or "is this how persuasion, affect, or discourse circulate and function?" Rather, I want to explore procedural questions about how state institutions with the power to create policies and organize vast systems of surveillance understand and/or imagine the process by which one decides to disclose classified information. I am concerned with the effect that this understanding has on the said policies and procedures, on how the physical and digital spaces are partitioned, put under surveillance, and disciplined, and on what comes to be considered normal and abnormal behavior. At the intersection of power and knowledge, where causal links are posited between behaviors and the potential to do harm, emerges the sketch of the potential leaker.

In order to chart this link, between a particular understanding of the process of radicalization and the act of leaking, I will look at various government documents collected under the devil term "insider threat." In a similar manner to the shift described by Foucault in *Discipline and Punish*—from punishing the crime to knowing the criminal before the crime and, thus, opening up new classes of object of knowledge and new domains of interventions for power—I want to trace through these documents the emergence of this figure—the leaker as insider threat—that must be known, must be put under surveillance, must be reported, must be excised from the governmental body before

committing the crime. It is not so much Manning and Snowden that are of interest to me in this chapter, as are the institutional policies that mushroom in their wake.

In such an ever-evolving object domain, any periodization is bound to be arbitrary. Therefore my anchorage point for isolating this figure of the insider threat is the Executive Order 13587 October 7, 2011, titled "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information." This is the presidential act that sets in motion a series of institutional attempts to define this insider threat. Here the president tasks governmental agencies to implement "structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties" and with developing "a Government-wide program (insider threat program) for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure."[189]

Accompanying the analysis of the executive order, I will scrutinize relevant documents, both prefiguring and resting their legitimacy on the executive order, from policies to studies and guides for mitigating such threats available on government institutions' websites, such as: the "National Insider Threat Policy" posted by the Office of the National Counterintelligence Executive (ONCIX); "The Psychology of the Insider Spy" published in *Intelligencer: Journal of US Intelligence Studies*, 2010; "Common Sense Guide to Mitigating Insider Threats 4th Edition" (2012) "funded and supported by the United States Department of Homeland Security under Contract with Carnegie

Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense;"[190] An FBI brochure, one of the only three document linked on the NCIX website (alongside CERT Common Sense Guide and Charney's "True Psychology of an Insider Spy"); The Department of Defense "Insider Risk Evaluation and Audit" 2009, authored by Eric D. Shaw from "Consulting & Clinical Psychology, Ltd.," Lynn F. Fischer from the "Defense Personnel Security Research Center," and Andrée E. Rose from the "Northrop Grumman Technical Services" under the auspices of PERSEREC (The Defense Personnel and Security Research Center) a Department of Defense entity "dedicated to improving the effectiveness, efficiency, and fairness of DoD personnel suitability, security and reliability systems;"[191] the Department of Energy report, dated September 30 2010, authored by FL Greitzer, CF Noonan, LJ Kangas, AC Dalton and titled "Identifying at-Risk Employees: A Behavioral Model for Predicting Potential Insider Threats," prepared by Pacific Northwest National Laboratory one of the ten U.S. Department of Energy national laboratories managed by DOE's Office of Science; the Army regulation 381-12, "Threat Awareness and Reporting Program" from October 10, 2010; and the Department of Defense Directive number 5240.06, from May 17 2011, incorporating Change 1 from May 30 2013. My focus in this chapter is on how the very conceptualization of the radicalization process, akin to Mudd's characterization, materializes through these documents, mentioned above, in policies and procedures designed to detect, anticipate, and deter insider threats. I am interested in how a particular institutional understanding of how people are driven to leak sensitive information,

rhetorically articulated in these documents, provides the logic of a system of surveillance and monitoring to be implemented in all governmental institutions in a post-Wikileaks era.

My theoretical inspiration for this chapter comes from the intersection between rhetoric's concern with, and Foucault' role in our disciplinary understanding of, power. What I want to isolate for my analysis is Foucault's concept of the delinquent in *Discipline and Punish*. Foucault notices a shift in the power to punish (from sovereign punishment to "humane" disciplining) and the invention of the delinquent as the criminal existing before the crime. Thus, a rhetorical perspective/reading that takes this shift from acts to propensities, from criminals to delinquents, as the logic organizing the apparatus of power reorganized in the wake of Wikileaks, allows us to look in these texts for a certain logic of a governmental apparatus, a logic Dave Tell dubs "metonymical." Furthermore, the panoptic relation, present in remarks on visibility and the need for co-workers to monitor each other, complements the emergence of what I labeled as an *insider threat apparatus*.

To put it simply, digital leaks have become a problem of and for governance, a cause for concern, and thus the object of attention for state institutions, for knowledge domains, and for intervention. What my analysis of these documents, authored for or by prominent government institutions such as Department of Defense or FBI, will illustrate is that the "insider threat" is the equivalent of Foucault's "dangerous individual." First, I will show the insertion of the act of disclosure among the offenses associated with espionage by which those who disclose—whistleblowers/leakers—become "insider

threats." Next, I will define the insider threat as the new delinquent of the digital age. Third, I link the problematization of truth to the emergence of an insider threat apparatus, as an ensemble of discourses and institutions that obeys what Tell calls a metonymical logic, briefly defined here as abstract concepts resulting from observation being posited as the cause of those very events. I detail next the constitution of a field of knowledge, largely reliant on behavioral science, pertaining to insider threats. And lastly, I conclude with a discussion of "observables" (observable behaviors) as panoptic visibility in the deployment of the insider threat apparatus.

The Whistleblowers as "Insider Threats"

> It's about people's profiles, their approach to work, how they interact with management. Are they cheery? Are they looking at *Salon.com* or *The Onion* during their lunch break? This is about "The Stepford Wives,"[192]

Thus, it all begins with a joke: the way to spot a whistleblower is to see if he or she is reading *The Onion*. What sounds like the beginning of a humorous article in said satirical publication is in fact an offhand remark made by a Pentagon official intended to dramatize how to spot a potential insider threat. In a Defense Department strategy obtained by McClatchy DC, the text reads: "Hammer this fact home . . . leaking is tantamount to aiding the enemies of the United States."[193] Thus, behind the "reading *The Onion*" joke, lies a program according to which millions of federal employees and contractors "must watch for 'high-risk persons or behaviors among co-workers and could face penalties, including criminal charges, for failing to report them" while "leaks to the media are equated with espionage."[194] With such a clear and harsh mandate, the issue of

how state institutions define and manage the issue of insider threats is crucial for our overall attempt to understand the role of truth in the relation between citizens and government as brought to the forefront by the issues of leaks. I am interested specifically in the relationship between behaviors marked as dangerous, the knowledge that envelops and develops around these behaviors, and the apparatus that translates this knowledge into institutional policies, setting in motion systems of surveillance and ultimately of intervention and control.

In a post 9/11 world, two categories of people become relevant for my discussion: "illegal enemy combatants" and "insider threats." The first is a category beyond law, akin to Giorgio Agamben's "Homo Sacer" who stripped of all rights, reduced to bare life, can, consequently, be killed by anyone.[195] The scandals involving indefinite imprisonment at Guantanamo as well as the long list of enemy combatants killed by drone strikes, speaks of the deadly power of the rhetorical category "illegal enemy combatant." However, as the scandal of the U.S. drone strike deliberately targeting an American citizen, involving Anwar al-Awlaki, killed on Sept. 30, 2011, and his son Nasser al-Awlaki killed two weeks later, proves that erasing an U.S. citizen by using the same label and the same legal sleight of hand might not be as easy as it is to rendition strangers/foreigners, even if proven to be a well-known Muslim orator and jihadist, nicknamed the "emir of the Internet". [196]

Enter "insider threat." The label itself is not new, as it was used to designate potential threats to economic interests (economic espionage, selling trade secrets, and so on) long before the emergence of leaks as a public issue. What is of interest to me in this

project is the extension of this label to threats of national security, particularly in relation to leaks of classified documents. This label allows the transition from threatening *other* to threatening *self*. Insider threat is for U.S. leakers what illegal enemy combatant is for foreign fighters—it becomes a legal definition, a ghostly subjectivity that enables the development of new forms of knowledge and new surfaces and modes of intervention. We are no longer simply talking about threats to national security by self-serving individuals betraying the country to foreign governments for economic or ideological reasons (meaning spies), but also about what was regarded as a bastion of democracy: the domain of the whistleblower. The discussion about insider threats now refers to revealing secrets to the press. It is this shift in domain of application of this label, corroborated with the criminalization of printing information obtained from such sources, and the emergence of this new figure of the leaker oscillating between "aiding the enemy" and "democratic hero," that is worthy of note. This is the domain of application of Foucauldian rhetoric, particularly as it brings into focus a more robust theorizing of the links between power, knowledge, and subjectivity.

Preventing an insider threat is a reactive measure on the part of the government. The existing legislation, policies and procedures designed to prevent something like this to occur, or mitigating its effects, have failed. The permeability of digital borders as well as the possibility to remove vast troves of classified documents on a simple thumb drive makes even one leak potentially disastrous. For comparison, it took Ellsberg three months in 1969 to photocopy 47-volumes of the content of what was subsequently published as the Pentagon Papers in June 1971, after two years of effort to make them public. By

contrast, according to government sources, NSA is still unable to quantify how many documents were removed by Snowden, with new revelations regularly cropping up. With such vast revelations exposing the scope and gargantuan dimensions of the systems of global surveillance, (revealed by the Snowden documents), the government documents working toward a model of deterrence seem to acknowledge a certain failure of previous policies. The need for further study and increased vigilance is articulated in every document analyzed here.

Deterring insider threats begins with defining the insider. "Malicious insider" is variously defined as a "current or former employee, contractor, or business partner" who "has or had authorized access to an organization's network, system, or data" and "has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems,"[197] or the "any activity by military, government, or industry employees whose actions or inactions, by intent or negligence, result (or could result) in the loss of critical information or valued assets." [198] This threat that an insider will use his or her authorized access to do harm to the United States includes "espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities."[199] As leaks to the press about nefarious practices or day to day operation of state institutions have become commonplace, these documents begin to include such offenses alongside espionage. The digital space is undisciplined; it leaks. As such it needs to be reined in or disciplined.

Indeed, The Department of Defense Directive number 5240.06, from May 17, 2011, modified on May 30, 2013, incorporates more directly what other documents only vaguely refer to: namely the issue of unauthorized leaks. Among the "reportable contacts, activities, indicators, and behaviors" the document directly refers to "acquiring, or permitting others to acquire, unauthorized access to classified or sensitive information systems," "discussions of classified information over a non-secure communication device," "reading or discussing classified or sensitive information in a location where such activity is not permitted ," and "unauthorized copying, printing, faxing, e-mailing, or transmitting classified material." Similarly, the Army regulation 381-12, "Threat Awareness and Reporting Program," October 10, 2010, also includes among the "indicators of potential terrorist associated insider threats" alongside illegal diversion of military technology and unauthorized intrusions into automated information systems, the "unauthorized disclosure of classified information."

In some documents, unauthorized disclosures have made it to the top of the list of potential dangerous acts by insiders. In the Army's threat assessment manual about espionage and terrorism, the first reportable threat-related incidents are "attempts by anyone, regardless of nationality, to obtain or acquire unauthorized access to classified or unclassified information concerning DOD facilities, activities, personnel, technology, or material through questioning, elicitation, trickery, bribery, threats, coercion, blackmail, photography, observation, collection of documents or material, correspondence (including electronic correspondence), or automated systems intrusions." Contact with individuals that might suggest potential recruitment by a foreign intelligence service or

international terrorist organization and actual espionage, personnel who are "engaging in, or have engaged in, actual or attempted acts of treason, spying, or espionage," come second and third after disclosures.[200] If this list is also a hierarchy of importance, we get a sense of the increasing salience of disclosures to the insider threat apparatus.

Some documents make finer distinctions between espionage and leaking. The Department of Energy (DoE) report titled "Identifying at-Risk Employees: A Behavioral Model for Predicting Potential Insider Threats," separates serious crimes and abuses associated with insider threats—such as espionage, sabotage, terrorism, embezzlement, extortion, bribery, and corruption—and a larger, broader category of "malicious activities" including copyright violations, negligent use of classified data, fraud, unauthorized access to sensitive information, and illicit communications with unauthorized recipients alongside the more serious crimes. This distinction however is simply a definitional one. Leaking classified information does not yield discrete modes of intervention. As we can see, these documents lump together unauthorized leaks of documents with espionage, theft, and sabotage on behalf of foreign powers or economic entities. This proximity to crimes such as espionage, theft, and sabotage thus makes the act of disclosure activate a system of surveillance and intervention designed for enemies of the state.

It is important to note, however, that the insider is not considered a spy per se. As Patrick Reidy, a former Chief Information Security Officer with Federal Bureau of Investigation, emphasizes during his presentation at *Black Hat Briefings* (a computer security conference), *insiders become threats*. In other words, insider threats do not join

the organization for malicious purposes but develop such purposes once inside the organization. This is to separate spies, who join the institutions for the express purpose of doing harm) from leakers, who become malicious after joining the organization. This separation also serves to emphasize the failure of using strategies of detecting spies or outsiders (hackers) for the detection of potential leakers.

As we have seen, the person disclosing unauthorized information, no matter how relevant to the citizens of the country that information might be, is associated with espionage, with thieving, and sabotage. Next, I explore the consequences of this inclusion of disclosures alongside espionage via Foucault's concept of the "delinquent."

The New Delinquent of the Digital Age

> … the 'criminal' as existing before the crime and even outside it.[201]

Foucault describes a shift in the power to punish, and the emergence of what he dubs the carceral archipelago. While Foucault is not a rhetorician, he reads voraciously anything from newspapers, describing in gruesome detail a regicide, plans for ideal prisons, to musings on the issues of punishments and rules for detentions houses. What he sees in this dispersion of texts is the double process of the disappearance of the "spectacle of the scaffold" and the elimination of pain. He tries to define what would be later called disciplinary power. "This book" remarks Foucault in *Discipline and Punish* "is intended as a correlative history of the modern soul and of a new power to judge; a genealogy of the present scientific-legal complex from which the power to punish derives its bases, justifications and rules, from which it extends its effects and by which it masks

its exorbitant singularity."[202] Set against the excesses of sovereign power, with the right to kill and let live, with its juridical subjects, the disciplines function productively, subtly, on the body, in order to reach the soul. Of interest for my analysis is this shift from the body to the soul, this "substitution of objects" of which Foucault talks about when it comes to penal practice. My argument is we can see that this logic—governing the understanding of crime, criminals, and criminal propensities as it pertains to leaks—is still at play in the incipient domain of understanding and deterring leakers.

The delinquent is not a criminal, but *the individual with a propensity to commit a crime*, the privileged object of knowledge for a constellation of scientific domains and, consequently, a plastic, never-ending surface for intervention. I am interested in isolating this figure, as a result of the shift in the logics of punishment, in Foucault's conceptualization of disciplinary power, as an essential element for understanding the consequences of including leakers or whistleblowers into the political and legal category of "insider threat."

At first, Foucault begins to talk about this shift with people who are caught and punished. Apart from the crimes as juridical objects, judgments begin to be passed also on "passions, instincts, anomalies, infirmities, maladjustments, effects of environment or heredity."[203] In other words, it is no longer a matter of simply punishing the act but of understanding it, unpacking its causal chain. Thus, the juridical verdict begins to take into consideration "knowledge of the criminal, one's estimation of him, what is known about the relations between him, his past and his crime, and what might be expected of him in the future."[204] It is no longer a matter of figuring out the torturous spectacle appropriate

to the nature of the crime. New knowledge becomes relevant not only for sentencing criminals but for punishing them as well. All these pieces of information, as Foucault notes, "behind the pretext of explaining an action, are ways of defining an individual."[205]

The seriousness of the crime of leaking classified documents combined with the ease of removing large troves of documents (the Afghan War, Iraq War logs, and the State Department leaks combined amount to over seven hundred thousand documents) makes "understanding" leakers, establishing behavioral causalities, a must for state institutions. By extrapolating what a leaker is before the crime, based on cases of people that have already perpetrated this crime, these lists of behavioral and psychological factors become the driving force and justification of an institutional surveillance machine that directed at all employees. Leakers are defined before the act of leaking occurs. It is not the crime of leaking that defines the criminal but something else, a propensity that must be read in the employee's life and psychology.

If insiders become threats, then we are dealing with a process, a process unfolding over time and, thus, opening the lives of those going through this process to intervention. The authors of the "Common Sense Guide ..." note that malicious insiders "do not fit a particular profile" and "there is no way to use demographic information to easily identify a potentially malicious insider," but they are quick to add that there are "ways to identify higher risk employees," and it is possible to "implement mitigation strategies to reduce their impact."[206] The authors expressly caution companies to identify malicious insiders "not by stereotypical characteristics but by their behavior" which includes "threatening the organization or bragging about the damage the insider could do to the organization …

downloading large amounts of data within 30 days of resignation ... using the organization's resources for a side business or discussing starting a competing business with co-workers … attempting to gain employees' passwords or to obtain access through trickery or exploitation of a trusted relationship (often called 'social engineering')."[207] The "Common Sense Guide …" is a practical guide replete with technical advice on how to secure networks and when to terminate someone's' access. This advice is accompanied by a plethora of case studies where disgruntled and jaded employees lash out during or after being fired. In discussing (good) "practice 16," where companies are urged to develop a formalized insider threat program, citing Obama's Executive Order 13587, the authors tasks the HR team with detecting "possible signs of behavioral issues related to insider threats." Prominently among these are "repeated policy violations … disruptive behavior … financial difficulty or unexplained extreme change in finances … job performance problems" each an indicator correlated to sabotage, fraud, and IP theft respectively.[208] "Training supervisors to recognize and respond to such behaviors, claim the authors, "is a worthwhile investment of an organization's time and resources."[209] The attention is focused here on *observable behaviors as signifiers of potential risk.*

Indeed most documents list such observable behaviors creating the profile of a potential malicious insider. The FBI PowerPoint presentation at RSA conference [named after the initials of its co-founders] in 2013, an annual conference related to information security, authored by Kate Randal, an Insider Threat Analyst, and Patrick Reidy, a former Chief Information Security Officer with Federal Bureau of Investigation (still with the Bureau at the time of this particular report), clusters psychological factors in four

categories: (1) disgruntlement (respond poorly to criticism; cannot cope with stress at work; exhibits sudden change in work performance; and reacts inappropriately to stress act work); (2) ego (acts domineering, harasses others, acts argumentative; superiority issues; acts selfish; manipulative; acts like rules do not apply; poor teamwork abilities; irritability; makes threats; engages or threatens to engage in retaliatory behavior); (3) emotional vulnerability (change in beliefs, unusual level of pessimism; unusual level of sadness; irritability; makes threats; difficulty controlling emotions); and (4) relationship/financial problems (problems with divorce or with marriage; stress in home life; financial problems; difficulty coping with stress at home; sudden change in financial status; irresponsibility; acts selfish.) The action caption encourages participants to "get plugged into your HR reporting chain and look for these issues." What emerges is the common attempt in all these documents to scientifically link certain behaviors, certain predispositions with certain crimes, in this case, that crimes perpetrated by a trusted insiders. While this is very common, this is also mimics the shift in the power to punish, in the way apparatus of power conceptualizes crime and responsibility.

As Foucault notes, "The delinquent is to be distinguished from the offender by the fact that it is not so much his act as his life that is relevant in characterizing him."[210] The distinction between "illegal enemy combatants" and "insider threats" is relevant here. One can be erased, the other must be known. The latter's life must yield its secrets so a system of prevention can be established. As Foucault further argues "the introduction of the 'biographical' is important in the history of penality. Because it establishes the 'criminal' as existing before the crime and even outside it."[211] It is this existence outside

and before, that becomes the target of surveillance and monitoring. These documents detailing modes of dealing with insider threats do not simply establish a system of indiscriminate surveillance (of one and all) but an intelligent system that read signs of potential criminal behavior, that surveils and catalogues lives, that must know in order to prevent.

Foucault further contends that "as the biography of the criminal duplicates in penal practice the analysis of circumstances used in evaluating the crime, so one sees penal discourse and psychiatric discourse crossing each other's frontiers." It is at this intersection that Foucault sees forming the notion of the "dangerous individual," which makes it possible "to draw up a network of causality in terms of an entire biography and to present a verdict of punishment-correction."[212] In "The Psychology of the Insider Spy," one of the select few documents featured on the NCIX website (the Office of the National Counterintelligence Executive),[213] Dr. David L. Charney M.D., a clinical psychiatrist, involved in the defense of three convicted spies, defines a new paradigm for understanding the insider. If previous studies arguably have given a high priority to money and greed, Charney points to deeper psychological factors. Charney provides us with the ten "life stages" of the insider spy, "a dynamic rather than static view" of the motives that lead someone to spy. This story of a composite spy, based on his experience as a consultant of the C.I., takes us from "the sensitizing stage" (stage one) where one's unfortunate upbringing while not per se an indicator seems to be a contributing factor, to the "brooding in jail stage" (stage ten); in between a slow decent into treachery. Second stage, the "stress/spiral stage" uses the biblical story of Job as shorthand for the

psychological "perfect storm." "We all like to think we could weather anything," Charney cautions us, "but try adding impending financial bankruptcy, severe personal health threats, an IRS audit, teenage son getting arrested, spouse having an affair, teenage daughter getting pregnant—all at the same time—and one can imagine even the strongest person buckling under the pressures. However, as Charney himself notes "what adds up to the breaking point for any individual will vary and is probably not predictable." As in the case of a "less than optimal childhood," this series of divine plagues hitting one's adult life might not be an indicator/predictor. Stage three, the "Crisis/Climax/Resolution" stage heralds the entrance into the "personal bubble psychology" defining one's view of the world "in terms that are internally logical, coherent and consistent, but in terms of the real world, also very wrong." In other words, a view of the world internally consistent yet epistemically wrong. Here is where spies are born, out of failure, lashing out at the wrong target. For Charney it is the "intolerable sense of personal failure, as privately defined by that person" that explodes outward towards one's institution/country/co-workers making most spies "not so much recruited by the skill of a hostile service intelligence officer but is rather self-recruited." For the rest of the article, Charney takes us from the "post-recruitment" stage, through "remorse/morning-after," "active spy career," "dormancy," "pre-arrest," all the way to the "arrest and post-arrest stage" and the final "brooding in jail stage." As the author of one of the few documents posted on the website of the Office of the Director of National Intelligence, Charney's assertions carry a lot of weight.

For Foucault, thus, the observation of the delinquent "should go back not only to the circumstances, but also to the causes of his crime; they must be sought in the story of

his life, from the triple point of view of psychology, social position and upbringing, in order to discover the dangerous proclivities of the first, the harmful predispositions of the second and the bad antecedents of the third." [214] Poor upbringing combined with psychological failure defines the doomed spy. Thus, based on the analysis of convicted spies, Carney paints the picture of a man—"95% of insider spies are males"—with an unfortunate childhood, besieged by adversities in adult life, yet privileged enough to get the kind of education that would allow one to apply for a job in community intelligence, a man whose ego makes him look for the root cause of his own woes outside, all in all a self-perceived failure in all stages of his life. Thus the key, argues Charney, is "how this intolerable sense of personal failure gets managed. Almost always, this is a state of mind based on male psychology." The picture of someone who, after making the decision of spying under "pressure cooker conditions," feels remorse and a renewed sense of failure tied to his handling of his own bad situation, an active career in which the "honeymoon" is followed by ebbs and flows in an attempt to withdraw oneself form the spy career and yearns to be caught and thus end this stressful existence. For Charney "the usual suspects of insider spy motivations" (greed, sociopathy, ideology, ego and arrogance) are less important than the "unfolding of the movie of a person's life." Lack of patriotism is rarely an issue. "Surprisingly," contends Charney the insider spy "is rarely truly dedicated to the subversion and destruction of his native land." "His beef," colorfully adds Charney, "was always primarily with himself, and with the local people or institutions that were his nearby, handy targets." For Foucault the delinquent is a "biographical unity, a kernel of danger, representing a type of anomaly." The insider is a man with a male

ego, unable to take the adversities of life, lashing out. Presumably, being able to watch each employee's "life –movie" would give us the best chance for early detection.

Foucault notes that what distinguishes the delinquent from the offender is that "he is not only the author of his acts (the author responsible in terms of certain criteria of free, conscious will), but is linked to his offence by a whole bundle of complex threads (instincts, drives, tendencies, character). The penitentiary technique bears not on the relation between author and crime, but on the criminal's affinity with his crime." [215] For Carney, the existential dilemmas of the insider spy related to failures (failure to navigate his own life, failure to find a proper solution and failure to succeed at being a spy), a sense of being stuck between equally strong forces (what Charney calls "stuckness") and a perfect storm of stressors and remorse or what he calls "convergence of psychology" (fear of being caught, constant uncertainty, yearning for deliverance and relief, despair and hopelessness.) He also discusses other factors such as the socioeconomic pyramid: the low level access employees where their "troubling life issues are described well by country music lyrics: money woes, mean bosses, women who betray trust, and other basic life stresses"; the midlevel employees whose "problems tend to be the "mid-life crises" more typical of the middle class"; and the top level employees, the most dangerous if turned and whose individual psychologies are "more idiosyncratic and tend to be based on affronts to personal and professional pride." Based on this life picture, Charney contends that the long-term dynamic evolution of the insider spy, he suggests "mechanisms that create safe exits for troubled insiders" because conventional approaches, reliant on screenings during hiring background investigations, stringent

security practices, and various high tech monitoring schemes do not work very well. Charney acknowledges that his model does not "encompass all insider spies" gesturing towards what he calls "insider spies who seem to hark back to the ideological spies of the thirties and forties" among other unnamed "anomalous cases." What make one move in one direction or another, what make one deal successfully with life's adversities or fail to deal with them, is unclear.

For Foucault, the prison fabricated the delinquent in the sense of recidivism, and, of more importance, "has introduced into the operation of the law and the offence, the judge and the offender, the condemned man and the executioner, the non-corporal reality of the delinquency that links them together and, for a century and a half, has caught them in the same trap.[216]" It is this delinquency, contends Foucault, "that now comes to haunt the untroubled courts and the majesty of the laws; it is this delinquency that must be known, assessed, measured, diagnosed, treated when sentences are passed. It is now this delinquency, this anomaly, this deviation, this potential danger, this illness, this form of existence that must be taken into account when the codes are rewritten."[217] Despite Carney's repeated attempts to joke and point to the lack of predicting power of these signs—"if having gone through a tough childhood … predicted a likely turn towards insider spying, perhaps the vast majority of the entire intelligence, law enforcement and defense communities would have to be let go"— the document does mark all these phenomena and events (tough childhood, adult adversities, inability to deal with frustration, etc.) as significant. This significance translates into surveillance of individuals that display such marks.

The Metonymical Logic of the Insider Threat Apparatus

As we have seen, based on caught and convicted insiders, the notion of a life movie, of a long process in virtue of which trusted insiders become threats raises the issue of psychological and behavioral causalities, an issue reminiscent of Foucault's discussion of delinquency. What we see is a retrospective assessment of behaviors of convicted spies translated into a matrix of indicators of potential insider risk designed to preventively label employees as potential leakers.

My main claim in this chapter is that the problematization of digital leaks engenders the emergence of an insider threat apparatus that obeys a metonymical logic. Next, I unpack this claim by delving into its constituent concepts. First, problematizations. For Foucault himself, as we have seen, problematization "is the totality of discursive or non-discursive practices that introduces something into the play of true and false, and constitutes it as an object for thought (whether in the form of moral reflection, scientific knowledge, political analysis, etc.)."[218] For this project the point of departure is the emergence of information sharing—as in leaks—as a problem in our digital present. Truth-telling, whistle-blowing, treason, government, corporations, consumers, surveillance, "freedom fighters," technologies and digital practices all intersect into the emergence of on old problem—transparency in governing—with a new twist brought about by the unruliness and permeability of the digital systems and the accessibility of information. From the initial "Collateral Murder" video leaked by the now infamous WikiLeaks whistleblower website to Romney's "47%" video, partially credited with losing him the 2012 presidential election, or to the Vatican leaks,

"principled" leaks have been in the middle of an ideological and rhetorical scandal, a phenomenon oscillating between "high treason" and "democratic necessity." The prosecution of Bradley Manning, Aaron Swartz's suicide allegedly caused by the threat of a 30-year prison sentence for sharing academic articles at no cost, the current administration's alleged "war on whistleblowers," all raise important question about truth, about sharing information, about ownership of knowledge and ultimately about power structures in a digital world.

With the understanding of the apparatus as complex machinery assembled through various interactions between discursive and nondiscursive elements in mind, as detailed in the introduction, my claim is that this strategic drive to manage the problem of insider threats functions according to a metonymical logic. What is, then, metonymical logic? I must begin by noting that despite being concerned with discourse and its role in the makeup of the world, Foucault has been charged with ignoring rhetoric. Foucault's critics mean here perhaps that Foucault is ignoring a particular disciplinary understanding of rhetoric as an omnipresent art of symbol use and an equally generalizable art of interpretation. Foucault falls victim here to what Greene calls "the monstrous morphology of rhetoric" as in rhetoric "shape shifts from a practice (a presidential speech) into a perspective/method (a mode of inquiry), into a discipline (rhetorical studies), and, finally, into a process (power)."[219] In his last seminars, Foucault not only engages *parrhesia* but opposes it to the art of rhetoric, thus reactivating our platonic traumatic disciplinary moment. Paradoxically, Dave Tell sees precisely in this opposition of *parrhesia* or techniques of the self and rhetoric as evidence of Foucault's rhetorical

thinking. Not only does Foucault not ignore rhetoric, but, following Tell's account, Foucault is a "rhetorical thinker of first order," not for his emphasis on discourse but for his conceptualization of power and confession through a Nietzschean inspired tropological understanding of rhetoric.[220] "In my reading," posits Tell "Foucault is an eminently rhetorical thinker … because of his profound insight that modern power works metonymically—it intensifies its effects by substituting origins for events" and thus is "a distinctively rhetorical analysis of power." [221]

For Tell, what makes Foucault a rhetorical thinker is his critique of confession that takes Nietzsche's understanding of knowledge as metonymical and extends it to the functioning of power. For Nietzsche metonymy is the substitution of abstract causes for concrete appearances. In other words, the eruption of events and the materiality of the world are being domesticated through language. Abstract concepts resulting from observation are posited as the cause of those very events. For Nietzsche, points out Tell, the metonymical movement par excellence is "Plato's replacement of *eide* (that which appears) with *ideai* (ideal forms)." [222] For Tell, Foucault's long life efforts to understand confession and the functioning of power are buttressed by a critique of metonymical logic. Indeed, Foucault "sought to recover the world of surfaces from the tyranny of metonymy."[223] Foucault's concept of dangerousness—meaning "the individual must be considered by society at the level of his potentialities, and not at the level of his actions; not at the level of the actual violations of an actual law, but at the level of the behavioral potentialities they represented"[224]—is a "distinctively metonymical concept." Tell

showcases how Foucault sees the dangerous individual, the delinquent, the criminal, the author, the homosexual, and sexuality as results of the same metonymical logic.

The distinctions between "author," "criminal," and "dangerous individual" are, for Tell, ultimately, of intensity not of substance. As Tell argues "the 'delinquent' provides power a new 'hold' or 'point of application'; it is no longer the 'crime or offense exactly' against which power is directed but rather crime's double: the life behind the offense, the criminal behind the crime, the delinquent behind the offender—in sum, the cause inserted ex post facto behind the effect."[225] These "metonymical subjects" are created after the fact, by observation, by juridical examination, by confession and then posited as the origins of the acts. This metonymical operation thus "renders the subject vulnerable to new modes of power"—disciplinary power which now can be applied before the act. Tell thus argues that for Foucault confession is a fundamentally metonymical practice, that the function of confession "was always to divorce language from events—crimes, sexual acts, and so forth—and attach it instead to abstractions in which the particularities of the event were ignored."[226] Furthermore, confession, understood as such, is "an essential ingredient in the development of modern power."[227] Examination and confession, argues Tell, "were the sine qua non of individualizing power; they were an essential condition, an intrinsic component, without which such power could not be exercised."[228]

My interests lie primarily in using metonymic subjects (delinquent) and the metonymic logic as the process of substitution of causes for effects, to sketch the function of the insider threat apparatus. The metonymical subject here is the "insider threat," and

the logic that governs the assemblage of discourses, technologies, and institutions, is the metonymical logic. Hence my main claim in this chapter that the problematization of digital leaks—the "becoming problem" of digital leaks for governance—engenders the emergence of an insider threat apparatus—replete with changes in how networks function, public discourses about the link between leaks and loss of life, changes in policies regarding the surveillance of employees by their co-workers, etc.—obeys a metonymical logic—by which I mean that the psychological traits, observable behaviors, and work related behaviors observed in/reported by convicted spies become slowly part of an developing apparatus of surveillance, detection and deterrence that classifies these "observables" as indicators for higher insider threat risk (meaning the substitution of effects for causes). This process creates an area of dangerousness that opens all state institutions and employees to fields of knowledge and spaces for surveillance and application of power.

The Insider Threat as Metonymical Subject

> "Behind the offender … stands the delinquent whose slow formation is shown in a biographical investigation."[229]

All the documents reviewed here suggest a causal relation between certain behaviors and higher insider threat risk. The FBI brochure, one of the only three documents linked on the NCIX website (alongside CERT Common Sense Guide, and Charney's True Psychology of an Insider Spy), is "an introduction to detecting and deterring an insider spy." The document, a simpler and more direct document, designed for quick dissemination, starts with a few choice words on the front page: disgruntled,

working odd hours, unexplained affluence, and unreported foreign travel. The brochure points to accessing networks and classified information from taking proprietary or other material home without need or authorization, proprietary or classified information not related to one's duties, remotely accesses the computer network, to working odd hours, unexplained affluence, and showing unusual interest in coworkers as abnormal behaviors. The brochure also list personal factors such as greed or financial need, anger/revenge, problems at work, ideology/identification, divided loyalty, ego/self-image adventure/thrill, vulnerability to blackmail, ingratiation, compulsive and destructive behavior, family problems. Of particular interest, resonating with the problem of the leaker, is ideology/identification translated for us as the "desire to help the 'underdog' or a particular cause." We are cautioned, as in other documents that while many people "experience or exhibit some or all of the above to varying degrees … most people will not cross the line and commit a crime." I am not so much concerned with whether this profile is real, whether it is empirically correct; for now I am concerned with how the apparatus of power (especially that of national security) defines the figure of the leaker, the insider thereat.

As we have seen, the metonymic subjects are composites; their traits, extracted from the cases of convicted spies, become an elusive figure haunting the halls of state institutions. The Department of Defense (DoD) "Insider Risk Evaluation and Audit" paints such a picture. According to the report the offenders are generally driven by greed, disgruntlement, conflicting loyalties, ego-satisfaction and "often exhibit similar early indicators or precursors of subsequent damaging behavior." In other words, the

behaviors exhibited by convicted spies, extracted from retrospective studies, though metonymical substitution, become signifiers of dangerousness. Consequently, the report suggests developing practices and policies designed to "detect these precursors and intervene effectively." Some of the areas of intervention designated are: policies and practices, recruitment, preemployment screening, training and education, continuing evaluation and policy implementation, and employee intervention. These constitute new areas of intervention, new subjects to be surveilled, with more scrutiny, for longer periods of time, throughout all stages of employment.

The report, like all the other documents, acknowledges its epistemological limitations. "Due to a lack of controlled research," we are cautioned by the authors, "we do not know if individuals with all the risk indicators … are at significantly greater risk than individuals without." The significance of this disclaimer cannot be overstated. The problem with such disclaimers is that these reports are not subjected to the same rigorous scientific procedures as research in a peer reviewed journal, for example. Nonetheless, once the apparatus of power considers the insider problem as "significant enough to use the best data available to try to suggest ways to mitigate the risk," the machinery of surveillance, the reporting, monitoring, and interventions, is activated. Even though the authors claim that "this tool is not designed to be an infallible predictor," and that "the risk of false positives for any single, or even multiple risk factors, is much too great to use these measures in this fashion"[230] once a behavior is problematized as potentially "disruptive" or constituting a "precursors of subsequent damaging behavior" it becomes

of target of knowledge and intervention of power. The insider threat as metonymical subject lurks behind these disclaimers.

Regardless of their limitations, these documents tend to set up complex systems of early detection and surveillance with overlapping categories of indicators. The DoD report speaks of contextual risk factors ranging from cultural (especially when dealing with cross cultural assumption and communication), social, and political conflicts that can increase the risk of whistleblowing, all the way toe economic and sector specific local factors (from generalized economic pressures to pressures within a specific sector) can lead to, claim the authors, an increased insider risk. However, the focus of the report is on "observable behaviors" common to insiders. Citing the CERT Study, the authors point to six observations common to both IT sabotage and espionage: most insiders "had common personal predispositions"; stressful events (such as sanctions by the organization) worked as a contributing factors; the insider displayed "behaviors of concern" before and during the attacks; their technical/digital/online behaviors were suspect; organizations failed to detect or "ignored rule violations;" and "lack of physical and electronic access controls" facilitated both IT sabotage and espionage. A complex table sets up a grid of what the authors call "predispositions," "counterproductive work behaviors" or CWBs (as "any intentional behavior on the part of an organizational member viewed by the organization as contrary to its legitimate interests,") [231] as well as anomalous network behaviors, overlaid on the lifespan of an employee (from preemployment to work) and particular moments of organizational intervention (before or during the hiring process, during the employment lifespan of the employee). The result in

a matrix of knowledge (the need to know certain predispositions), of surveillance, monitoring, and reporting (of observable behaviors and digital systems), and of intervention.

Thus, to know, one must begin with history. Surveillance unfolds backward in time because in order to determine "if an applicant has previously engaged in criminal activities or questionable behavior," and thus potentially do so again, "civil and criminal record checks should be conducted."[232] Records can "provide information on possible personal irresponsibility" ranging from lawsuits to judgments and liens. This "financial irresponsibility" increases the risk that candidates for a job might engage in insider activities for economic reasons.[233] Such background checks for applicants, celebrates the report, "has recently been extended to the world of online activity" from "looking for candidates' names on search engines" to "examining their personal sites … Facebook" all the way to "assessing their role play in alternative online social networks like Second Life," which "may now be as important to a successful background check as traditional sources."[234] One's history becomes a legible catalogue of potential risk indicators.

This process by which one becomes a malicious insider appeals to the term "self-radicalization." "Self-radicalization" is described as "significant steps an individual takes in advocating or adopting an extremist belief system for the purpose of facilitating ideologically-based violence to advance political, religious, or social change. The self-radicalized individual has not been recruited by and has no direct, personal influence or tasking from other violent extremists. The self-radicalized individual may seek out direct or indirect (through the Internet for example) contact with other violent extremists for

moral support and to enhance his or her extremist beliefs."[235] The use of the internet, one's online behaviors as it were, one's beliefs, ideology are termed dangerous. I am not claiming that the DoD does not have legitimate reasons to phrase it this way nor am claiming that there are nefarious reasons for vague terminology one that can be used to suppress dissent. The signs of dangerousness are no longer tied to terrorist organizations but tied to individual (online) behaviors, to a self-generating and self-contained process called self-radicalization. The burden of proof seems to be lower. As noted earlier, Mudd's theory of persuasion, linking young, impressionable people, driven by emotion, who live their life online and are immediately and directly affected by images from abroad, self-radicalization is by no means an irrelevant term.

Indeed, self-radicalization and its attended online behaviors can trigger the scrutiny of this apparatus. The vast NSA surveillance system that spies on everyone can be traced in a sense to both the technological ability as well as to this diffused notion of dangerousness. Mudd's statements can be seen as an off-hand remark during a TV interview on a satirical news show but if we link it to terms such as self-radicalization as deployed in the DoD report, as well as the list of online behavior to watch for and report others doing it as employees of the DoD, we see that this perspective is not a joke. Colbert's amusing rejoinder—where he asks if we should put boots on the ground or just watch YouTube to see what's inspiring these kids— is prescient and funny. As it turns out, the NSA mass surveillance included infiltrating massive multiplayer online games such as World of Warcraft and Second Life.[236] So in a very real sense, virtual boots are put on the virtual grounds in order to monitor and catch terrorists. The emergence of the

insider threat as metonymical subject happens at the intersection of existing knowledge and research in behavioral science and the need, expressed by all these documents, for consolidating this knowledge as well as of further research. In the next section, I trace through "guides" and regulations, the (re)constitution of a field of knowledge pertaining to dangerousness in relation to the problem of insider threats.

The Constitution of a Field of Knowledge

> Indeed, it is in discourse that power and knowledge are joined together.[237]

These metonymical subjects, as we have seen, are born out of observations and shrouded in a field of knowledge. All documents reviewed speak of the need to push research into the direction of causally linking predispositions and observable behaviors to the act of leaking classified information (beside espionage, theft, sabotage.) As Foucault notes, "a corpus of knowledge, techniques, and 'scientific' discourses is formed and becomes entangled with the practice of the power to punish."[238] Foucault argues that we should abandon the idea that knowledge exists independently of power relations and that in fact "power produces knowledge."[239] This is not simply by encouraging it or applying it, adds Foucault. In fact, power and knowledge "directly imply one another" as in "there is no power relation without the correlative constitution of a field of knowledge, nor any knowledge that does not presuppose and constitute at the same time power relations."[240] The Carnegie Mellon university's "Common Sense Guide to Mitigating Insider Threats

4th Edition" "funded and supported by the United States Department of Homeland Security under Contract with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense,"[241] offers a concrete example of the this notion of power/knowledge. This evidently is not the subtle connection Foucault talks about; it is rather of the obvious species of power encouraging and applying certain knowledges; nonetheless, besides having state institutions concerned with national security funding a university to do research into insider threats, we also have the sense of a budding field of knowledge.

The repeated disclaimers of the lack of predictability of these models of detection combined with the call for further research speak to the formation of a new field of knowledge, albeit a limited one, a new "science of man (as dangerous insider)," to play with Foucault's notion that the shift in the power to punish contributes to the development of the "science of man." The link between problematization (the leaks/leakers becoming a problem for thought, for governance, for the public), and the emergence of apparatuses designed to deal with the problem, emergence which both engenders and is supported by domains of knowledge, is here most obvious. If we go along with Tell's account of Foucault's critique of metonymical logic, we must not forget that very logic is first theorized by Nietzsche in the constitution of knowledge.

The leaker must be known. What makes an insider a threat must be detected in the minutia of his or her behavior. As I have already noted, one's behaviors, one's archive (reports, travels,) must be under surveillance; a new archive must be kept to allow the

possibility of determining variations; a baseline for proper behavior - a norm of conduct is to be determined and the variation must be regarded with suspicion. This Common Sense Guide thus stems from collaboration between the U.S. Secret Service and Carnegie Mellon University Software Engineering Institute's CERT[242] Coordination Center (CERT/CC) "designed to develop information to help private industry, government, and law enforcement better understand, detect and ultimately prevent harmful insider activity." This first report, focusing on the banking and finance sector, was, according to its authors and financiers "the first of its kind to provide a comprehensive analysis of insider actions by analyzing both the behavioral and technical aspects of the threats."[243] Reidy, in his presentation at the RSA security conference, praises Carnegie Mellon's work as "the go-to *academic collection* of insider threat cases." The term "*academic collection*," rhetorically legitimizes this body of research. This growing repository of knowledge is referenced and widely disseminated potently forming the basis for early detection systems though may more institutions then the ones identified here.

This constitution of a field of knowledge is perhaps most evident in the connections created in these documents between the science of threat detection and other domains of knowledge. While not fully developed, some documents contain allusions to the link between medical histories, particularly related to mental illness, and the propensity to engage in insider attacks. As Foucault argues, biography becomes crucial in defining and understanding the delinquent. "The observation of the delinquent" argues Foucault "must be sought in the story of his life, from the triple point of view of psychology, social position and upbringing, in order to discover the dangerous

proclivities of the first, the harmful predispositions of the second and the bad antecedents of the third."[244] Citing CERT's SEI (Software Engineering Institute) the authors discuss such biographical predispositions alongside rules violation and "serious mental health disorders and interpersonal skills and decision-making biases."[245] Based on this study, the authors indicate that "certain historical actions (e.g., arrest or previous security or policy violations) and personal characteristics (e.g., serious mental health problems, drug abuse, and personality issues) have been associated with insider activities." The authors do take the time to mention that "it should be noted that many more persons will have a history of these actions (or possess these personal characteristics) than will commit insider offenses" and as such increase the risk for false positives.[246] Nonetheless, these disclaimers do nothing more that rehearse over and over the old rhetorical trope of occultatio (or paralepsis), the drawing attention to something in the very act of pretending to pass it over.[247] In fact, within a still unformed domain of knowledge, the metonymical movement relies heavily on occultatio.

The "science of detection" is linked most closely with psychology. The DoD Insider Threat analysis talks about an "intensive psychological assessment" referring to honesty testing, psychological assessment and the polygraph. The authors contend that these methods can be controversial given that "their reliability and validity have been questioned and have been the focus of legal and legislative actions."[248] Citing research that looks at personal characteristics correlated with the risk of CWBs, the authors point to the use of dimensions of personality defined by the Five Factor Model (FFM - personality factors of openness to experience, extraversion, conscientiousness,

agreeableness, and neuroticism or emotional stability.) The authors proclaim that "significant literature" indeed supports that there is a relationship between FFM dimensions and CWBs with "significant correlations were found between irresponsible behaviors and measures of achievement, agreeableness, and openness from FFM."[249] Foucault talks about a process of "exchange" between disciplinary networks within the penal apparatus. "as medicine, psychology, education, public assistance, 'social work' assume an ever greater share of the powers of supervision and assessment, the penal apparatus will be able, in turn, to become medicalized, psychologized, educationalized."[250] The authors of the DoD analysis cite research claims that although "academic researchers have not been successful in finding correlations between these characteristics and CWB's" in fact "personality disorders—especially malignant narcissism and psychopathic or sociopathic disorders—have been associated with espionage in post-hoc, prison based assessments of espionage subjects."[251] We note here both occultation and metonymy at work. The disclaimer is wrapped in a projection forward based on a retrospective analysis. Although "extreme scores on conscientiousness or agreeableness or high scores on personality disorder traits might not disqualify an individual for employment" argue the authors "in combination with at-risk scores on honesty testing, questionable references or background data" combined with a sensitive position "the scores might contribute to an overall decision against hiring."[252] "Employees," argue the authors, "must be educated to recognize these predispositions in the form of observable behaviors and be trained on how to report these risks and react when confronting them." For this purpose "human and IT detection and recording

programs must be in place" as well as put in place "scripts … that guide how the organization responds when these personal predispositions manifest themselves in the form of observable risks." [253]

The "science of detection" extends beyond psychology. The DoE's "Identifying at-Risk Employees …" builds knowledge on insider threats on solid ground. They cite 30-40 studies and relevant research on workplace aggression, entitlement, and counterproductive work to computer deviance in the workplace, information security, and criminal profiling. The authors argue that "this disparate literature has far-reaching application in a variety of fields of inquiry including information security studies, computer science, criminology, psychology, organizational behavior, and many more."[254] What we see in the DoD document is an attempt to bring all these diverse fields of knowledge, mentioned above, to bear upon the problem of the leaker. All these government studies and guides for dealing with insider threats do is try to ascertain early indicators—before the job is even offered—to monitor social problems—during employment—alongside instituting digital systems of monitoring network behavior.

This process of detection, of surveillance, and of intervention thus requires multiple fields of knowledge. The potential leaker becomes a psychological being, a social being, and a cyborg with a detectable behavior in virtual environments. As an object of knowledge, the leaker also becomes the target of prevention and intervention. Although the language of dismissal is always there, these documents advocate mostly pre-emptive intervention. Indeed most threats, argue the authors citing research, "could have been prevented by timely and effective action to address the anger, pain, anxiety, or

psychological impairment of perpetrators, who exhibited signs of vulnerability or risk well in advance of the crime."[255] As Foucault argues, "the prison … is the place where the power to punish, which no longer dares to manifest itself openly, silently organizes a field of objectivity in which punishment will be able to function openly as treatment and the sentence be inscribed among the discourses of knowledge."[256] Indeed, this is a mutually beneficial solutions as this process of surveillance that lead to identifying employees with elevated risk of insider threat can prevent an "unnecessary cost to the employer" as well as "helping the employee before a bad situation turns worse." [257] Insider threats can be cured or distracted.

The development of a "science of detection" depends on creating accurate knowledge about the link between behaviors and the propensity for crime. "Despite a growing body of research into the psychology and motivation of insiders, it is difficult to predict who will commit security fraud," the authors nonetheless speak of certain dispositions, certain observable behaviors. The DoE study ("Identifying at-Risk Employees …") tries to fill the gap in research in terms of methods to evaluate "psycho-social" behaviors that "can predict increased risk for insider threats." This study thus tries to integrate into one instrument workstation and network activity logs but also include preparatory behavior, verbal behavior and personality traits. They align their research and efforts alongside others advocating that behavioral evaluation, monitoring and profiling must be integrated with securing the networks and monitoring network behaviors to achieve "an effective overall security package." The roadblocks are, as the authors acknowledge, existing laws such as Americans with Disabilities Act, Rehabilitation Act,

making it illegal to use clinical testing to discover mental disabilities in the job hiring process or during employment, as well as the lack of valid comparison between good and disgruntled employees. In other words, to discover something meaningful, one must be able to compare (and thus gather data and monitor) good employees scores/behaviors/trait with the disgruntled ones. Nonetheless, there is a litany of correlations and behaviors and indicators, that are observable, can be monitored and recorded. The workaround the law is not to administer clinical test but to "conduct audits aimed at identifying manifestations of these personality factors such as absenteeism, disgruntlement, disciplinary issues, and so forth."[258] Here the authors advocate the development of instruments of psychological evaluation that would bypass the laws put in place to prevent such knowledge interfering with one's employment prospects.

It is precisely this science of detection that allows for the metonymical movement. For Foucault knowledge of the offence, of the offender, and of the law "made it possible to ground a judgment in truth." In other words

> The question is no longer simply: 'Has the act been established and is it punishable?' But also: 'What is this act, what is this act of violence or this murder? To what level or to what field of reality does it belong? Is it a phantasy, a psychotic reaction, a delusional episode, a perverse action?' …. it is no longer simply: 'Who committed it?' But: 'How can we assign the causal process that produced it? Where did it originate in the author himself? Instinct, unconscious, environment, heredity? … no longer simply: 'What law punishes this offence?' But: 'What would be the most appropriate measures to take? How do we see the

future development of the offender? What would be the best way of rehabilitating him?'[259]

This science born out of convicted spies, hackers, and saboteurs does not turn around to punish those convicted, in manner similar to that described by Foucault. Rather, the metonymical movement here is precisely the transformation of this body of knowledge into a preemptive apparatus that takes these signs of dangerousness and, based and them, implants this ghostlike leaker in the real body of one who has not disclosed information yet. Thus, workplace disgruntlement and employee dissatisfaction are "two key underlying causes of deviance in the workplace and organizational crime" while extra-organizational factors—marital and familial problems, personal finances, and addictions—are seen as influencing the intensity of the two factors; similarly "employee attitudes … strong negative affect" are considered "precursors of intentional counterproductive (and even subversive) behaviors ranging from absenteeism to various forms of retaliation." This *semiotics of dangerousness* is developed around clinical testing, which is against the law, by linking the signifiers—behaviors, manifestations—to the signified—dangerous personality traits. Thus, despite the reasoning of the law, the insider threat issue is grave enough to try to get that kind of information the law expressly forbids.

This "science of detection" must integrated all these disparate fields of knowledge for better predictability power. The "Identifying at-Risk Employees" report ends with proper acknowledgments of limitation and suggestions for future research.[260] One problem is "the extent to which HR or management personnel in an organization are

informed about the kinds of behavioral indicators posited in our model." Thus one of the areas is training of HR personnel and managers about being aware of the connection between these psychosocial factors, behaviors and insider threats. But beyond this, the authors advocate developing the cyber monitoring system beyond simply "anomaly/signature detection methods" towards their integrated model that links observables with these anomalous cyber behaviors in "in an effort to develop a more effective system with potential to anticipate and prevent insider crimes."[261] Prediction, admittedly for Reidy as well, is "very difficult." In short notes Foucault, "it is not the activity of the subject of knowledge that produces a corpus of knowledge, useful or resistant to power, but power-knowledge, the processes and struggles that traverse it and of which it is made up, that determines the forms and possible domains of knowledge."[262] Foucault thus divorces the production of knowledge from the subject. The focus is on this complex intertwining of power and knowledge; what comes to be known is not determined by some objectives laws but by the complex interactions between what is known, and relations of power.

The problematization of leaks that poses a problem for and of governance engenders the emergence/consolidation of an insider thereat apparatus that uses existing knowledge while stimulating new directions of research. The need to push the research in new directions, specifically in the direction of causally linking behaviors and predispositions with insider threat crimes, is evident. The disclaimer that this research is not yet solid enough to make predictions, that one should be cautious, gets lost in the detailed description of behaviors and surveillance apparatuses that must be deployed to

detect, deter, and mitigate insider threats. In all these discussions about causal links, the term "observables" is a common refrain. "Visibility" thus is central for the insider threat apparatus. As such, in the context of discussing the insider threat in relation to Foucault's conceptualization of disciplinary power, I will address, next, the Panopticon.

"If You See Something, Say Something": Power and Visibility in Panopticon

> He who is subjected to a field of visibility … becomes the principle of his own subjection[263]
>
> Monitoring promotes productivity and affords better control over counterproductive employees."[264] (Department of Defense)

As Foucault notes in *Discipline and Punish*, "the success of disciplinary power derives no doubt from the use of simple instruments; hierarchical observation, normalizing judgment and their combination in a procedure that is specific to it, the examination."[265] Disciplinary power is visual; it looks and it needs to be seen in its exercise; the ultimate point of this visuality being the integration of these mechanisms into oneself. The Panoptic architecture—as the annular building always exposed to the perpetual surveillance of the middle tower—allows Foucault to illustrate the functioning of the modern disciplinary power. Indeed, "the Panopticon must not be understood as a dream building" but as a "diagram of a mechanism of power reduced to its ideal form; its functioning, abstracted from any obstacle, resistance or friction, must be represented as a

pure architectural and optical system: it is in fact a figure of political technology that may and must be detached from any specific use."[266] In other words, the principle of visibility buttressing surveillance makes the panopticon function as a generalizable technology of power; its constituent (metaphorical) elements— a central tower presumed occupied, always looking, a group of "prisoners" always aware of being watched—make it possible for us to identify a panoptic principle of power relations, "a generalizable model of functioning; a way of defining power relations in terms of the everyday life of men."[267]

These documents set up a mesh of surveillance, perpetual training, and ceaseless reporting. Thus, for the authors of "Common Sense Guide," the information security team "can conduct periodic inspections by walking through areas of your organization, including workspaces, and identifying security concerns" in order to spot security concerns which should be brought to the employee's attention "in a calm, nonthreatening manner and in private" and where "employees spotted doing something good for security" such acts should be rewarded and, "where possible" the rewards "should be presented before a group of the employee's peers."[268] The examination, for Foucault, is a "normalizing gaze, a surveillance that makes it possible to qualify, to classify and to punish. It establishes over individuals a visibility through which one differentiates them and judges them." That is why, adds Foucault, "the examination is highly ritualized. In it are combined the ceremony of power and the form of the experiment, the deployment of force and the establishment of truth."[269] What we see here, as much as it is visible, the establishment of "normal" behavior. The guide sketches behavioral baselines from proper conduct in the work place to normal network behavior. "Whenever one is dealing with a

multiplicity of individuals on whom a task or a particular form of behavior must be imposed," Foucault tells us, "the panoptic schema may be used."[270]

The Panopticon is not simply an issue of surveillance but of being seen seeing. The DoD Directive number 5240.06 not only names behaviors as dangerous, but makes observing and not reporting these behaviors in others a crime in its own right. "If you see something say something," has a threatening implication, "… or else." Indeed "personnel who fail to report the contacts, activities, indicators, and behaviors … may be subject to judicial and/or administrative action."[271] Similarly, the Army regulation 381-12, "Threat Awareness and Reporting Program" the surveillance net is prefaced by claiming that these behavioral threat indicators are not only visible but often overlooked. Indeed "coworkers, associates, friends, and supervisors of those engaging in espionage or terrorist activity have overlooked indicators of potential threats … which, had they been reported, would have minimized the damage to national security or saved the lives of DA personnel."[272] That is why "as an adjunct to threat awareness training, CI units are encouraged to use all forms of DOD Media to promote threat awareness."[273] "Personnel subject to the UCMJ who fail to comply with the requirement to report these incidents are subject to Punishment."[274] In other words, not reporting, not keeping one's co-workers under permanent surveillance is a punishable offence. This, however, is not a secret net of spies, keeping an eye on each other, without everyone knowing. This needs to be public. The panopticon function rests on the principle of visibility. The relation of force, of surveillance, must be present and known. Indeed, Foucault talks about the effect of the Panopticon as inducing in the inmates "a state of conscious and permanent visibility that

assures the automatic functioning of power."[275] In other words, contends Foucault, "he who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjection."[276] This distribution of surveillance (making employees keep each other under surveillance), or "crowd sourcing security" as Reidy calls it, does nothing more than disseminate the Panopticon function within institutions. The disciplining gaze comes from anywhere, even if it comes from nowhere. Employees become human relays for the disciplinary gaze. As in the case of the Panopticon, this burden ultimately acts as a self-disciplining mechanism. The point here is not whether one personally would engage in espionage or unauthorized leaking/whistleblowing, or whether one accepts the task of watching the others or reject such a practice for creating a toxic work environment, the point is to feel watched.

This evident visibility of surveillance is recognized and integrated in these models. The only real issue with this increased visibility and surveillance, these documents suggest, comes as a psychological drawback, as the knowledge of monitoring can affect job satisfaction and trust. Citing certain studies, the authors of the DoE report contend that that "workers are driven to semi-schizoid responses" in relation to the power and authority of "technologically mediated supervision" and this loss of privacy "can create feelings of vulnerability that may give rise to deep-seated feelings of alienation." The productive reason for which an employer should engage in surveillance—such as assessing worker productivity, protecting company assets, ensuring compliance with

workplace policies, and national security—must be weigh against this psychological effect. Here we get a sense that, as opposed to the Panopticon, we are not dealing with prisoners. The solution is "procedural justice" as in the full disclosure of the process of surveillance. Thus "disclosed fully, explained, and managed equitably across employees" it might not in fact "be considered as unfair by employees, and the mutual trust relationship required for a healthy organization may remain intact." In other words, surveillance is not truly a secret operation. The Panopticon does not function as it is designed to if nobody knows the tower in the middle exists. In the end, as Foucault notes, "a real subjection is born mechanically from a fictitious relation."[277]

Conclusion: The Insider Threat Apparatus

So what does this all amount to? Regardless of the differences between the proposals for the creation or improvement of systems of early detection, all documents reviewed here advocate the creation of something new. This something new, this "science of detection," has to rely on knowledge, particularly behavioral science, to write the grammar of dangerousness for insider threats. Some authors decry the previous models designed to detect anomalous network behavior (similar to our credit card fraud detection). Most advocate integrate in this preemptive strategy of detection one's biography, one's work and private behavior, one's financial situation, one's travels and website visits. This is not simply the indiscriminate extension of surveillance to everyone but a carefully assembled system of policies and procedures that obey the metonymical logic by creating the profile of a potential leaker (a composite out of studies of convicted

hackers, spies, and saboteurs) that then organizes an apparatus of surveillance and intervention and compels the development of a new domain of knowledge.

For example, Reidy, advocates a "holistic approach," combining HR information, context (financial, reports, travel), psycho-social factors and behavioral indicators (particularly in relation to use of information networks). Behavioral based detection means "a baseline based on users volume, velocity, frequency, and amount based on hourly, weekly, and monthly normal patterns." Normal behavior is defined and, as such, anomalous behavior becomes an indicator of heightened risk justifying further surveillance and potentially intervention. What is distinct about this approach is the overlaying of all these factors. Individually they do not work or predict, but overlaying normal behavior at work over contextual factors and psychosocial factors, should, according to Reidy, work better. Observables" (something you can see) in term of behaviors, monitoring of behaviors in relation to networks (something credit card companies already do), establishing baselines for comparison, monitoring each individual and establishing patters of differentiation (behavioral analytics), all these are glossary terms for a vocabulary of discipline. As Foucault argues, the lines between confinement, punishment, and institutions of disciplines, already blurred in the classical age, disappeared, constituting "a great carceral continuum" leading to the diffusion of penitentiary techniques through institutions and practices. If the prison "transformed the punitive procedure into a penitentiary technique" the carceral archipelago, argues Foucault, "transported this technique from the penal institution to the entire social body."[278]

So what is the psychosocial model? This model is based on the accepted relationships between certain personality characteristics and counterproductive work behaviors (CWB) or "higher-risk employees." The authors of the DoE report developed the model by conducting discussions with HR professionals and managers to identify "behavioral 'proxies'" for the personality characteristics that could lead to heightened concerns insider threats. Thus, note the authors, the model was "highly observation-based" focusing on "observable behaviors that could be recorded and audited." Despite being based on behavioral observables, the model "can support making inferences about the possible psychological/personality/social state of an employee." The psychosocial indicators are disgruntlement, not accepting feedback, anger management issues, disengagement, disregard for authority, performance, stress, confrontational behavior, personal issues, self-centeredness, lack of dependability, absenteeism. Confronted yet again with the commonality of these "observables" the authors caution us that the judgments based on these observations "will necessarily be subjective" as their intent is not to emerge at the other end with "an objective test instrument." "Nonetheless" add the authors, "with appropriate training … management and HR personnel would better understand the nature of the threat and the likely precursors or threat indicators that may be usefully reported to cyber security officers. This is thus an early warning/detection system that could lead to further and increased monitoring. Indeed, "for security analysis purposes, only individuals about whom a manager is 'highly concerned' would be considered for further analysis in the insider threat model." Without going into details, the result is a Bayesian network—or "belief network" a probabilistic graphical models,

combining graph theory, probability theory, computer science, and statistics representing probabilistic dependencies among random variables.

As Foucault argues "by means of a carceral continuum, the authority that sentences infiltrates all those other authorities that supervise, transform, correct, improve …. its function, the power to punish is not essentially different from that of curing or educating. It receives from them, and from their lesser, smaller task, a sanction from below …. The carceral 'naturalizes' the legal power to punish, as it 'legalizes' the technical power to discipline."[279] The DoE report advocates the combination of behavioral indicators in the workplace in addition to the workstation monitoring methods. This is not just human surveillance. As the authors note, particularly for large organizations, "it is difficult and costly to train sufficiently many experts" and therefore a "computer model based decision aid will help ensure that the "system" is applied consistently and fairly."[280] Such a model "automates this process" if the organization creates employee evaluation processes that enable "appropriate data to be recorded into a database of personnel files either at regular intervals such as during employee performance evaluations or when these behaviors are observed."[281] The Panopticon goes digital. As Foucault contends "the carceral texture of society assures both the real capture of the body and its perpetual observation; it is, by its very nature, the apparatus of punishment that conforms most completely to the new economy of power and the instrument for the formation of knowledge that this very economy needs."[282] This vision of an integrated system, similar to the one in Reidy's psychosocial model, that takes into account indicators in the form of observable behaviors and monitoring of workstation

takes shape here as well. “We are advocating,” proclaim the authors, “the establishment of a system for collecting and tracking concerning behaviors so they may be taken into account by an objective system that integrates these psychosocial indicators with physical and cyber monitoring data to derive a more complete picture of potential ‘problem employees’ and insider threats.”

Thus, certain behaviors flag individuals for further surveillance and monitoring, a system that is well known to all individuals. This is a complex model integrating data from multiple sources. Indeed, there is a vision at the heart of this statistical model. The authors envision a psychosocial model helpful to HR experts with access to a database “containing information and judgments associated with the psychosocial factors;” a system developed for recording these judgments, combined with “other behavioral data that may be available (such as disciplinary actions)” and with cyber/workstation monitoring data to “produce a composite picture that a security analyst can examine.” The results would be the object of analysis for a “multidisciplinary team comprising management, HR, security, cybersecurity personnel as well as counterintelligence officer for the most serious transgressions.”[283] This model, argue the authors, is not to be used for dismissal but as a guide, as an aid to identify potential risk that warrants further surveillance, monitoring, and perhaps intervention. Thus “rather than being regarded as a Machiavellian/punitive system, the use of such tools can be considered to offer a fair and consistent application of behavioral monitoring, and with proper privacy safeguards in place, it benefits both employees and employers.” The vision is completed; the system becomes neutral, objective, applied to all in equal measure, polished gradually to detect

only the wicked; known to all and thus working by its mere existence for the benefit of all. The authors thus move from research that established that in the majority of cases malicious intent was "observable" before the fact to abstracting those observables and transforming them into indicators. The result is a prototype psychosocial model using 12 indicators to predict levels of risk. "Assuming that these behavioral indicators are available for collection," argue the authors, then a predictive model can be developed a valid model—tested alongside HR expert evaluations of behavior. The Panopticon, contends Foucault "functions as a kind of laboratory of power. Thanks to its mechanism of observation, it gains in efficiency and in the ability to penetrate into men's behavior; knowledge follows the advances of power, discovering new objects of knowledge over all the surfaces on which power is exercised."[284] This integrated system is part human part machine, a surveillance cyborg. Thus, indicators feed the system with behaviors that flag certain individuals who then are further placed under surveillance, by monitoring their cyber activity.

Without denying the existence of real threats posed by employees that betray the trust of state institutions, what we see in these documents, in the wake of all the scandals of the past 10 years involving the leaks of classified documents, is:

(1) First, the problematization of digital leaks, the "becoming a problem" for and of governance. By this I do not mean simply, the government has a problem, but though the insistent contestations over this issues (as we will see in the next chapter on *parrhesia*) the problem of digital leaks ties into the problem of transparency in governance, to link up with a gradual erosion of the trust in state institutions;

(2) Second, the inclusion of this offense—leaking classified documents—alongside espionage, theft, and sabotage with all its attendant contaminations through proximity. Manning had to fight the hardest the charge that he was "aiding the enemy," a crime caring the penalty of life imprisonment. Furthermore, the criminalization of leaking is accompanied by criminalization of distributing the information, such as the AP phone tapping incident or the DOJ's attempt to indict a journalist as a co-conspirator in a leaking scandal.[285]

(3) Third, the emergence of a "new" domain of knowledge, a "science of detection," with a specific object: the shift from a trusted insider to a threatening insider. As I noted, the issues of spies go farther in time that the emergence of leaks as a problem of governance, the specific calls in all these recent documents for renewed research in behavioral science that can provide a better model of detection, prediction, and deterrence, alongside recognizing the failures of the previous ones – does allow me to add the "new" in "new domain of knowledge" to signify the gravity of the leaks and the impact they have on policies and procedures of surveillance.

(4) Fourth, the assemblage of methods of inquiry, techniques of surveillance, authorities, and departments into what I have labeled an *insider threat apparatus* whose logic of functioning is metonymical. This means extracting behavioral patterns and psychological predispositions from apprehended insiders and transforming them into signifiers of delinquency; this new *semiotics of dangerousness* becomes material in new systems of surveillance of employees, evolving beyond simply monitoring anomalous

network behavior, to include biographical details, behaviors outside the workplace, psychological predispositions, etc.

(5) And fifth, the emergence and/or consolidation of an insider threat apparatus, buttressed by this new domain of knowledge, whose governing logic is metonymical, rests on panoptic visibility. Employees becomes visible for the institutional structures and for each other. Perhaps Snowden's revelation of the vast NSA surveillance machine and the public awareness that follows does not spell the doom of this apparatus but its immortality.

Thus, the delinquent is our guiding metaphor for the insider threat. The metonymical logic is the logic governing the apparatus coagulating around the problematization of leaks. The power knowledge confluence moves towards the knowable threatening self. And panopticism provides the mechanism for a technology of surveillance via human relays. The insider threat program is, in its infancy, trying to manifest the metonymical logic into a new apparatus of organizational surveillance.

Chapter IV

"But what of the man?"[286] From Manning to Snowden, the Leaker as *Parrhesiastes*

> "I don't consider myself a 'pacifist,' 'anti- war,' or (especially) a 'conscientious objector' … I am a 'transparency Advocate'" (Manning).[287]

In the governmental imaginarium, at the intersection of an established term—*insider threat*—and a new problem—*leaks of classified documents*—emerges the spectral figure of the *digital delinquent*. Born out of convicted spies, thieves, and disgruntled saboteurs, the digital delinquent comes to inhabit an ever expanding apparatus of surveillance designed to know, detect, deter, and intervene in the life of the criminal before the crime has been committed and comes to define the criminal as such. This metonymical reversal of effects for causes, of ex post facto observations about the lives of "infamous 'men'" for what made them infamous, feeds off of admitted speculations. However, despite caveats, disclaimers, admitted predictive limitations, and repeated calls for behavioral science to intensify its efforts to account for the mutation from a trusted

insider into threatening self, the documents reviewed in the previous chapter continuously build an expanding library of suspicions behaviors linked to the act of disclosing information. Consequently, through this metonymical reversal, everything about a federal employee becomes significant. One's biography, mental health, and psychological predispositions, one's life, movements, and financial situation, and one's work, domestic, and network behaviors—the *observables* in short—become signifiers of a *semiotics of dangerousness* providing the conditions of existence for a prescient insider threat apparatus. This mutation, however, is anything but uncontested. As the apologia goes, what we are witnessing is not the trusted insiders becoming a monstrous threat but the courageous whistleblower rhetorically framed to appear a spy. If there is a perversion, say the apologists of these leaks, it is the one perpetrated by the state apparatus itself; it is not a war on government databases, it is a "war on whistleblowers." If the previous chapter was devoted to charting how the leaker as digital delinquent comes to haunt the halls of the state apparatus, this one addresses a complementary question: what kind of shadow do the leakers themselves cast on public discourse?

In this chapter I will consider how (in)famous leakers think and speak of themselves and of their actions. Wikileaks' mission statement,[288] Chelsea Manning's declarations during and after her trial, and Edward Snowden's public interviews and statements, make up the texture of this chapter. I take the ancient concept of *parrhesia*, as the courage to speak the truth, as my theoretical and methodological guide through these texts. To be sure, I am not interested in whether these individual are truly *parrhesiastes* (if such determinations can be made) or if their acts (leaking classified documents) can be

qualified as "speaking" the "truth." My focus lies rather in sketching through these texts how the leakers construct themselves as seeming akin to the ancient *parrhesiastes*. My contention is that through these highly publicized cases, we can see thrown back into political and rhetorical play the ancient concept of *parrhesia* as the courage to speak the unadorned truth in the agora.

Although it is difficult to untangle these threads in the arguments themselves, first I will consider the rhetorical construction of an Orwellian world emerging in the public communications of Wikileaks, Manning, and Snowden. Second, against the background of this contemporary manifestation of *1984*, the vision of a transparent political universe, akin to Habermas' ideal public sphere, begins to take shape. Third, within the contrast between these two worlds, the leakers come to define themselves as *parrhesiastes*. Their tragic existence becomes necessary in the gap between existing democracies and ideal ones.

"The Big Brother is Watching You:" The Orwellian Government

> "You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized."[289]

My focus in this section is not to establish empirically the political reality of an Orwellian state apparatus but rather to discerning its rhetorical articulation in the statements and interviews of the leakers themselves. Indeed, the *parrhesiastes* identity emerges against this blinding dystopian reality. In a statement, read by her lawyer David Coombs, Manning summarizes her views of the United States' morally dismal logic of

war, its bankrupt humanitarianism, and jingoism masquerading as patriotism and self-defense.[290] Manning links the trauma of 9/11 and the new kind of enemy it engenders to new ways of waging war. Thus for Manning, since 9/11 "our country has been at war … with an enemy that chooses not to meet us on any traditional battlefield, and due to this fact we've had to alter our methods of combating the risks posed to us and our way of life."[291] Although she "initially agreed with these methods and chose to volunteer to help defend my country," the reality of the war, with its attendant secrecy and atrocities, has made an impact, making her "question the morality of what we were doing."[292] The contours of these foreign policy scandals are common place by now:

> We consciously elected to devalue human life both in Iraq and Afghanistan … sometimes killed innocent civilians … instead of accepting responsibility for our conduct, we elected to hide behind the veil of national security and classified information in order to avoid any public accountability … we internally debated the definition of torture … held individuals at Guantanamo for years without due process … inexplicably turned a blind eye to torture and executions by the Iraqi government … stomached countless other acts in the name of our war on terror.[293]

This summary of a deadly and morally corrupt foreign policy is a stand-in for the steady accumulation of atrocities that made Manning realize that "in our efforts to meet this risk posed to us by the enemy, we have forgotten our humanity."[294] This lost moment of humanity is linked historically to other questionable events, to "similar dark moments for the virtues of democracy," such as the Trail of Tears, the Dred Scott decision, McCarthyism, and the Japanese-American internment camps "to name a few."[295] "I am confident" adds Manning, "that many of our actions since 9/11 will one day be viewed in a similar light."[296] These comparisons, as well as the confidence in the harsh judgment of

history, paint a bleak picture of the overall post 9/11 war effort. "Patriotism" concludes Manning "is often the cry extolled when morally questionable acts are advocated by those in power."[297] Lest we forget, Manning ends by citing Howard Zinn, that "there is not a flag large enough to cover the shame of killing innocent people."[298] Reading these morally questionable government sanctioned actions as part of this brief history of atrocious polices with tragic consequences legitimizes, as we will see, Manning's own actions as courageous acts of disclosure.

We get a similar bleak picture of an overbearing state apparatus on the wrong side of history from Edward Snowden's public appearances. In his first interview in Hong Kong, conducted by Glenn Greenwald and Laura Poitras, Snowden reveals the existence of a vast US-lead system of global surveillance. The NSA and the intelligence community are focused on getting intelligence "wherever it can by any means possible," argues Snowden.[299] Right from the start, we get the image of an indiscriminate system of surveillance that purportedly serves the national interest based on "sort of a self-certification."[300] It is not just its global reach that raises questions about NSA's role in protecting national interests but its indiscriminate deployment of this system of surveillance. Now, NSA "targets the communications of everyone" and "ingests them by default," decries Snowden.[301] Although he contends that the intentions might be to target someone associated with a foreign government or a terrorism suspect, "they're collecting your communications to do so."[302] Thus, right from the beginning, we see Snowden articulating the existence of an indiscriminate system of surveillance, with global reach, gorging on information. Indeed, Snowden reveals that "if a surveillance program

produces information of value, it legitimizes it."[303] This means, argues Snowden, that "in one step, we've managed to justify the operation of the Panopticon."[304] For Snowden, the Panopticon seems to function as a stand-in for the ideal apparatus of surveillance that covers the entire social field, an image not far from Jeremy Bentham's original vision. As Snowden further remarks, "every time you pick up the phone, dial a number, write an email, make a purchase, travel on the bus carrying a cell phone, swipe a card somewhere, you leave a trace and the government has decided that it's a good idea to collect it all, everything, even if you've never been suspected of any crime."[305] The extent to which our cyborg selves leave virtual marks in the world is not unknown to us; the sheer number of traces and the extent to which these traces are being assembled in vast databases, however, clear was unknown to us. Thus, the image of this all-seeing eye, collecting all our digital traces, comes to confirm democratic fears of an autocratic government.

Snowden continues to paint the picture of an overbearing state apparatus that accumulates data and can create suspicion round any life. When asked "Why should people care about surveillance?" Snowden begins to paint the picture of an Orwellian universe, where "even if you're not doing anything wrong you're being watched and recorded."[306] This totalitarian pipedream is now accessible as a consequence of technology advancements. As Snowden points out, "the storage capability of these systems increases every year consistently by orders of magnitude."[307] This capability means that a total archive begins to accumulate. As Snowden argues, "you don't have to have done anything wrong … simply have to eventually fall under suspicion … then they

can use this system to go back in time and scrutinize every decision you've ever made, every friend you've ever discussed something with."[308] Suspicion becomes the organizing principle of this hermeneutics.

Indeed, a total archive read through a hermeneutics of suspicion (of terrorism) is the very logic of an Orwellian universe where thought can be a crime. The thought's immaterial nature leads the system to search for its traces in behaviors, in actions, in encounters with others, etc. As Snowden notes, this indiscriminate accumulation of data allows the state apparatus "to derive suspicion from an innocent life and paint anyone in the context of a wrongdoer."[309] This is the distinction that Snowden himself draws between the good old days when "the government would identify a suspect … go to a judge … get a warrant and then they would be able to use the totality of their powers in pursuit of the investigation" and the dismal present where the government uses "the totality of their powers in advance - prior to an investigation."[310] We see not only a government that perhaps oversteps in order to protect, but also a system that can be abused, an ever accumulating archive that provides a real support for the fictional "thought crime" featured in Orwell's *1984,* an author and an image that Snowden directly invokes at times.

This images are confirmed at least in part by these revelations as well as by our analysis in the previous chapter of the institutions tasked with collecting everything—biography, behavior, archives, and network habits—as a source of information to derive the potential of becoming an insider threat. It is those who possess the total archive that are also authorized, to echo Snowden's expression, by a sort of "self-certification," to

read the connections between behaviors and the thought that generated it. Snowden speaks of all the programs of information and data collection, of the cooptation of corporate power (Google, Facebook, Apple, and Microsoft) that cast a net so wide that there are "no ingress or egress points anywhere in the continental United States where communications can enter or exit without being monitored and collected and analyzed."[311] What we get is the image of an information society whose borders, as invisible, immaterial, and permeable as they might seem, are nonetheless constantly monitored.

Indeed, the very term "Orwellian," which has become the shorthand for such revelations in media, is overtly referenced. Snowden reminds us in his 2013 taped Christmas message that the US and UK governments have created a system of mass surveillance extended both worldwide and in-depth in the minutia of everyday traffic, and "Great Britain's George Orwell warned us of the danger of this kind of information."[312] Today's technological abilities, however, dwarf even Orwell's prophetic imagination. As Snowden adds, "the types of collection in the book—microphones and video cameras, TVs that watch us—are nothing compared to what we have available today. We have sensors in our pockets that track us everywhere we go."[313] For Snowden, this dystopian future possible is being actualized. "A child born today will grow up with no conception of privacy at all," Snowden cautions, never knowing what it means to have "an unrecorded, unanalyzed thought."[314] If the invasion of privacy seems either not severe enough or a price we are willing to pay "to be safe," children become a way to speak of a future possible. As such, the appeal to the fictional *1984*, as the quintessential metaphor

for tyrannical governments, guides our imaginations on a slippery slope into the future to see these problems compounding over time.

This surveillance machine is global in its reach and intent, and thus, according to Snowed, that much more dangerous. Snowden speaks of the "Five Eyes" alliance—an Anglophone formation including UK's GCHQ, US' NSA, Canada's C-Sec, Australian Signals Intelligence Directorate and New Zealand's DSD—results in a decades-long development of a "supra-national intelligence organization that doesn't answer to the laws of its own countries."[315] Here we have a sense of a larger surveillance system that goes beyond the confines of NSA and the USA Snowden hints at a globalized system that keeps up with technological advancements for the purpose of tracking everyone. Indeed, Snowden illustrates this point with "XKeyscore," described as "a front end search engine" that allows intelligence agencies with access to it to "to look through all of the records they collect worldwide every day."[316] What this does is to allow intelligence agencies to read anyone's email. Moreover, and more gravely, suggests Snowden, this program allows individual tagging which can lead to the creation of a "fingerprint," as in the network activity unique to one particular person based on tracking of usernames, associations, friends etc. This, according to Snowden, allows one to be tracked even when one tries to hide their online presence. This global reach amplifies the image of this ever encroaching state apparatus.

The specter of an ever accumulating total archive, the development of algorithms that track and define our network behaviors making us visible even when we attempt not to be, the global reach of this system, as well as the automated search feature, paint the

picture of a bureaucracy capable of knowing us and predicting our behaviors more then we can do so ourselves. The logics of this vast system of surveillance echoes Foucault's discussion of bio power in *History of Sexuality Vol. I*. It is both totalizing and individualizing. The analytics track both statistical movements of populations and individual behaviors; it can look for significant patterns in data and individual aberrations. To turn on its head Jacques Lacan's famous statement about the unconscious—*in you more than you*—we can say, in relation to the digital self, *outside you more than in you*. In other words, our selves are out there being assembled from digital traces with greater predictive accuracy that we can muster. However, instead of "If you watched *V for Vendetta* you might also like to watch *1984*," the fear that this digital totalitarian future seems to activate is that this algorithm can be repurposed to say "If you watched *V for Vendetta* you might also like to visit the closest FBI office." As we have seen in the previous chapter, for the purposes of surveillance, intervention and termination, the algorithm of detection does not need proof of wrongdoing but certain indicators to trigger it. In other words, this digital self is public and, thus, ties our real selves to its purported actions and thoughts betrayed by those actions. Snowden revelations about this system, filtered through his references to Orwell, seem to suggest that what was once designed to detect enemies is slowly repurposed to keep everyone under surveillance and, thus, under control.

Apart from its global reach, this system is also fraught with abuse and itself permeable to attack. The potential abuses of the system, Snowden suggests, are already happening. LOVEINT refers to the not so common yet "common enough to garner its

own spycraft label" practice of using the NSA's surveillance capability to spy on love interests.[317] Besides this "minor" infringement, Snowden reveals that the potential risk of abuses is far greater. While its *raison d'etre* seems still to harken back to the traumatic moment of 9/11, this system of surveillance, according to Snowden, now steps into economic espionage. Asked on German television whether the United States spies on Siemens, on Mercedes, or on other successful German companies, Snowden maintained that he not able to give detailed information as journalists are still processing this information; hoverer, he added, "there's no question that the US is engaged in economic spying."[318] Love interest and economic interests sneak in, alongside protecting the US from threats both foreign and domestic, as reasons for accessing these databases.

It's not just the abuse that makes this machinery increasingly dangerous. Another concern that Snowden expresses is that the privatization of government functions. Not only is this a vast system of surveillance, fraught with abuse and overreach, but it is also strangely permeable. As comedian Stephen Colbert once quipped, the NSA is impervious to anyone who is not a 29-year-old hacker with a thumb drive. Indeed, Snowden himself contends that his own case "highlights the dangers of privatizing government functions." Thus, "you have private for profit companies doing inherently governmental work" such as espionage, surveillance, hacking foreign systems. There is "very little oversight," concludes Snowden.[319] Lobbying leads to a situation in which "government policies are being influenced by private corporations who have interests that are completely divorced from the public good."[320] You end up, notes Snowden in a self-referential quip, with "private individuals who have access to what the government alleges were millions and

millions of records that they could walk out the door with at any time with no accountability, no oversight, no auditing" while "the government didn't even know they were gone."[321] In other words it is not just an ever expanding apparatus of surveillance overstepping the constitution and moral bounds, but it is a permeable system.

It is the unjustified nature of this machinery that brings his revelations closest to the Orwellian universe. In the end, contends Snowden, this is not about "any sort of particular program, this is about a trend in the relationship between the governing and the governed in America."[322] There's a "far cry" argues Snowden, "between legal programs, legitimate spying, legitimate law enforcement where it's targeted, it's based on reasonable suspicion, an individualized suspicion, and a warranted action – and a sort of dragnet mass surveillance that puts entire populations under a sort of eye that sees everything, even when it's not needed."[323] Snowden thus paints the picture of a security apparatus that uses its technological capabilities and prowess to overstep what Snowden considers reasonable boundaries, to spy on everyone in the world.

While the Manning and Snowden speak of different things—one about the excesses and secrecy of war and violence and the other about national security encroaching on human rights—the images they draw are related, part of a continuum. At the level of their rhetorical construction, both Manning's questions about the morality of some of the war policies as well as Snowden's revelations about an all-enveloping surveillance apparatus, originate in the trauma of 9/11. Furthermore, both apparatuses (of war and surveillance) operate on the same preemptive logic—whereby the rhetorically articulated dangers posed to the nation become justifications for preemptive strikes, wars,

and invasions—raised at the level of state policy by the Bush administration. Lastly, both seem to criticize the rhetorically vague concept of manifest destiny, particularly evident in pro-war and pro-surveillance arguments maintaining the morality of these actions (war in Iraq and Afghanistan, torture, unwarranted surveillance) despite their contested moral worth. Against this system of "dragnet mass surveillance," of war abuses, of careless laughter at civilian deaths, of torture and indefinite imprisonment, of government opacity and silencing, a different, democratic vision coagulates.

"Habermas was Right": Transparency, Criticism, and Control

> Before entering into the detail of the operations of the assembly, let us place at the head of its regulations the fittest law for securing the public confidence, and causing it constantly to advance towards the end of its institution. This law is that of publicity.[324]

The rhetorical thread that links the war abuses reported by Manning and the perversion of national security via a dragnet global surveillance machinery revealed by Snowden is the kind of secrecy resonant with totalitarian fears. The democratic counterpoint to this modern day *1984* rests on the conceptual vocabulary that predictably links truth, transparency, accountability, and freedom of expression to the public good and health of a democracy. Within this democratic vision, as we see in the leakers' own statements, the term "leak" gets an ethical lift becoming "principled leak."

The rhetorical construction of a counterpoint the Orwellian universe, detailed in the previous section, begins with the Wikileaks' mission statement. The reasons for such a choice, given that Wikileaks as an organization does not fit the profile of a

parrhesiastes, are the following: first, it is a concise exposition of both the crisis of democracy and transparency as well of the potential solution, an exposition that buttresses many of accounts of the leakers themselves; second, it is the mission statement of the organization that is at the center of these scandals as well as the origin point for the revival of our debates on whistleblowing and national security; third, Manning herself talks extensively in her trial statement about gradually developing trust in Wikileaks leading up to the disclosures; and fourth, recent revelations based on Snowden's documents show that indeed Wikileaks is still perceived as a threat, kept under surveillance, marked as the object for covert operation designed to dismantle it and the "human network that supports Wikileaks," meaning its website visitors.[325]

Wikileaks articulates its legitimacy by linking its principles to historical documents that articulate the key terms of a transparent and democratic society. Wikileaks' broader principles buttressing its mission are thus "the defense of freedom of speech and media publishing" as well as "the improvement of our common historical record and the support of the rights of all people to create new history," derived, according to their own statement, from Article 19 of the Universal Declaration of Human Rights, which includes "freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." "We agree," proclaims Wikileaks, "and we seek to uphold this and the other Articles of the Declaration."[326] Freedom of expression and freedom of the press, fundamental to modern understandings of democracy, are here reinforced through the Universal Declaration of Human Rights.

Wikileaks makes connections between its mission and an enlightenment vision of society, as well as articulating its own mission as contributing to a betterment of society. Truth-telling, disclosure, and transparency are linked to a better functioning of democracy. "Publishing improves transparency, and this transparency creates a better society for all people" and "better scrutiny leads to reduced corruption and stronger democracies in all society's institutions, including government, corporations and other organizations."[327] In this democratic vision of society, "a healthy, vibrant and inquisitive journalistic media plays a vital role in achieving these goals." "We are," proclaims Wikileaks, "part of that media."

Wikileaks' mission statement can be read here alongside Jürgen Habermas' notion of the Public Sphere. The two narratives move in sync from scrutiny, transparency, access, to a healthy and informed public sphere. We remember Habermas' story: private individuals assemble to form a public body; this public body depends on certain constitutional freedoms such as the freedom of association and freedom of expression; a healthy public body demands that information be accessible to all. The topics for this great public conversation are matters of general interest, connected to the activity of the state. Citizens behave "as a public body," contends Habermas, when "freedom of assembly and association and the freedom to express and publish their opinions-about matters of general interest"[328] are guaranteed. Based on the principle of public information, two of the crucial elements for a strong and healthy public sphere are transparency and access to media. "In a large public body" maintains Habermas, "this kind of communication requires specific means for transmitting information and

influencing those who receive it."[329] Newspapers, magazines, radio, and television "are the media of the public sphere."[330] Thus, media, and now we can add the internet to Habermas' list, works to facilitate this conversation essential for democracy.

Wikileaks articulates the vision of a democratic world, globalizes the task of criticism and control reserved for the nation state. For Habermas, public opinion mediates between society and state. "The expression 'public opinion'" argues Habermas, "refers to the tasks of criticism and control which a public body of citizens informally—and, in periodic elections, formally as well—practices vis-a-vis the ruling structure organized in the form of a state."[331] Thus, from transparency we get accountability and from accountability we get stronger democracies. Citing the U.S. Supreme Court in the landmark ruling on the Pentagon Papers—only a free and unrestrained press can effectively expose deception in government—the Wikileaks project wholeheartedly agrees. "We believe that it is not only the people of one country that keep their own government honest, but also the people of other countries who are watching that government through the media," the statement continues. In a sense we see here also a globalization of this task of scrutinizing government. It's no longer the citizens of one nation inspecting their own government. The global reach of internet in a sense seems to make democratic accountability also global.

Wikileaks situates itself both as *part of* and *apart from* this inquisitive media deemed crucial for democratic societies. If at the start, as we have seen, they proudly state "we are part of that media," as the story develops, they set themselves apart. As Habermas notes, "at one time the process of making proceedings public … was intended

to subject persons or affairs to public reason, and to make political decisions subject to appeal before the court of public opinion. But often enough today the process of making public simply serves the arcane policies of special interests; in the form of "publicity" it wins public prestige for people or affairs, thus making them worthy of acclamation in a climate of non-public opinion."[332] This refeudalization of the social-welfare-state democracies, as Habermas dubs them, translates the contemporary conjecture of competition among conflicting interests, in which "organizations representing diverse constituencies negotiate and compromise among themselves and with government officials, while excluding the public from their proceedings."[333] Thus, continues, Habermas, public opinion can no longer be conceptualized as unrestricted public discussion" but rather by terms such as "public opinion research," "publicity," "public relations work," wherein "the press and broadcast media serve less as organs of public information and debate than as technologies for managing consensus and promoting consumer culture."[334]

Traditional media are framed as part of the problem; its failures are partly responsible for the excess and abuses of the state. Echoing Habermas' concern with the refeudalization of the public sphere, where media coagulates around centers of power, around an increasingly reduced number of conglomerates, where publicity as scrutiny of the state gives way to PR and mass-mediated manufacture and manipulation of public opinion, the Wikileaks project finds that "in the years leading up to the founding of WikiLeaks, we observed the world's publishing media becoming less independent and far less willing to ask the hard questions of government, corporations and other institutions."

What we see is opaque governments in conjunction with lack of access and a complicit and compliant media leading to a diminution of the power and role of the public sphere in politics. Without transparency and access, public opinion cannot be formed, and the common dialogue cannot take place. "We believed this needed to change," goes the Wikileaks statement. Of course this is a simplification of the Habermasian argument, but at least in broad strokes it seems that the Wikileaks project envisions itself as the realizations of this ideal.

If the world's media have become complicit in governments managing public opinion, Wikileaks positions itself an alternative to the failed model of traditional journalism, providing "a new model of journalism." Wikileaks thus posits itself as a solution to an old problem. "WikiLeaks has provided a new model of journalism," given that the organization is mainly based on volunteers and anonymous submissions, thus not motivated by profit and, consequently, not dependent for its revenue on competition for information. Anonymous secret document submission becomes a way to bypass the security and secrecy inherent in government operations. "We don't hoard our information," touts the statement, "we make the original documents available with our news stories." Raw data also means that the information lacks in theory the usual partisan spin of traditional media. This is indeed transparency at a level which cannot be ignored. This mode of journalism also contributes to a participatory scrutiny of institutions. "Readers," the statement reminds us, "can verify the truth of what we have reported themselves." Other media outlets are also encouraged to pick up the stories. The world's media, goes the argument, "should work together as much as possible to bring stories to a

broad international readership." In its design, this is indeed a model that subverts the for-profit 24-hour news cycle.

This alternative model of journalism provides the context to rhetorically and ethically rearticulate the act of leaking classified documents. Indeed, this new model of journalism depends on new modes of news gathering. The citizen as an investigative journalist enters the scene. Leaks are thus rhetorically articulated as ethical acts and placed in relation to the history of a gradual erosion of the power of media and to the advances in technology that lower risks associated with conveying important information as well as give governments new tools to actualize dystopian futures. "*Principled leaking* has changed the course of history for the better," triumphantly announces the mission statement, adding "and it can lead us to a better future."[335] Indeed, "the power of principled leaking to call governments, corporations and institutions to account is amply demonstrated through recent history." The origin point of this history is placed with Daniel Ellsberg and the Pentagon Papers. This is the case that allows the statement to articulate the principled part of the expression *principled leaks*. Thus "he [Ellsberg] comes into contact with the Pentagon Papers ... reveal the depths to which the US government has sunk in deceiving the American people … yet the public and the media know nothing of this urgent and shocking information." Despite secrecy laws and "at great personal risk," notes the statement, "Ellsberg manages to disseminate the Pentagon papers to journalists and to the world." The result is thus exposure of government lies and deception, a hastening of the war's end, and saving of "thousands of both American and

Vietnamese lives." Wikileaks thus positions itself as the moral inheritor of the pentagon papers moment.

Thus, generally, the supportive discourse surrounding Wikileaks fits and is designed to inscribe itself within the larger conversation about the public sphere, about transparency and better governance. The link between transparency of government operation, public access to such information as well as an unrestrained access to media as outlets for opinion formation is reestablished in Habermasian fashion in the Wikileaks statement. What we have here is a cogent rehashing of familiar tropes linking technoculture with democracy. As Hubertus Buchstein remarks, "If one accepts the claims of the optimists, the new technology seems to match all the basic requirements of Habermas' normative theory of the democratic public sphere: it is a universal, anti-hierarchical, complex, and demanding mode of interaction."[336] Activating similar tropes, Wikileaks connects the technological advances of the digital age to their democratic potential, particularly the ability to access and distribute confidential information at a scale unmatched in history, both in term of the quantity as well as in terms of its reach.

Wikileaks thus weaves in technological advances, universal human rights, concrete historical cases of whistleblowing, and the impetus toward a popular and participatory investigative journalism to articulate the vision of an open, and fully transparent to its citizenry, government. Apart from the well-known case of Daniel Ellsberg, the statement references the Declaration of Human Rights as well as the words of the founders. "The great American president Thomas Jefferson once observed that the price of freedom is eternal vigilance…We believe the journalistic media plays a key role

in this vigilance," proclaims the statement. As a media publisher, WikiLeaks claims to rely "upon the power of overt fact to enable and empower citizens to bring feared and corrupt governments and corporations to justice." The result is open government which "answers injustice rather than causing it … exposes and undoes corruption." Indeed, "open governance is the most effective method of promoting good governance." Wikileaks operates discursively within this logic of transparency, resonant with both international principles and US constitutional values, as an essential requirement for a "true" or strong democracy. Rhetorically, it is in the gap between the Orwellian society suggested by war crimes and vast systems of surveillance, and this enlightenment ideal of a transparent polity, accountable to the public, visible in its dealings, that the leakers situate themselves and their actions.

"I am a 'transparency advocate'": On Frankness, Truth and Criticism

> When he [Diogenes the Cynic] was sunning himself in the Craneum, Alexander [the Great] came and stood over him and said, "Ask of me any boon you like." To which he replied, "Stand out of my light."[337]

The above excerpt describes the quintessential scene of *parrhesia*: Diogenes the cynic, living life in self-imposed poverty and simplicity, living in the streets in order to be able to tell the truth, speaking up in defiance to one of the most powerful men of the time. Thus, we move from the rhetorical articulation of a transparent public sphere to the place the leakers reserve for themselves in it. Leakers are both maligned by governments and embraced by those celebrating transparency as the cornerstone of democracy. Each of these discourses circulates and is relevant for a fuller understanding of the

problematization of truth as disclosures in a digital world. There is, however, another way in which we should think about the people disclosing classified information: a third discourse pertaining to leakers, generated by the leakers themselves. As Foucault notes in *The Courage of Truth*, "it would be equally interesting to analyze the conditions and forms of the type of act by which the subject manifests himself when speaking the truth, by which I mean, thinks of himself and is recognized by others as speaking the truth."[338]

As threading on an intensely contentious ground, leakers take great pains in rhetorically framing their actions. In her statement released to *The Guardian* in October 2013, Chelsea Manning professes herself to be "very concerned" about a "substantial disconnect" between "what I've experienced in the last few weeks" and "what's occurred in the rest of the world." She reacts here to receiving the 2013 Sean McBride Peace Award, accepted on her behalf by retired US Army Colonel Ann Wright. Manning claims she had no knowledge of having received this award, "let alone accepted it." While she is "absolutely flattered and honored" to receive it, Manning protests being left out of the process. To make matters worse, adds Manning, "there exists the possibility that there might be more false impressions" regarding "how I feel about the award, how it ties to my actions in 2010, and who I am." She protests the sentence, spoken on her behalf, that she was purportedly "overwhelmed that such an organization would recognize [my actions] as actions for peace." "There are a few issues with this sentence," she adds. "From my perspective it's not terribly clear to me that my actions were explicitly done for 'peace...I do not consider myself a 'pacifist,' 'anti-war,' or (especially) a 'conscientious objector,'" she said, adding that "While there may be "'peaceful' or 'anti-

war' implications to my actions" this is "purely based in your subjective interpretation." Manning also believes that it is reasonable to interpret these documents as reasons for war, which is "precisely the reason why I avoided overboard and unnecessary redactions" of the documents. "I am a 'transparency advocate,"[339] proclaims Manning. In the meantime Manning remembered talking with her lawyer, David Coombs, about the award and stated, according Coombs, that she "has been feeling isolated and out of touch with the outside world during the indoctrination period at the United States Disciplinary Barracks, which is what led to her confusion over this issue."[340] This story speaks of the need to investigate how leakers see themselves and their actions, and how they rhetorically articulate their status within a world of imperial ambitions, perpetual war, surveillance, and intense media scrutiny. As it is clear here, leakers do not always see themselves portrayed accurately not even by the most favorable media coverage.

In this section I explore how the leakers articulate their rationales and motives behind the act of disclosing classified information. As Snowden eloquently states, "I grew up with the understanding that the world I lived in was one where people enjoyed a sort of freedom to communicate with each other in privacy without it being monitored, without it being measured or analyzed or sort of judged." However, "as we've seen the internet and government's relation to the internet evolve," contends Snowden, "that sort of open debate, that free market of ideas, sort of lose its domain and be shrunk"[341] The leakers situate themselves at the precipice. They emerge in the slow transition from a democratic society to an autocratic, bureaucratic and corporatist society. Against the backdrop of the dystopic present detailed in the first section, leakers link their own

actions to an effort to stave of the tyrannical tendencies discernible in the abuses of power thus buttressing the vision of a moral and transparent political universe sketched in the second section.

To speak of leakers as *parrhesiastes,* as courageous truth-tellers, a short definitional detour is in order. *Parrhesia* designates a sincere mode of addressing the public theorized and practiced in Ancient Greece. There is no shortage of definitions, from philosophy, to political theory, and to rhetoric. Foucault defines *parrhesia* as "saying everything," "speaking frankly," "stating the truth" or "frank-spokenness."[342] As Foucault indicates, the Athenian democracy was defined as a constitution (*politeia*) in which people "enjoyed demokratia, *isegoria* (the equal right of speech), *isonomia* (the equal participation of all citizens in the exercise of power), and *parrhesia*."[343] Isegoria and *parrhesia* balance each other. Robert W. Wallace calls 'frank,' and 'equal speech' (*parrhesia* and isegoria) "central qualities of democratic ideology and also of daily life in Athens."[344] In fact 'equal speech' in public assemblies "was complemented by *parrhesia*, open and candid speech in private and public life."[345] Sara Monoson defines speaking with *parrhesia* as "'saying everything' … speaking one's own mind, that is, frankly saying what one thinks, and especially uttering a deserved reproach."[346] Arlene Saxonhouse defines it as "the saying of all by the unbridled tongue," as "the democratic practice of shamelessness."[347] For Elizabeth Markovitz *parrhesia* "described the speech of a person who spoke without reservation, ornament, or regard for personal safety."[348] Ryan K. Ballot points to free speech as "commonly expressed by the word *parrhesia* which lay stress on frank and outspoken speech."[349] As "part and parcel of Socratic

dialectic," contends Marlein Van Raalte, *parrhesia* amounts to "the freedom to speak the truth, however unwelcome it may be to the audience."[350] J.J Mulhern translates *parrhesia* as "the mainly descriptive 'candor.'"[351] All these definitions communicate with each other and revolve around the same constituent terms.

The most referenced, comprehensive, and illuminating description of the subtleties and intricacies of *parrhesia*, particularly in respect to its constituent elements, comes from Foucault's discussion of the problematization of frank speech in ancient Athens. My primary interest is not in arriving at the true definition of *parrhesia*, identifying its essential characteristics, and empirically equating such a definition with the acts carried out by Manning or Snowden. For example, David R. Novak looks at Malcolm X as a *parrhesiastes*, scrutinizing his speeches for the five constitutive features of *parrhesia*. Not only is Malcom X a *parrhesiastes*, but also, concludes Novak, *parrhesia* "should be a quality emulated by current speakers and demanded by those who listen."[352] As Pat J. Gerke notes, there are many senses of the word *parrhesia*, quipping that "if I ask you 'is *parrhesia* a kind of rhetoric?' you might reply, 'do you mean fifth century Athenian civic *parrhesia*? Socratic *parrhesia*? The *parrhesia* of friendship and teaching in Philodemus? Quintilian's *parrhesia* as figure? The witness and ministry of Pauline *parrhesia*?''[353] What I am particularly focused on is, however, how *parrhesia* functions as a practice in society.

In Ancient Athens, the very word *parrhesia* was well known, used in speeches, and thus can be said to have done ideological work by buttressing a particular understanding of democracy, of the relation between citizens, deploying as a specific

practice of celebrating freedom and righting tyranny through speech. Monoson defines *parrhesia* as saying everything, speaking one's own mind, or uttering a deserved reproach. For her, *parrhesia* is associated primarily with criticism (confronting, opposing, or finding fault with another or with the popular view) and with truth-telling (speakers sincerely and strongly believe his view to be right.)[354] Monoson's intervention is useful for it sides neither with those trying to appropriate *parrhesia* for rhetoric nor with those trying to appropriate it for philosophy, but sees it as a concept and a practice part of an Athenian democratic imaginary, one that alongside other concepts did ideological work. Exploring the question of what work *parrhesia* does "in the construction of a patriotic self-image of democracy," Monoson contends that "frank speaking worked at Athens to assert the excellence of democracy in two significant ways … it forcefully articulated some of the meaning of the Athenian conception of freedom (*eleutheria*) …. it expressed an idealized version of Assembly debate."[355] She attributes the importance and visibility of *parrhesia* "in the popular Athenian understanding of freedom" to its contribution to the representation "of a sharp contrast between democratic citizenship and life under a tyranny."[356] The fear of the tyrant and of one's neighbors under tyranny fueled this understanding of *parrhesia*. Thus, contends Monoson, "The coupling of freedom and *parrhesia* in the democratic self-image therefore functioned to assert two things: the critical attitude appropriate to a democratic citizen, and the open life promised by democracy."[357] She conceptualizes Athenian democracy as "a cluster of cultural practices and normative imagery as well as a set of governing institutions" wherein "ideas of antityrantism, reciprocal exchange, responsible ruling, *frank speaking*, unity, and strong-

mindedness are central to the Athenian understanding of the demands of democratic citizenship."[358] Indeed, according to Monoson, "the Athenians considered democracy to require not only a widespread participatory ethic in the political culture and strict observance of the formal, legal privilege of all citizens to address their fellows in the Assembly (isegoria), but also the maintenance in their culture of a pervasiveness ethic of frank speaking (*parrhesia*.)" *Parrhesia* must not be confused, argues Monoson, with "mere audacious speech, with playing the devil's advocate, or even with bold speculation."[359] For Monoson Athenians thought of frank speaking as a "necessary precondition for the smooth functioning of democratic deliberative and decision-making institutions."[360] As Elizabeth Markovits also indicates, that *parrhesia* was a "powerful norm" becomes clear from its use as a trope for orators. "It was so much a part of the Athenian identity," posits Markovits, "that the speakers would invoke its meaning to signify their commitment to the public good."[361]

What guides my movement through the leakers' own words is this understanding of *parrhesia*: something like bold speech/disclosure that requires courage in the face of danger, done to support a vision of an egalitarian society that can survive only if people speak the truth to those in power. I want to sketch the contours of something like *parrhesia* operating in the discourses of the leakers acting as an explanation and justification for their acts, situating them within a democratic ethic of acting. I am not interested in analyzing Manning and Snowden's statements for traces of these constitutive elements and then proclaim them to be *parrhesiastes*. What I am more interested to see is how these speakers, like those of Ancient Athens, articulate these

features overtly, sketching in their own words, alongside the tyrannical tendencies vs. democratic transparency dichotomy, a mode of address. Although the ancient orators integrated the word and references to the practice of *parrhesia* in their own speeches, it is less likely that the modern speaker would name it as such. Nonetheless, their articulation of unadorned disclosure, a duty when confronted with the abuse of the public will, that is overtly understood to entail a risk and thus require courage to engage in, is evident in their statements. The speakers referenced here not only engage in *parrhesia*, but also activate and reference *parrhesia* as a mode of address necessary for democracy, contrasted with the lie/deception/manipulation of administrations and traditional media.

For now I use Foucault's extensive work in progress on *parrhesia* that can be credited not only with inspiring renewed attention to this concept, prompted by the publication of his last two seminars entirely devoted to it, but also with the most comprehensive attempt at charting its traces and evolution. Speaking of the characteristics of this practice, Foucault defines *parrhesia* comprehensively as a "kind of verbal activity where the speaker has a specific relation to truth through *frankness*, a certain relationship to his own life through *danger*, a certain type of relation to himself or other people through *criticism* (self-criticism or criticism of other people), and a specific relation to moral law through *freedom and duty*.[362] These characteristics—truth/frankness, danger, criticism, and duty—provide the lens through which themes rehearsed throughout Manning and Snowden's self-presentation begin to assemble into something like *parrhesia*. Evidently, to make the claim that *parrhesia* is thrown back into political and rhetorical play with the digital leaks scandals would involve an additional

analysis of the defense in media and popular culture of these acts, to see how these themes are dispersed through diverse discourses. For now, I will limit my analysis to statements and interviews with the two most prominent names in leaking scandals in the past decade. While it is difficult to separate these features, I will try to speak first of the cluster *frankness – truth – criticism*, a cluster of features that refers to what is being told, and then about the cluster *danger – risk – courage – duty* which touches on the motives and commitments of the *parrhesiastes*.

To begin with, for Foucault, frankness means saying everything one has in mind and thus "refers to type of relationship between the speaker and what he says," and what he says "is his own opinion."[363] This notion of truth as one sees it, as one possesses it, complicates my analysis and thus is in need of further elaboration. The digital disclosures of information are qualified in my argument as "speaking" the "truth." First, in a simple sense, the transfer of digital documents to media is a form of communication—"speaking." Second, the validity of the documents disclosed by Manning and Snowden has never been questioned and this, yet again in a simple empirical sense, is "truth." The documents released are digital copies of the originals, they refer to the topics they purport to refer to, and have been vetted by a number of prominent media outlets. Rather than using this empirical version of "true" to support my contention that what we see in these discourses by the leakers themselves is *parrhesia*, I would link this feature to the notion of "disclosure."

Delving into Greek once more, Foucault points out that *aletheia* (truth) is also (1) "that which, not being hidden, not concealed, is given to view in its entirety, is

completely visible, no part of it being concealed or secret," that (2) "which is not added to or supplemented … not altered by any foreign element which would thus distort it and end up concealing what it is in reality," (3) "that which is straight … direct," and, finally, (4) "that which exists and remains beyond any change, which remains in its identity, immutability, and incorruptibility."[364] In other words, "the unconcealed, the unalloyed, the straight, and the unchanging and incorruptible." For Foucault this fourfold understanding of truth can be applied not only to the logos itself but also to the ways of being, to modes of actions and conduct. So for Foucault *logos alethes* is not simply that which is true empirically, "a set of propositions which turn out to be exact and can take the value of truth," but also is "a way of speaking in which, first, nothing is concealed … second, neither the false, nor opinion, nor appearance is mixed with the true; [third], it is a straight discourse, in line with the rules and the law; and finally … a discourse which remains the same, does not change, or become debased, or distorted, and which can never be vanquished, overturned, or refuted."[365] Thus we can think of "speaking the truth as one sees it" in relation to the issues of digital disclosures as exposing government lies and deception, of bringing the truth, that which has been concealed, to light. It means to give, unadorned, the documents to the public.

This theme of unmediated access to the raw data of history is present in the Wikileaks statement, and echoed in Manning's and Snowden's different public statements. Certain details might be omitted from the documents put forth by Wikileaks, but "we," proclaims the site's authors, "do not censor our news." Indeed, Wikileaks is well known for making the original documents available, as the mission statement goes,

so “readers can verify the truth of what we have reported themselves.” This modus operandi—publishing the original unedited documents alongside the news stories—“is the way in which we show the public that our story is authentic.”[366] Unmediated access becomes a way to claim truth and authenticity (a total archive in another direction).

We see here contrasted the idea of unmediated access to raw data with traditional media that compete for information and hoard it as a commodity. As Foucault notes when speaking of frankness, the *parrhesiastes* speaks the truth “by avoiding any kind of … form which would veil what he thinks” and “the *parrhesiastes* acts on other people's minds by showing them as directly as possible what he actually believes.” [367] What is of interest is that whether we look at the ancient Greeks or to modern political discourse, a distinction between straight talk/speaking truth to power and manipulation/public relations/spin operates in public discourse to separate those who want the better for the city and its people and those with suspect intentions. In the texts analyzed here—Wikileaks, Manning, Snowden—corporate media spin seems to take the role of deception and concealment. The dichotomy between speaking the truth in the agora for the betterment of the city and speaking to deceive, between subversive and conservative discourses, remains the same.

Access to the raw data also contributes to Manning’s motives for revealing the Iraq and Afghan War Logs. In her trial statement, Manning talks about CIDNE-I and CIDNE-A SigAct tables, vast databases containing a trove of documents pertaining to significant acts in war, representing “the on-the-ground reality of both the conflicts in Iraq and Afghanistan” as “two of the most significant documents of our time.” As such,

maintains Manning, "if the general public, especially the American public, had access to the information contained within the CIDNE-I and CIDNE-A tables, this could spark a domestic debate on the role of the military and our foreign policy in general." "I also believed," claims Manning that "detailed analysis of the data over a long period of time by different sectors of society might cause society to reevaluate the need or even the desire to even engage in counterterrorism and counterinsurgency operations that ignore the complex dynamics of the people living in the affected environment every day."[368] So we have truth—via disclosure, exposure of government lies—we have frankness—through unconcealed, unmediated, unedited direct communication of government documents content—and we have criticism.

As Foucault contends, the danger "comes from the fact that the said truth is capable of hurting or angering the interlocutor."[369] The function of *parrhesia*, adds Foucault, "is not to demonstrate the truth to someone else, but has the function of criticism."[370] The *parrhesiastes* "is always less powerful than the One with whom he speaks," meaning that *parrhesia* "comes from 'below' … and is directed 'above.'"[371] In personal relations, contends Monoson, *parrhesia* meant "candid speech among friends," in theater, it referred to comedy and "specifically to hurling insults at identifiable individuals and ridiculing Athens," while in oratory "speakers also utter blunt, and at times nasty criticisms of policy and of specific people."[372] In all these contexts, points out Monoson, "*parrhesia* is consistently and closely associated with two things: criticism and truth-telling."[373] Speaking with *parrhesia* "was to confront, oppose, or find fault with another individual or a popular view in a spirit of concern for illuminating what is right

and best."[374] Thus, states Markovitz, "to have the quality of *parrhesia*, a speech must criticize someone who has the power to somehow injure the speaker" [375] For Saxonhouse, *parrhesia*, understood as free speech, "ties the word too strongly to the passive language of rights rather than the active expression of one's true beliefs."[376] Saxonhouse argues that the anachronistic language or rights conceals "the daring and courageous quality of the practice ... the exposure of one's true thoughts, the resistance to hiding what is true because of deference to a hierarchical social and political world or a concern with how one appears before the gaze of others, that is shame."[377] All of these definitions point to criticism as a defining feature. Indeed, if anything, *parrhesia* is subversive.

All these disclosures are based on a critical impetus toward what these leakers perceive as imperial and totalitarian ambitions of their society and government institutions. As we have already seen in the first section, both Manning and Snowden portray a bleak present state of affairs, a dystopian future in the making, a post 9/11 United States engaged in perpetual war and Orwellian surveillance. Manning maintains, after receiving her court sentence that the decisions she made were "out of a concern for my country and the world that we live in." She goes on to state that she began "to question the morality of what we were doing" and gradually began to understand that "in our efforts to meet this risk posed to us by the enemy, we have forgotten our humanity." She goes on to argue that "we consciously elected to devalue human life" and that "we sometimes killed innocent civilians" and that "we elected to hide behind the veil of national security and classified information in order to avoid any public

accountability."[378] This is a scathing critique of war conduct from an insider privy to a broad range of information.

Snowden, whose moniker in early exchanges with a Washington Post reporter was *Verax*—truth teller in Latin and, thus, not an inconsequential choice—gives a similarly forceful critique of foreign policy.[379] As a service member and a longtime employee of the intelligence community, Snowden speaks of propaganda and deception. Gradually, however, as exposure to true information "that had not been propagandized in the media" increased, Snowden confesses that "we were actually involved in misleading the public and misleading all publics not just the American … to create a certain mindset in the global consciousness and I was actually a victim of that."[380] This is a powerful indictment of US foreign policy, of systematic manipulation of public opinion. Snowden claims himself as a victim of the ideology of the war on terror that moves people around the way Marx imagined ideology to work. There are "good people" with "good values" that want to do "the right thing," but "the structures of power that exist are working to their own ends to extend their capability at the expense of the freedom of all publics."[381] Institutions as structures here take on a monstrous form, superseding the good of the public as well as the will of the people. So the leakers themselves conceptualize these disclosure of raw documents either directly to the public (as Manning did) or to media (as Snowden did), as telling the truth, without concealment, with frankness, a truth that is highly critical of the US policies and actions post 9/11, from the invasion of Iraq and Afghanistan, to the war time behavior toward the population of these counties, to the invention of legal categories that transform individuals into extra-legal beings that can be

tortured and imprisoned indefinitely, to the recent issues, arising under the same Patriot Act, where surveillance gains a global reach and where the digital makes it possible. The criticism of power structures implicit in *parrhesia* also indicates the civic duty to speak the truth, a duty that must be fulfilled despite the dangers associated with it. *Parrhesia* entails risk and thus requires courage.

"Wouldn't you go to prison to help end this war?"[382] On Duty, Danger, and Civic Courage

We got to get this son of a bitch. (Nixon on Ellsberg)[383]

The title—Wouldn't you go to prison to help end this war?—and the motto—We got to get this son of a bitch—stand in contrast and define the constitutive warring sides of the most invoked *parrhesia*stic scene: the Pentagon Papers. On one side, Daniel Ellsberg, called "the most dangerous man in America," ready to go to prison to defend the leak of the study detailing decades of deception in the Vietnam War, and, on the other side, President Richard Nixon, "the most powerful man in the world," one of the more notorious monikers of the US presidents, threatening to employ the might of his, in retrospect, corrupt administration to silence the publication of the study and annihilate its source through means both legal—such as stopping the publication of the papers—and illegal—such as the breaking into Ellsberg's psychiatrist's office in order to gain damning information, an act that, incidentally, scuttled the government's case against Ellsberg.

This is a relevant appeal first because, as we have seen in the Wikileaks mission statement, the Pentagon Paper disclosures and the Supreme Court case that followed in its

wake are invoked as precedent, as a success story of the democratic necessity of leaks. Not only do the present day leakers identify themselves with this moment but Daniel Ellsberg himself is very active in his defense of both Manning and Snowden. The picture, attached to the petition to free, then, Bradley Manning, depicts Ellsberg holding a hand written sign "I was Bradley Manning. Pentagon Papers 1971" sitting in front of a bookshelf where, in the background, the Pentagon Papers published in book form can be clearly seen.[384] Second, this comparison, between Ellsberg and the Pentagon Papers and the present day leaks is a contested one. Government representatives want to deny precisely the legitimacy that result from this comparison. In relation to Julian Assange and Wikileaks, then Secretary of State Hillary Clinton proclaimed that "there have been examples in history in which official conduct has been made public in the name of exposing wrongdoings or misdeeds. This is not one of those cases."[385] Similarly, when asked if Assange is closer to a hi-tech terrorist than a whistleblower sharing similarities with Daniel Ellsberg's Pentagon Papers case, U.S. Vice President Joe Biden stated, "I would argue it is closer to being a hi-tech terrorist than the Pentagon Papers."[386] Third, and most important, the contrast between the title and the motto point to the most distinctive characteristic of the *parrhesia*stic act: duty and courage when confronted with the risk of speaking truth to power.

In rapport with the dystopian vision presented in the first section, it is one's duty to disclose. As Foucault notes, *parrhesia* "is a verbal activity in which a speaker expresses his personal relationship to truth, and risks his life because he recognizes truth-telling as a duty to improve or help other people (as well as himself)."[387] Markovits

similarly sees in *parrhesia* a notion that emphasizes "not just the right to speak but also the duty to speak the truth."[388] Asked by journalist Greenwald to walk the people through the process of becoming a whistleblower, Snowden speaks of how having access to a lot of information on a broader scale exposes one in such a position to "things that may be disturbing." The frequency of being exposed to these disturbing issues leads to the recognition that "some of these things are actually abuses." Over time, adds Snowden, "that awareness of wrongdoing sort of builds up and you feel compelled to talk about" it, and "eventually you realize that these things need to be determined by the public and not by somebody who was simply hired by the government." These questions probe not only the decision to go public but also the decision to associate himself with leaks, to identify himself as the source of these disclosures. Snowden's response speaks precisely to this notion of duty emerging form the conflict between an idealized transparent/accountable society and a dystopic present. "I think that the public is owed an explanation," claims Snowden, particularly for disclosure of classified information "that are outside of the democratic model." As just "another guy" zipping through information and realizing "'this is something that's not our place to decide, the public needs to decide whether these programs and policies are right or wrong.'" The public accountability permeates the argument to disclose as well as to reveal himself. "I'm willing to go on the record" states Snowden "to defend the authenticity of them and say, 'I didn't change these, I didn't modify the story. This is the truth; this is what's happening. You should decide whether we need to be doing this.'"[389] This deference to the public interest permeates most of Snowden's statements.

Snowden's entire history, in his own re-telling, is one of service and dedication to the country: "I joined the intelligence community when I was very young," he says. Enlisting in the Army after the invasion of Iraq, Snowden confesses that he "believed in the goodness of what we were doing" and "in the nobility of our intentions to free oppressed people overseas." America, proclaims Snowden, "is fundamentally a good country."[390] Patriotism, understood as oath to one's country—which Snowden broke—is reframed as doing the right thing when confronted with abuse, with deception, and with propaganda. "The oath of allegiance is not an oath of secrecy," maintains Snowden, but to the Constitution. "That is the oath," he continues, "that I kept that Keith Alexander and James Clapper did not," referencing the now infamous incident where high ranking government officials lied about the extent of the surveillance of American people to Congress.[391] "I am not trying to bring down the NSA," adds Snowden, "I am working to improve the NSA." "I am still working for the NSA" Snowden quips, but "they are the only ones who don't realize it." Pressed on the issue of the location of his exile—China and then Russia—Snowden affirms "If I defected at all … I defected from the government to the public."[392] Democracy is at stake. The US government is set in stark opposition to the public. Regardless of oaths then, the duty is to the good of the "city."

Duty, ultimately, is a refusal to be party to the abuses perpetrated by the government. To the question, what about this dismal present, this "set of developments" you have witnessed "that makes them sufficiently menacing or threatening to you that you are willing to risk what you've risked in order to fight them," Snowden replies, "I don't want to live in a world where everything that I say, everything I do, everyone I talk

to, every expression of creativity or love or friendship is recorded."[393] This morally corrupt bureaucracy, going global, overreaching and overstepping its boundaries is "not something I'm willing to support, it's not something I'm willing to build, and it's not something I'm willing to live under," adds Snowden.[394] This refusal to endorse, support or keep quiet about the abuses he witnessed compel him to talk, lest he be complicit in them. "I think anyone who opposes that sort of world has an obligation to act in the way they can," he says.[395] This is particularly true, maintains Snowden, given the failure of the system and of its leadership. "I've watched and waited … and tried to do my job in the most policy-driven way … and allow our leadership, our figures, to sort of correct the excesses of government," he says. [396] However, the failure of the democratic process to account for, expose, and change these process is becoming evident through these revelations. Indeed, "we're compounding the excesses of prior governments … making it worse and more invasive, and no one is really standing to stop it."[397] Silence becomes complicity. Thus the duty to speak out against these excesses and abuses of power, to speak outside the official channels that have failed consistently, becomes the only way to intervene and slow the gradual erosion of democratic checks and balances.

The mendacity witness in the country's representatives leads Snowden to the inevitability of disclosure. Asked in an interview with German television NDR on January 26, 2014, about the decisive moment for becoming whistleblower, Snowden specifically identifies James Clapper's infamous lie to Congress. "There's no saving an intelligence community that believes it can lie to the public and the legislators who need to be able to trust it and regulate its actions," adds Snowden.[398] "Even the wider body of

our elected representatives were prohibited from knowing or discussing these programs," adds Snowden, all the while there is "the creeping realization that no one else was going to do this."[399] Thus, the failure of the system and its clear inability to correct itself, exposed by Clapper's lie, reinforced by congressional cluelessness or inaction, constitute powerful motivators. "Dianne Feinstein elected me when she asked softball questions," emphasized Snowden; "Mike Rogers elected me when he kept these programs hidden. . . . The FISA court elected me when they decided to legislate from the bench." Indeed, Snowden claims, the system "failed comprehensively" while in terms of oversight "each level of responsibility that should have addressed this, abdicated their responsibility."[400] The government's incompetence, inability or unwillingness to deal with these issues provides the catalyst for his action. The parrhesiastic duty is born out of the need to speak a harsh truth that nobody else seem to be willing to utter.

The *parrhesiastes* articulate their actions as a duty to the people. The public, posits Snowden, "had a right to know about these programs … to know that which the government is doing in its name, and that which the government is doing against the public."[401] Reinforcing this dichotomy between general public and the government, the public good and institutions (private or governmental) overstepping their authority, allows Snowden to side with the public, against the government, and thus rearticulate the notion of duty, the oath to the Constitution, as a bond with the people and not a formal pact with the government. As Saxonhouse notes "freedom of speech is enshrined not for the benefit or freedom of the individual; it exists in the vision of these orators for the sake of the city. The one whose actions and character demonstrate a supposed incapacity to

add to the welfare of the common (ta koina) can make no claim to the practice of *parrhesia*."[402] "It's a continuation of trying to do everything I could to prosecute the public good in the most effective way," states Snowden when asked why he joined the CIA, "and it's in line with the rest of my government service."[403] Snowden reinserts his professional trajectory into the larger arc of doing his duty to the American people. Indeed, adds Snowden,

> no matter how deeply an individual is embedded in the government, no matter how faithful to the government they are, no matter how strongly they believe in the causes of their government as I did during the Iraq war, people can learn, people can discover the line between appropriate government behavior and actual wrongdoing and I think it became clear to me that that line had been crossed.[404]

The government is set not just opposite to the people but actively against the people. Snowden rhetorically delinks patriotism and duty from the formal oaths and attaches it to the higher calling of serving the people. This moves allows Snowden to keep the spirit of all the while breaking the letter of his oaths. In this way, moral authority is preserved.

Consequently, serving the people can be reinterpreted in a broader sense to include the act of subverting the government via disclosures of classified documents. For Snowden, to speak of the duty to intervene in this widening split between people and their government, "you have to try something rather than do nothing."[405] As Foucault contends, "when you accept the *parrhesiastic* game in which your own life is exposed, you are taking up a specific relationship to yourself: you risk death to tell the truth instead of reposing in the security of a life where the truth goes unspoken."[406] Snowden indeed lays out this precise dichotomy between a comfortable life in silence and the duty to

speak the truth. “You have to make a determination about what it is that's important to you” contends Snowden and

> if living unfreely but comfortably is something you're willing to accept, and I think it many of us are it's the human nature; you can get up every day, you can go to work, you can collect your large paycheck for relatively little work against the public interest, and go to sleep at night after watching your shows. But if you realize that that's the world you helped create and it's gonna get worse with the next generation and the next generation who extend the capabilities of this sort of architecture of oppression, you realize that you might be willing to accept *any risk* and it doesn't matter what the outcome is so long as the public gets to make their own decisions about how that's applied.[407]

For Snowden inaction is not possible in the face of abuse; this line of reasoning buttresses the very notion of duty, doing what must be done for the betterment of the city, despite great danger. Snowden indeed believes that the cost of “frank public debate about the powers of our government is less than the danger posed by allowing these powers to continue growing in secret.”[408] This “direct threat to democratic governance”[409] speaks to the tension permeating post 9/11 discussions pitting national security against human rights. “We have a moral duty to ensure our law and values constrain surveillance programs and protect basic human rights,” argues Snowden.[410] Indeed, as Foucault notes, the *parrhesiastes* “prefers himself as a truth-teller rather than as a living being who is false to himself.”[411] This is the relationship to himself the Snowden sets up through this dichotomy between a life of complicit silence and the perilous life of a truth teller bound by duty.

Speaking to his larger duty of serving the public good, Snowden proclaimed that his mission was already accomplished. "For me, in terms of personal satisfaction, the mission's already accomplished …I already won," claims Snowden, adding, "all I wanted was for the public to be able to have a say in how they are governed."[412] Thus, echoing Habermas once more, transparency leads to the possibility of a public dialogue on matters of common concern. Snowden's contribution, as he sees it, is that of making things public and starting this conversation. He appeals directly to the notion of the marketplace of ideas. The decision to disclose, when weighed against the alterative of not acting, leads to the realization that "some analysis is better than no analysis."[413] Thus "even if your analysis proves to be wrong, the marketplace of ideas will bear that out."[414] As a side commentary on his exile, Snowden feeds off of the debate itself. "It's becoming increasingly clear that these leaks didn't cause harm in fact they served the public good," claims Snowden.[415] Consequently, he hypothesizes, it would be "very difficult to maintain sort of an ongoing campaign of persecution against someone who the public agrees serves the public interest."[416] Snowden thus situates his action, within this antagonism between government and the people, on the side of the public, linking his actions to ideological concepts with powerful democratic resonance such as the marketplace of ideas, public debate, or transparency, etc.

This sense of duty, of doing the right thing, emerges from Manning's statements as well. Manning speaks of a sense of relief after releasing the Iraq and Afghanistan war logs, having felt he "had accomplished something" that allowed him to have "a clear conscience based upon what I had seen and read about and knew were happening in both

Iraq and Afghanistan every day."[417] For Manning the duty to report the abuses witnessed follows a more personal approach. If, for Snowden, the good of the public is always overtly articulated as a reason or framework for his actions, Manning frames her justification in terms of a deep commitment to justice. Speaking at her trial about the diplomatic cables she released, she brings up the issue of Iceland. What Manning saw reading "Reykjavik 13" cable (the only cable cited by name in her charges) was Iceland "essentially being bullied diplomatically by two larger European powers," and that "despite the quiet request for assistance, it did not appear that we were going to do anything."[418] The sense of wrong and the deliberate inaction on the part of the United States, leads to the decision to leak the respective diplomatic cables. "I felt that I would be able to right a wrong by having them publish this document," states Manning.[419] Manning articulates this incident as an offense to a sense of justice that provide the impetus for action.

A similar narrative of witnessing injustice and abuses unfolds in the characterization of the leak of the infamous video of the Apache helicopter, dubbed "Collateral Murder." Manning uses charged expressions such as "war porn" to describe in detail the insensitive behavior of the helicopter crew. "The most alarming aspect of the video to me," notes Manning, was "the seemly delightful bloodlust they appeared to have."[420] The lack of concern for human life, evidenced by the callous comments of the crew, by their lack of remorse, by their heartless comments when children are discovered at the scene, by their lack of accountability evidenced by blaming the unarmed civilian that stopped to help for "bringing their kids into a battle," all the way to verbalizing

"enjoyment at the sight of one of the ground vehicles driving over a body," paint a gruesome picture of a military culture rife with abuse and driven by callousness.[421] Burdened emotionally, in her own words, Manning released the video hoping "that the public would be as alarmed as me about the conduct of the aerial weapons team crew members."[422] Manning wants to expose the routine inhumanity of the battlefield. He uses pictorial images to detail what he characterizes as "war porn," because at least some of what the actions he attributes to soldiers seem to serve no strategic purpose but are done because they can be done; that they are shocking is their justification. Manning does presents himself as an ordinary person, an innocent, horrified by the casual cruelties of battle. Like Snowden, Manning also is encouraged by "the response in the media and general public." "As I hoped," she says, "others were just as troubled—if not more troubled than me by what they saw." [423] A sense of public vindication further legitimizes, in their own narratives, their original impetus for disclosure.

It is not simply a matter of witnessing and remaining silent, it is also a matter of complicity. Detailing another case from her experience as an information analyst, Manning speaks of situations where the abuses are evident, where the US military is purposefully used for eliminating political opponents of puppet governments. She states, "I knew that if I continued to assist the Baghdad Federal Police in identifying the political opponents of Prime Minister al-Maliki, those people would be arrested and in the custody of the Special Unit of the Baghdad Federal Police and very likely tortured and not seen again for a very long time—if ever."[424] Thus, instead of being complicit, "instead of assisting the Special Unit of the Baghdad Federal Police," Manning states, "I decided to

take the information and expose it to the WLO, in the hope that before the upcoming 7 March 2010 election, they could generate some immediate press on the issue and prevent this unit of the Federal Police from continuing to crack down on political opponents of al-Maliki."[425] Yet again, the details of abuse lead to a troubling feeling, which triggers a sense of justice, and subsequently results in the leak of the documents. What is of interest to me is the rhetorical construction of this chain that connects a sense of justice with the duty to the public. In other words, reading about these scenes of injustice leads Manning to disclose information, the only option available, in order to address the situation. Rhetorically, Manning paints horrendous scenes of abuse and torture followed by a justified moral evaluation that triggers the only option that someone with such little power can do, meaning disclosure.

Manning's position in this argument is somewhat complicated by her apologies at sentencing. While she maintains that at the time she believed she was "going to help people, not hurt people," she apologized that her actions did hurt people and the United States and that she "did not fully appreciate the broader effects of my actions."[426] In retrospect, Manning wonders, "how on earth could I, a junior analyst, possibly believe I could change the world for the better over the decisions of those with the proper authority?"[427] Many of Manning's mistakes were purposefully corrected by Snowden– more selective and damning disclosures (as opposed to vast raw data leaks); avoiding capture; the use of traditional media outlets that would avoid the debate on Wikileaks' status as a media entity. Thus, returning to Manning's statement that opened this inquiry, protesting not knowing about the peace award, and resisting labels such as "pacifist,"

"anti-war," "conscientious objector," Manning proudly proclaims herself a "transparency advocate" who feels that "the public cannot decide what actions and policies are or are not justified if they don't even know the most rudimentary details about them and their effects."[428] Manning's statements display as well the relationship between witnessing abuses, disclosing that information, and a democratic deference to the public good. The sentence that prompted the apology—30 years in prison—as well as the repeated request for Snowden's deportation, speak of the last *parrhesia*stic feature of note: the danger one faces when speaking a critical truth to those in power.

As Foucault notes, however, there are many and diverse modalities of telling the truth. Speaking specifically about ancient Greek culture, he points to prophecy, wisdom, and teaching as, alongside *parrhesia*, modes of veridiction. One of the distinguishing features—apart from each of these modalities involving different characters (the prophet, the sage, the teacher, the *parrhesiastes*), involve different modes of speech, and relate to different domains (fate, being, *tekhne*, and ethos)—is danger. "Clearly," quips Foucault, "this teacher, this man of *tekhne*, of expertise and teaching, does not take any risk in the truth- telling."[429] For Foucault then "someone is said to use *parrhesia* and merits consideration as a *parrhesiastes* only if there is a risk or danger for him in telling the truth."[430] Thus, the proof of one's sincerity, contends Foucault, is courage. "The fact that a speaker says something dangerous—different from what the majority believes—is a strong indication that he is *parrhesiastes*," argues Foucault.[431]

"There is always *parrhesia*" contends Foucault when the fact of telling the truth "will, may, or must entail costly consequences for those who have told it."[432] The danger

of telling the truth entails a series of pacts. For Foucault, the act of stating the truth implies a *parrhesia*stic pact "of the subject with himself" in which the speaker binds him or herself to the content of the statement and to the act of making that statement.[433] When one states the truth one states what one knows and believes to be true; at the same time, one binds oneself to the act of stating the truth given that stating the truth entails a certain risk. To put it differently, "the *parrhesiastes* is someone who emphasizes his own freedom as an individual speaking." [434] For Foucault *parrhesia* brings to the forefront a fundamental philosophical question: the connection between freedom and truth. "How and to what extent is the obligation of truth— the "binding oneself to the truth," "binding oneself by the truth and by truth-telling"—at the same time the exercise of freedom, and the dangerous exercise of freedom?"[435] *Parrhesia* thus is a way of telling the truth, a way entailing a risk, binding the speaker to the statement of truth and to the act of stating it in the form of a courageous act.[436] Thus we get from "frank-spokenness" to veridicity, to a modality of truth telling that speaks of power relations as much as it does of the constitution of the subject through the act of speaking the truth.

Similarly, Monoson points to the difference between *parrhesia* and our modern understanding of free speech. She notes that "the celebration of *parrhesia* in democratic politics did not carry any demand for a notion of protected speech" and as a matter of fact, speaking with *parrhesia* "retained a strong association with risk."[437] These risks associated with speaking in public with *parrhesia* "were not thought by the Athenians to undermine or even conflict with the practice of frank speech;" rather, argues Monoson, they "affirmed that the speaker could be held accountable for the advice ventured."[438]

The citizen of democratic Athens, "presupposed by the ethic of *parrhesia* is daring and responsible, self-confident and eager to enter the fray," argues Monoson, "the very antithesis of the slavish subject of a tyranny."[439] "To have the quality of *parrhesia*" notes Markovits as well, "speech must criticize someone who has the power to somehow injure the speaker."[440] Markovits speak of *parrhesia* as the speech of a person "who spoke without reservation, ornament, or regard for personal safety."[441] "In ideological representation," argues Ryan K. Balot, free speech "had substantial benefits to offer the citizenry, but in practice it entailed grave risks for the speaker."[442]

Based on Snowden's leaks, we know that Wikileaks has not receded in the background. One document revealed that there is a concerted campaign of disrupting Wikileaks operation, apart from the US-led banking blockade, in which "by exploiting its ability to tap into the fiber-optic cables that make up the backbone of the Internet, the agency [GCHQ – British intelligence Agency] … was able to collect the IP addresses of visitors in real time, as well as the search terms that visitors used to reach the site from search engines like Google.[443] Other documents reveal the Obama administration pressuring allies to file criminal charges against Assange. In her request for a pardon Manning speaks of disclosing the information "out of a love for my country and a sense of duty to others." "If you deny my request for a pardon," she adds, "I will serve my time knowing that sometimes you have to pay a heavy price to live in a free society." "I will gladly pay that price," Manning insists, "if it means we could have country that is truly conceived in liberty and dedicated to the proposition that all women and men are created equal."[444]

The conflict between benefits and danger resulted, according to Balot, in orators developing "a discourse on civic courage—a virtue that, they claimed, enabled them to steer an honorable course in public life."[445] Indeed, contends Balot, "orators themselves foregrounded the dangers of free speech and argued that they deserved credit for their courage in running risks for the sake of Athens' welfare"[446] and that "their courage made a unique contribution to democratic deliberation."[447] In other words, the risks to speaking were not in the background but a topic of speech. However, self-asserting one's courage was "a delicate matter" which is why, as Balot points out, "it had to be embedded in the framework of patriotically doing one's duty and counseling the city to do what is best for it." [448] "Athenian orators argued that their willingness to run the risks in order to speak freely indicated their sincerity and patriotism," Balot notes. [449]

Snowden, already privy to what happened to Manning, spoke at length and with awareness of the dangers he was exposing himself to even before the leaks. "I understand that I will be made to suffer for my actions, and that the return of this information to the public marks my end," claims Snowden.[450] As a connoisseur, Snowden claims that the US intelligence community "will most certainly kill you if they think you are the single point of failure that could stop this disclosure and make them the sole owner of this information."[451] In the same interview with the Washington Post, Snowden adds "You can't protect the source … but if you help me make the truth known, I will consider it a fair trade."[452] Both the danger to which one exposes oneself as well as the courage necessary to go through with the act are articulated here. The gravity of the criticism that needs to be brought to light makes the act of disclosure an act of civic duty and, in that

sense, inevitable. “There’s no saving me,” Snowden is quoted as saying. He considers that “the greatest danger to our freedom and way of life comes from the reasonable fear of omniscient State powers kept in check by nothing more than policy documents,” adding that the expansion of the surveillance state is “such a direct threat to democratic governance that I have risked my life and family for it.” [453] We see In Snowden’s various statements a clear articulation of the dangers of disclosing information, the awareness of the risk entailed, as well as the articulation of the duty to speak despite these dangers. “Good evening, London. Allow me first to apologize for this interruption”[454]

The title references V’s speech given while pirating the emergency channel in James McTeigue’s 2006 movie *V for Vendetta*, made (in)famous, in part, by the cooptation of the main character’s Guy Fawkes mask by the hacktivist group Anonymous and Occupy Wall Street movement. The speech is an interruption in more than one sense; besides disrupting the normal TV program, the speech disrupts the fantasy of a harmonious society; truth crashing in and shattering the brittle ideological construction nobody takes seriously while nobody challenges. Lest we forget, the fact that the emperor is naked is not really news. The ideological edifice is sustained by silence and obedience. As Slavoj Zizek said to Julian Assange in a conversation mediated by Amy Goodman, “you are not just violating the rules. You are changing the very rules how we were allowed to violate the rules. This is maybe the most important thing you can do.”[455]This is precisely the function leakers reserve for themselves. Interrupting and disrupting the normal flow in order to tell a truth that needs to be spoken and heard being spoken out loud.

Leakers rhetorically situate themselves in the gap between the advent of an Orwellian government, of an unopposed and ever expanding empire, relying on economic, military and technological might, and the vision of a transparent society built around the public good, reliant on informed citizenry. The act of disclosing classified information, an act of espionage as government institutions see it, becomes a "principled leak," an act enacted out of democratic principle, an act of civic courage, a fulfillment of a public duty, made all the more relevant as it entails grave risks to one's being and standing in the world. The concept of *parrhesia*, as courageous truth telling, allows us to focus the discussion of Wikileaks, Chelsea Manning, and Edward Snowden around a practice that places in political and rhetorical play one's relation to oneself and others. Within preexisting relations of power, confronted with abuse, we see once more debated in public the need to risk one's life to subvert the tyrannical tendencies of governments and institutions.

My argument however is not simply one of equivalences between a specific definition of *parrhesia* and a concrete occurrence. The argument that the practice of disclosure of classified information with great risk to one's freedom perpetrated for the benefit of the people can be made successfully in this case. I can add my voice and call digital disclosure modern manifestations of *parrhesia*. What I am interested in, via authors that speak of *parrhesia* as a democratic practice not only in the sense of being practiced but also in the sense of being problematized, in Foucault' sense, as in becoming object of thought, of reflection, of use, abuse, and denunciation. As I have noted, the modern practice of speaking most akin to *parrhesia*, what we would dub "speaking truth

to power" is also contrasted with another way of communication – media spin, manipulation. This distinction operates and serves the function of distinguishing those who support the status quo, and those who want to subvert its perceived tyrannical tendencies. Wikileaks/Manning/Snowden – speak in different terms of the same dichotomy that still survives between deception, artifice, official communication intended to calm and subdue, and something else, unmediated access to truth guaranteed by the risk that conveying such truth entails. This dichotomy operates to discriminate between modes of address and thus modes of relating to power structures.

Ultimately, I treat *parrhesia* as ideological topoi. The digital disclosure functions in a similar way to *parrhesia* in Ancient Greece: it is predicated upon exposing corruption and lies, keeping the democratic government accountable; it has the same formal characteristics, meaning it is grounded in duty, it exposes one to danger and thus requires courage, and it is done in the interest of the people with an eye toward maintaining democracy. As such it functions as a counterbalance to the official communique, to media spin, to press releases and 24 hour news cycles in discourse advocating democracy as reliant on freedom of speech and transparency, the Habermasian twin conditions for a functioning public sphere.

Chapter V

A Rhetorical Hermeneutics of Danger

While the damaging aspect of unauthorized disclosures is in debate—whether it weakens the security of the state or contributes to the health of the republic—their frequency and impact are certainly not. From December 2006, when the Wikileaks published its first document, to January 2015, when, yet again, the "analysis of documents released by whistleblower Edward Snowden reveals"[456] something or other, leaks have become an uneasy yet common fact of life. Apart from their commonality, the sheer magnitude of these disclosures in the past 10 years, both in terms of their number as well as in terms of the quantity of documents released, makes this an irruption of (secret) discourses that cannot be ignored.

Their commonality and their magnitude can be traced back to the unavoidable, ubiquitous, and versatile nature of the digital environment. While disclosures of state secrets are not new, there is nonetheless something quantitatively and qualitatively different. More material can be obtained and released faster, reaching a global audience with incredible speed. In other words, instant access to secret information as well as immediate impact on politics. "The most powerful institutions," comments Assange,

"from the CIA to News Corporation, are all organized … using computer programmers, using system administrators, using technical young people." "What does that mean," asks Assange, "when all those technical young people adopt a certain value system, and that they are in an institution where they do not agree with the value system, and yet actually their hands are on the machinery?"[457] Mario Savios' famous call, during the 60's, about the "operation of the machine" where one's body, thrown upon the gears, wheels and levers, must prevent its odious functioning, seemed mirrored here for the digital age. This time it is not so much about stopping the machinery as much as it is about the downloading and posting its secret operations online. Beyond this (digitally) revolutionary call, Assange's comment speaks most of all about the permeability of these digital borders that make us susceptible to global surveillance all the while making governments and corporations vulnerable to increased and unwitting "transparency."

The commonality and magnitude of these disclosures as well as the permeability of digital borders ripple, as we have seen, through state institutions, juridical procedures, and mediascapes, and, as such, require our devoted attention. As such, my objective in this project was to interrogate the discourses, practices, and policies animated by the series of scandals and revelations of the last five years, engendered by the high profile leaks of classified documents perpetrated by Chelsea Manning and Edward Snowden. I wanted to question more generally the milieu in which these discourses circulate, and the themes they activate, and the apparatuses they create. From there, the project spiraled out, first by tracing the way governmental institutions devised solutions to the problem of leaks, and second, by charting the discourses produced by the leakers themselves.

The debates surrounding these leaks rehearse themes of transparency and government accountability as well as themes linking national security to secrecy and unauthorized exposure of information to harm to national security. As a result, I began to trace in Chapter Two, though several strands of U.S. jurisprudence and legal practice, how the objects of discourse are prohibited or, in other words, what according to law can be known by the public, under what conditions that access can take place, and through which kinds of procedures. I also explored the related theme of the subject's relation to these leaks, particularly in regard to the question of who can have access to this information and the consequences of divulging it. Specifically, I mapped these questions of access to information onto the enactment and successive transformations of several strands of legislation including The Freedom of Information Act, The Whistleblower Protection Act, the *Espionage Act*, and the Presidential Executive Orders on national security.

Foucault's *Discourse on Language* provided the critical vocabulary to speak of the will to truth, of direct prohibitions, of ritual and fellowships of discourse as rarefaction strategies, as strategies of regulating discursive flow, of dealing with dangerous discourse of and about government or, as Foucault would put it, "to avert its powers and its dangers, to cope with chance events, to evade its ponderous, awesome materiality."[458] What I found as animating these different strands of legislation, from FOIA to the *Espionage Act*, were a "will to truth in politics" and "national security" as two distinct yet interrelated logics of organizing truth of and about government. I defined the will to truth in politics as a logic that loosely organizes and links together legislation,

arguments, and political demands that codify access to information—meaning government transparency—as an essential element of a real democracy. As such, I read the Freedom of Information Act and its metamorphoses as a veritable manifestation of this will to truth in politics, a never ending political project caught in a dialectical relationship with national security. Similarly, I defined national security, the counterpart of this will to truth in politics, as a logic that codifies secrecy as the essential ingredient in good governance and disclosure as the quintessential threat to the security of the people. As such, I read through the successive Executive Orders the attempt to balance the public's interest in accessing information about the government with the expanding desire to protect information deemed potentially damaging to national security.

Undergirding both these logics is the notion of *discourse of and about government* as dangerous. As a result, its release must be timed, its objects clearly defined, and its speaking subjects identified. Thus, on one hand, we have legislative efforts that link good governance to transparency, such as the *Freedom of Information Act* and the *Whistleblower Protection Act*, and, on the other hand, executive orders and prosecutions, such as the *Espionage Act* and Presidential Executive Orders, that link secrecy to national security. Despite their differences, what these two strands of legislative endeavors end up producing is what I've been calling a "multilayered architecture of access" by which the discursive field of and about government is controlled through divisions between *licit and illicit objects of discourse* (information that can be known always accompanied by evolving series of exceptions), *licit and illicit circuits of discursive flow* (procedures of request, systems of fees, litigation processes), and *authorized and unauthorized subjects*

(authorities of classification and declassification). *Chronos* and *Kairos,* as conceptualization of time in relation to rhetoric, afforded the opportunity to set the delayed release of classified information, defined by chronos as a set opportune time, against the kairotic eruption of unauthorized leaks. As illustrated in my analysis, the timelines associated with the disclosures of classified information in the successive Executive Orders prescribed the opportune moment of disclosures somewhere between 20 years and never. Against these prescriptions, the unauthorized disclosures create their own opportunity thus increasing their political valence.

In regard to the subject's relation to these systems, I looked at the whistleblower and the spy. The first was conceptualized as the subject personifying the *will to truth in politics,* the subject authorized to break the rules, to speak before the proper time for disclosure has elapsed, and yet, a protected subject. The second, the spy or the insider threat, was conceptualized as the corresponding speaking subject of *national security*, the subject who speaks out of turn as well but a subject who becomes hunted, an enemy subject. Both these subjectivities are evidently legal fictions that one inhabits, fictions bringing with them a series of material protections and/or dire consequences. The prosecution of Chelsea Manning and the hunt for Edward Snowden illustrate the contentious nature of these legal fictions and the inherent difficulty of inhabiting the subjectivity of the whistleblower.

It is precisely these two subjectivities at odds, interrelated in the contentious space of unauthorized leaks that I explored in greater detail in the following chapters. In Chapter Three, my subsequent goal was to focus on the subject that speaks out of turn by

charting the emergence of the "insider threat" as a prominent figure inhabiting the institutional landscape in the wake of the unauthorized disclosure scandals of the past 10 years. I wanted to see how prominent state institutions conceptualize the process by which a person decides to disclose classified information to the public. Foucault's *Discipline and Punish* was a particularly useful tool in unpacking the institutional discourses that set up systems of early detection and prevention. Foucault notes a shift from punishing the crime to knowing the criminal before the crime, thus opening up spaces for intervention. The operation of knowledge/power thus extracts a propensity from criminals and make that its object of analysis and intervention on the population. This reversal is what Tell calls metonymical, linking Nietzsche's critique of knowledge and Foucault's critique of power through tropology. Similarly, my attention was focused on tracing the emergence of the leaker as insider threat who must be studied, known, put under surveillance, and ultimately neutralized before the crime of disclosing information has been committed.

The result of this analysis was the sketch of what I called "the digital delinquent." The delinquent is not a criminal as much as it is an individual with criminal propensities and, thus, a prime object of knowledge and a new surface of power intervention, cure, and prevention. The result of this reversal, in which crime no longer defines the criminal, is what I've been calling an "insider threat apparatus." This apparatus then is tasked with defining and finding something else to place at the origin of the crime, something ineffable, something spread across thoughts, actions, personality traits, and biographical details. The result is a vast machinery of surveillance of both on and offline behaviors, a

repository of a growing archive about government employees, an expanding domain of knowledge trying to link behavioral science to detecting and intervening in the lives of those deemed insider threats before that threat materializes. To sum up, as digital leaks become a problem for government institutions, the state builds an insider threat apparatus whose functioning obeys a metonymical logic, by which I mean a reversal that substitutes the crime as the defining action of the criminal with psychological traits, observable behaviors, and work-related conduct. This knowledge domain buttresses a developing apparatus of surveillance, detection and deterrence that classifies these "observables" as indicators for higher insider threat risk leading to a vague notion of dangerousness opening state institutions and publics to fields of knowledge and spaces of surveillance and application of power as illustrated in my analysis of various publically available documents, such as *National Insider Threat Policy*, *The Psychology of the Insider Spy*, or *Identifying at-Risk Employees: A Behavioral Model for Predicting Potential Insider Threats*, from state instructions ranging from the Department of Defense and the Office of the President to the Federal Bureau of Investigation and the Department of Energy.

If, in Chapter Three, the institutional discourse defines the insider threat, in Chapter Four, the leakers themselves speak of their own subjectivity in relation to truth and governance. My goal here was to interrogate the discourses of those who disclose information as a way to sketch the emergence of the whistleblower as the democratic subject speaking the truth. The concept of *parrhesia*, as the courage to speak the truth, provided the theoretical and methodological guide through speeches and statements from Wikileaks, Manning, and Snowden. The results of my analysis revealed a complex

rhetorical construction of the leaker's role juxtaposing an Orwellian world, revealed by these leaks, with the vision of a transparent polity, akin to Habermas' ideal public sphere. Within the gap between these two worlds, the leakers tend to define themselves as something like the *parrhesiastes* of Ancient Greece. Indeed, through their own statements, we see thrown back into political and rhetorical play the ancient concept of *parrhesia* as the courage to speak the truth in the marketplace. Following Foucault's description of the constitutive elements of *parrhesia,* I analyzed how leakers articulate their actions to a necessary truth, to a duty when confronted with government abuse of the public will, and with risk and courage. No better illustration for this discursive articulation exists than Snowden's own choice of Verax—Latin for truth-teller—as the moniker used to protect his identity in his early exchanges with the Washington Post reporter. Like the ancient Greek *parrhesiastes,* leakers juxtapose their action with another type of discourse that conceals, that buttresses an increasingly undemocratic system. The vision of a transparent society built around the public good, reliant on informed citizenry is torn between something akin to state silence and "principled leaks" as acts of civic courage enacted out of democratic duty.

What links all these investigations together, apart from their common theme of unauthorized disclosure, is sketching the contours of a rhetorical hermeneutics[459] of dangerousness. A Foucauldian rhetoric is less of a rhetorical hermeneutics to uncover the power of discourse as it is a way to investigate how a rhetorical hermeneutics is put into operation by an apparatus to uncover problems and threats. This argument falls under the label "materialist rhetoric" by focusing, as Greene argues, "on how rhetorical practices

create the conditions of possibility for a governing apparatus to judge and program reality."[460] In this study, a rhetorical hermeneutics of danger is constructed and deployed to isolate the problem of leaks. In other words, Foucauldian rhetoric charts how acts of interpretation become weaponized, how reading an assemblage of histories, anamneses, and biographies is deployed as a way to define, isolate, and intervene in the unauthorized disclosures of classified information.

Rhetorically, *parrhesia* is juxtaposed as a challenge to this logic of dangerousness. Indeed Snowden himself overtly criticizes this rhetorical hermeneutics of danger by noting that the global surveillance apparatus accumulating data can make it possible to paint anyone as a wrongdoer.[461] However, as I have shown, "will to truth in politics," of which *parrhesia* would be a manifestation of, and "national security" are intertwined. "The rhetoric of *parrhesia*" thus is the dialectical other of "rhetorical hermeneutics of dangerousness." Mirroring Green, who notes that "rhetorical practices function as a technology of deliberation by distributing discourses, institutions, and populations onto a field of action," I argue that "the rhetorical hermeneutics of dangerousness" and "the rhetoric of *parrhesia*" are deployed as technologies of interpretation that distribute discourses, institutions, and populations onto a political field of action structured by access to information.

One of the main contributions of my project to rhetorical studies is to define and perform a critical sensitivity that joins rhetoric's objects and concerns with Michel Foucault's critical insights through an argument about the unauthorized disclosures of classified documents. As such my study is both situated in and tries to advance the 30

year old tradition of scholarship from Dilip Gaonkar's first attempts to transpose Foucault methods into rhetoric and argumentation, while warning of rhetoric's temptations exposed by this encounter in 1982[462] to, more recently, Pat Gehrke, Susan Jarratt, Bradford Vivian, and Arthur Walzer's forum debating the relationship between rhetoric and *parrhesia*[463] or Susan Jarratt's exploration of the shifts in Foucault's historiographical stance[464] focused on Foucault's last seminars in 2014, and, in between, among the most notable contributions, Carole Blair and Martha Cooper's exploration of the humanist turn in Foucault,[465] Raymie Mckerrow seminal essay on critical rhetoric,[466] Barbara Biesecker's famous theoretical musings in "Michel Foucault and the Question of Rhetoric*,"*[467] and Ronald Greene's exposition on the modernization of pastoral power.[468]

As a result of my survey of this vast body of scholarship, I have arrived at a set of principles that define this critical sensitivity. As detailed in the introductory chapter, Foucauldian Rhetoric (1) is archival, and thus spans great vistas of discourse, (2) its own conceptual logic is that of bricolage (the toolbox approach), (3) it is posthumanist, (4) it is articulatory, as in takes articulation as its logic, as its organizing principle linking the elements of the rhetorical situation, and (5) it is sensitive to the subtle relations between subjectivities, powers, and knowledge. The objective of this introductory chapter as well as the space allotted to this section precluded a more in-depth survey of this vast body of scholarship that would have allowed a more robust grounding of this theoretical and methodological sensitivity. There is both need and room to write a comprehensive history of the theoretical encounter between rhetorical studies and Michel Foucault. Such history would allow Foucauldian rhetoric to anchor itself both in our attempt to metabolize the

theoretical and methodological problems arising from this encounter as well as in our actual critical practice. Better answers to the questions, "How do we *understand* Foucault and Rhetorical Studies?" and "How do we *use* Foucault in rhetorical criticism?" would certainly deliver a more detailed sketch of this critical sensitivity, beyond the five points I have focused on.

In terms of the object of study, it is important not only to understand the public arguments for and against unauthorized disclosures but to inscribe those arguments in the larger discursive movements. By defining the different discursive logics—*will to truth in politics* and *national security*—that vie for control, we are able to chart how these logics cut across legislation, practices and public arguments. This genealogy of our current debates shows a much longer history, evident in 100 years of legislation, that legitimizes argument for the disclosures as well as for their prosecution. Foucauldian rhetoric allows us to map the contentious ground for two competing discursive logics, where arguments that rehearse themes of transparency or security ultimately end up molding new systems of surveillance and intervention that function according to a warped logic of reversal—metonymical substitution—that, in a digital post 9/11, blankets the public with potential signs of dangerousness. Regarding limitations, one of the underexplored aspects of my argument was precisely the digital-as-technology aspect. Thus, a more robust exploration of the role of the digital would provide, alongside my argument, an opportunity to explore how the permeability of digital borders extends the possibilities of surveillance, of archiving, and thus of constructing profiles of dangerous individuals as well as make

governments more open to inadvertent transparency and to kairotic irruption of information.

Perhaps the most productive avenue or research to emerge from this project is the one signaled by the expression *dangerousness*. At the intersection of things that become public problems and institutional modes of intervention a *rhetorical hermeneutics of dangerousness* emerges. By this I mean that signs of dangerousness develop alongside the interpretive gird that results in labeling one as an enemy. This can range, as we have seen, from one's biography, mental health, psychological predispositions, movements, and financial situation—meaning the *observables*—as indicators of a heightened risk of becoming an insider threat/leaker to the drone strikes labeled "signature strike" that do not target a particular person—a known terrorist for example—but are conducted against people who "match a pre-identified 'signature' of behavior that the U.S. links to militant activity."[469] The results of this rhetorical hermeneutics of dangerousness, as we can see, can be dire, from increased surveillance of populations to killing people across the globe. This reversal where it is not the crime but something assembled from signs that becomes the signifier of threat/of an enemy, must be exposed and critiqued, its warped logic—placing the criminal before the crime—and its dire implication must be exposed, and the apparatuses of surveillance, the intervention it engenders, that can lead to loss of life, must be mapped and, with its attendance conceptual issues, resisted.

[1] Michel Foucault, "Polemics, Politics, and Problematizations" in *Essential Foucault; Selection from The Essential Works of Foucault 1954-1984*, ed. Paul Rabinow and Nikolas Rose (New York: The New Press, 2003), 21.
[2] Erik Wemple, "Greenwald to Colbert: Next NSA story will make 'biggest impact,'" *Washingtonpost.com*, May 13, 2014, http://www.washingtonpost.com/blogs/erik-wemple/ wp/2014/05/13/greenwald-to-colbert-next-nsa-story-will-make-biggest-impact/.
[3] Michel Foucault, *The Archeology of Knowledge*, (New York: Vintage Books, 2010): 21.
[4] Barbara Biesecker, "Michel Foucault and the Question of Rhetoric," *Philosophy & Rhetoric* 25, no. 4 (1992), 351.
[5] John M. Sloop, *The Cultural Prison: Discourse, Prisoners, And Punishment* (Tuscaloosa: University of Alabama Press, 1996).
[6] Foucault, *The Archeology*, 25.
[7] Roger Deacon, "Theory as Practice: Foucault's Concept of Problematization," *Telos: A Quarterly Journal Of Critical Thought* 118, (2000), 128.
[8] Foucault, *The Archeology*, 25.
[9] Michel Foucault, "Foucault replies to questions from the audience at Berkeley's History Department in 1983", transcribed by Arianna Bove, http://www.generation-online.org/p/fpfoucault4.htm.
[10] Deacon, "Theory as Practice," 130.
[11] Gilles Deleuze, "What is a Dispositif?" in Michel *Foucault Philosopher*, trans. by Timothy J. Armstrong, (New York: Harvester Wheatsheaf, 1992), 164.
[12] Michel Foucault, *Politics, Philosophy, Culture. Interviews and Other Writings 1977-1984*, ed. by Lawrence Kritzman (London: Routledge, 1988), 257.
[13] Deacon, "Theory as Practice," 127.
[14] Foucault, "Polemics, Politics," 23.
[15] Ibid., 24.
[16] Ibid., 23
[17] Ibid.
[18] Deacon, "Theory as Practice,"140.
[19] Michel Foucault, "Prisons et asiles dans le mécanisme du pouvoir," in *Dits et Ecrits* vol. 11 (Paris: Gallimard, 1974), 523-4 as quoted in Clare O'Farrell, *Michel Foucault* (London: SAGE, 2005), 50.
[20] Joshua Gunn and Dana L. Cloud, "Agentic Orientation as Magical Voluntarism." *Communication Theory* 20, no. 1 (2010).
[21] Christian Lundberg and Joshua Gunn, "'Ouija Board, Are There Any Communications?' Agency, Ontotheology, and the Death of the Humanist Subject, or, Continuing the ARS Conversation," *Rhetoric Society Quarterly* 35, no. 4 (2005).
[22] Gunn and Cloud. "Agentic."
[23] Dilip Parameshwar Gaonkar, "Foucault on Discourse: Methods and Temptations," *Journal of American Forensic Association* 18, (1982): 253.
[24] Gaonkar, "Foucault on Discourse," 253.
[25] Ibid., 255.
[26] Ibid.
[27] Ibid., 256.

[28] Barbara A. Biesecker, "Rethinking the Rhetorical Situation from Within the Thematic of Différance," *Philosophy & Rhetoric* 22, no. 2 (1989): 110.
[29] Ronald Walter Greene, "Another Materialist Rhetoric." *Critical Studies in Mass Communication* 15, no. 1 (1998): 23.
[30] Biesecker, "Rethinking,"110.
[31] Greene, "Another Materialist," 23.
[32] Ibid.
[33] Lloyd F. Bitzer, "The Rhetorical Situation," *Philosophy & Rhetoric* 1, no. 1 (Winter 1968): 5-6.
[34] Biesecker, "Rethinking," 113.
[35] Ibid., 114.
[36] Biesecker, "Rethinking,"112.
[37] Ibid., 121.
[38] Ibid., 127.
[39] Kevin DeLuca, "Articulation Theory: A Discursive Grounding for Rhetorical Practice," *Philosophy & Rhetoric* 32, no. 4 (1999): 335.
[40] Ibid.
[41] Greene, "Another Materialist," 35.
[42] Kevin DeLuca, "Articulation," 334.
[43] Michel Foucault, "Technologies of the Self" in *Ethics: Subjectivity and Truth*, ed. Paul Rabinow, (New York: The New Press, 1997), 225.
[44] Ibid.
[45] Greene, "Another Materialist," 30.
[46] Ronald Walter Greene, "Y Movies: Film and the Modernization of Pastoral Power," *Communication & Critical/Cultural Studies* 2, no. 1 (2005): 20-36.
[47] Michel Foucault, "Confession of the Flesh," in *Power/Knowledge Selected Interviews & Other Writings 1972-1977*, ed. Colin Gordon, (New York: Pantheon Books. 1980), 194-195.
[48] Ibid., 195.
[49] Ibid., 196.
[50] Michel Foucault, "The Discourse on Language," in *The Archeology of Knowledge*, (New York: Vintage Books, 2010), 216.
[51] Foucault, "The Discourse," 220.
[52] Ibid., 216.
[53] Ibid.
[54] Ibid.
[55] Ibid., 220.
[56] Ibid., 224.
[57] "What is FOIA?" accessed February 1st, 2015, http://www.foia.gov/.
[58] Foucault, "The Discourse," 222.
[59] Ibid., 223
[60] Ibid., 224
[61] Ibid., 217.
[62] Ibid., 218.
[63] Ibid., 219.
[64] Ibid., 219.
[65] Ibid.
[66] Ibid., 220.
[67] Jeremy Bentham, "Of Publicity" in The Works of Jeremy Bentham Vol. 2, ed. John Bowring (Edinburgh: William Tait, 1838-1843), http://oll.libertyfund.org/titles/192.
[68] Jurgen Habermas, Sara Lennox, and Frank Lennox, "The Public Sphere: An Encyclopedia Article (1964)." *New German Critique* no. 3 (1974):49 – 50.
[69] Ibid., 55.

[70] *An Act to amend section 552 of title 5, United States Code, to codify the provisions of Public Law 89-187*, Public Law 90-23, *United States Statutes at Large* 81 (1967).
[71] *Privacy Act of 1974*, Public Law 93-579, *United States Statutes at Large* 88 (1974.
[72] Ibid., 1896.
[73] *Government in the Sunshine Act*, Public Law 94-409, United States Statutes at Large 90 (1967).
[74] Ibid., 1241.
[75] *The Electronic Freedom of Information Act Amendments of 1996*, Public Law 104-231, *United States Statutes at Large* 110 (1996).
[76] Ibid., 3048.
[77] Ibid.
[78] Ibid., 3048-49.
[79] *Openness Promotes Effectiveness in our National Government Act of 2007*, Public Law 110-175, *United States Statutes at Large* 121 (2007).
[80] Ibid., 2524.
[81] Ibid.
[82] Ibid.
[83] Ibid.
[84] Ibid.
[85] Ibid., 2524-25.
[86] *FOIA Oversight and Implementation Act of 2014*, H. R. 1211, 113th Cong., 2nd sess. *Congressional Record* 160, no. 31 (February 25, 2014).
[87] Ibid., H 1887-1888.
[88] Ibid., H 1889.
[89]Executive Order 12065 of June 28, 1978, National Security Information, *Homeland Security Digital Library*, https://www.hsdl.org/?abstract&did=457386.
[90] Jimmy Carter, "National Security Information Statement on Issuing Executive Order 12065," June 29, 1978, eds. Gerhard Peters and John T. Woolley, *The American Presidency Project*, http://www.presidency.ucsb.edu/ws/?pid=31008.
[91] Executive Order 12356 of Apr. 2, 1982, Classified National Security Information, *National Archives*, http://www.archives.gov/federal-register/codification/executive-order/12356.html.
[92] Executive Order 12958 of Apr. 17, 1995, Classified National Security Information. *Weekly Compilation of Presidential Documents* Volume 31, Issue 16 (April 24, 1995): 634-651. http://www.gpo.gov/fdsys/pkg/WCPD-1995-04-24/pdf/WCPD-1995-04-24-Pg634.pdf.
[93] Executive Order 13292 of March 25, 2003. Further Amendment to Executive Order 12958, as Amended, Classified National Security Information, *Weekly Compilation of Presidential Documents* Volume 39, no. 13 (March 31, 2003): 359-376. http://www.gpo.gov/fdsys/pkg/WCPD-2003-03-31/pdf/WCPD-2003-03-31-Pg359.pdf.
[94] Executive Order 13526 of December 29, 2009, Classified National Security Information, *Compilation of Presidential Documents*, http://www.gpo.gov/fdsys/pkg/DCPD-200901022/pdf/DCPD-200901022.pdf.
[95] Foucault, "The Discourse," 229.
[96] Ibid.
[97] Ibid., 229.
[98] Ibid.
[99] Ibid.
[100] Ibid.
[101] Ibid., 231 – 32.
[102] 5 U.S.C. 552 (2006), 27, http://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552.pdf.
[103] Ibid.
[104] Ibid., 28.
[105] Ibid.,. 27.
[106] Ibid., 31.

[107] E.O. 13526, 300.
[108] "Supreme Court Vacates Exemption 1 Decision," *FOIA Updated* XX, no 1, January 1, 1999, http://www.justice.gov/oip/blog/foia-update-supreme-court-vacates-exemption-1-decision.
[109] "Public information," Title 5 U.S. Code, 28.
[110] "H.R. Report 92-1419: Administration of the Freedom of Information Act," *Union Calendar* no. 738, 92nd Congress 2nd Session, 1972, 8, http://www.loc.gov/rr/frd/Military_Law/pdf/FOIA-1974.pdf.
[111] Jack Gillum, "Top Obama Appointees Using Secret Email Accounts," *Associated Press*, June 4, 2013, http://bigstory.ap.org/article/emails-top-obama-appointees-remain-mystery.
[112] "Public information," Title 5 U.S. Code, 29.
[113] Ibid.
[114] ""H.R. Report 92-1419," 8.
[115] "Public information," Title 5 U.S. Code, 29.
[116] E.O. 12065.
[117] Ibid.
[118] Ibid.
[119] E.O. 12356.
[120] E.O. 12958.
[121] E.O. 13292.
[122] E.O. 13526, 300.
[123] Carolyn R. Miller, "Kairos in the Rhetoric of Science," in *A Rhetoric of Doing: Essays on Written Discourse in Honor of James L. Kinneavy*, Ed. Stephen P. Witte, Neil Nakadate, and Roger D. Cherry, (Carbondale: Southern Illinois UP, 1992), 310.
[124] Ibid., 312.
[125] Ibid.
[126] Ibid.
[127] E.O. 12065.
[128] E.O. 13526, 292-299
[129] Miller, "Kairos," 313.
[130] Ibid.
[131] Michel Foucault, *The Government of Self and Others: Lectures at the College de France, 1982-1983*, ed. Frederic Gros, trans. Graham Burchell (New York: Picador, 2011): 63.
[132] Miller, "Kairos," 313.
[133] E.O. 13526, 292-99.
[134] Ibid.
[135] Foucault, "The Discourse," 225.
[136] Ibid., 226.
[137] Arron Swartz, "Guerrilla Access Manifesto,"*Archive.org*, Accessed February 1, 2015, http://archive.org/stream/ GuerillaOpenAccessManifesto/Goamjuly2008_djvu.txt.
[138] Foucault, "The Discourse," 226.
[139] Gerald A. Schroeder, "An Overview of Executive Order 12356," *FOIA Update* III, no. 3, 1982, http://www.justice.gov/oip/foia_updates/Vol_III_3/page6.htm.
[140] Foucault, "The Discourse," 224-25.
[141] Ibid., 216.
[142] Ibid., 225.
[143] Ibid.
[144] 5 U.S.C. 552 (2006), http://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552.pdf.
[145] Ibid.
[146] Ibid.
[147] Ibid.
[148] Ibid.
[149] Ibid.

[150] Ibid.
[151] Ibid.
[152] Ibid.
[153] Jon O. Shimabukuro and L. Paige Whitaker, "Whistleblower Protections under Federal Law: An Overview," *Congressional Research Service*, September 13, 2012, 17, https://www.fas.org/sgp/crs/misc/R42727.pdf.
[154] "S. 743 Report of the Committee on Homeland Security and Governmental Affairs United States Senate," *Union Calendar* no. 358, April 19, 2012, 112th Congress 2nd sess., 1, http://www.gpo.gov/fdsys/pkg/CRPT-112srpt155/pdf/CRPT-112srpt155.pdf
[155] Ibid., 5.
[156] Ibid.
[157] Ibid., 2.
[158] Ibid., 33.
[159] Jess Bravin, "Supreme Court to Hear Case on Whistleblower Protection for Air Marshal," *Wall Street Journal*, May 19, 2014, http://www.wsj.com/articles/SB10001424052702304422704579571850297006192
[160] Nina Totenberg, "Supreme Court Rules in Favor of Air Marshal Whistleblower," *NPR*, January 21, 2015, http://www.npr.org/2015/01/21/378905657/supreme-court-rules-in-favor-of-tsa-whistleblower.
[161] Woodrow Wilson, "Third Annual Message, December 7, 1915," *The American Presidency Project*, ed. Gerhard Peters and John T. Woolley, accessed February 7, 2015, http://www.presidency.ucsb.edu/ws/?pid=29556.
[162] *An Act to Prevent the Disclosure of National Defense Secrets*, H.R. 26656, *US Statues at Large* 34 (1909 - 1911): 1084, http://www.constitution.org/uslaw/sal/036_statutes_at_large.pdf.
[163] *An Act To Punish Acts Of Interference With The Foreign Relations, The Neutrality, And The Foreign Commerce Of The United States, To Punish Espionage, And Better To Enforce The Criminal Laws Of The United States, And For Other Purposes*, H.R. 291, *United States Statutes at Large* 40 (1919): 217 – 231, http://www.constitution.org/uslaw/sal/040_statutes_at_large.pdf
[164] Ibid.
[165] *An Act to Amend Section three, title one, of the Act entitled 'An Act To punish acts of interference with the foreign relations, the neutrality, and the foreign commerce of the United States, to punish espionage, and better to enforce the criminal laws of the United States, and for other purposes,'* H.R. 8753, *United States Statutes at Large* 40 (1919): 553– 554, http://www.constitution.org/uslaw/sal/040_statutes_at _large.pdf.
[166] Thomas L.Tedford, and Dale A. Herbeck, *Freedom of Speech in the United States*, 5th ed. (State College: Strata Publishing Inc., 2005), 47-48.
[167] *Schenck v. United States*, 249 U.S. 47 (1919).
[168] *Frohwerk v. United States*, 249 U.S. 204 (1919).
[169] *Debs V. United States*, 249 U.S. 211 (1919).
[170] *Abrams v. United States*, 250 U.S. 616 (1919).
[171] Jamie Tarabay, "Obama and leakers: Who are the eight charged under the Espionage Act?" *Aljazeera America*, December 5, 2013, accessed on May 30 2014, http://america.aljazeera.com/ articles/2013/12/5/obama-and-leakerswhoaretheeightchargedunderespionageact.html
[172] Foucault, "The Discourse," 216.
[173] E.O. 13526, 292-299.
[174] "The Nation: A Gallery of the Guilty," Time 105, no. 2 (1975).
[175] Richard Nixon and Charles W. Colson, "Conversation Tape 005-109 on June 17, 1971," *Presidential Recording Program*, http://millercenter.org/presidentialrecordings/rmn-005-109.
[176] "Charge Sheet," *The New York Times*, http://graphics8.nytimes.com/packages/pdf /politics/20110302-manning.pdf.
[177] "Verdict Special Findings," *The Freedom of the Press Foundation*, 1, https://pressfreedomfoundation .org /sites/default /files/Manning-verdict-special-findings.pdf
[178] Ibid., 6.
[179] Ibid., 1.

[180] Ibid., 6.
[181] Ibid., 2-3.
[182] "U.S. vs. Edward J. Snowden criminal complaint," *The Washington Post*, http://apps.washingtonpost .com /g /documents/world/us-vs-edward-j-snowden-criminal-complaint/496/
[183] "Defense Intelligence Agency assessment of damage done by Edward Snowden leaks– read the report," *The Guardian*, May 22, 2014, http://www.theguardian.com/world/interactive/2014/may/22/pentagon-report-snowden-leaks-damage-report.
[184] Ibid.
[185] Julian Sanchez, "Edward Snowden: Pentagon report on 'grave' threat is gravely overblown," *The Guardian*, 22 May 2014, http://www.theguardian.com/commentisfree/2014/may/22/pentagon-report-snowden-grave-threat-overblown
[186] Daniel Ellsberg, Ben Wizner, Andrew McCarthy, James Woolsey, and John Donvan, "Snowden Was Justified," *Intelligence Squared U.S.*, February 12, 2014, http://intelligencesquaredus.org/images/debates/past/transcripts/021214%20Snowden.pdf.
[187] Foucault, "The Discourse," 229.
[188] Philip Mudd, interview by Stephen Colbert, *"The Colbert Report," Comedy Central*, September 12, 2013, http://thecolbertreport.cc.com/videos/cm16zd/philip-mudd.
[189] Executive Order 13587 of October 07, 2011, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, *Code of Federal Regulations*, Title 3 (2011): 276-280, http://www.gpo.gov/fdsys/pkg/CFR-2012-title3-vol1/pdf/CFR-2012-title3-vol1-eo13587.pdf.
[190] George Silowash, Dawn Cappelli, Andrew Moore, Randall Trzeciak, Timothy J. Shimeall, and Lori Flynn, "Common Sense Guide to Mitigating Insider Threats," 4th ed., December 2012, *National Counterintelligence and Security Center*, http://www.ncix.gov/issues/ithreat/docs/Common_Sense_ Guide_to_Mitigating_Insider_Threats.pdf.
[191] "Welcome to PERSEREC." *The Defense Personnel and Security Research Center*. Accessed February 7th, 2015. http://www.dhra.mil/perserec/index.html.
[192] Marisa Taylor and Jonathan S. Landay, "Obama's crackdown views leaks as aiding enemies of U.S," *McClatchy DC*, June 20th, 2013, http://www.mcclatchydc.com/2013/ 06/20/194513/obamas-crackdown-views-leaks-as.html#storylink=cpy.
[193] Ibid.
[194] Ibid.
[195] Giorgio Agamben, *Homo Sacer: Sovereign Power and Bare Life,* trans. Daniel Heller-Roazen (Stanford: Stanford University Press, 1998).
[196] Jere Van Dyk, "Who were the 4 U.S. citizens killed in drone strikes?" *CBS NEWS*, May 23, 2013 http://www.cbsnews.com/news/who-were-the-4-us-citizens-killed-in-drone-strikes/
[197] Silowash and others, ""Common Sense Guide," xiii.
[198] Eric D. Shaw, Lynn F. Fischer, and Andrée E. Rose, "Insider Risk Evaluation and Audit," *The Defense Personnel and Security Research Center*, August 2009, vii, http://www.dhra.mil/perserec /reports/tr09-02.pdf.
[199] "National Insider Threat Policy," *Office of the Director of National Intelligence*, http://www.ncix.gov/nittf/docs/National_Insider_Threat_Policy.pdf
[200] "Army Regulation 381–12: Threat Awareness and Reporting Program," Army Publishing Directorate, October 2010, 7, http://www.apd.army.mil/pdffiles/r381_12.pdf.
[201] Michel Foucault, *Discipline and Punish. The Birth of the Prison*, trans. Alan Sheridan, (New York: Vintage Books, 1995): 252.
[202] Foucault, "Discipline and Punish," 23.
[203] Ibid., 17.
[204] Ibid., 17-18.
[205] Ibid., 18.
[206] Silowash and others, ""Common Sense Guide," 17.
[207] Ibid.

[208] Ibid., 77.
[209] Ibid.
[210] Ibid., 251.
[211] Ibid., 252.
[212] Ibid.
[213] David L. Charney, "IV. Insights into the Profession. The Psychology of the Insider Spy," *Office of the Director of National Intelligence*, http://www.ncix.gov/issues/ithreat/docs/Charney-PsychologyofInsiderSpyAFIO-INTEL_Fall-Winter2010.pdf
[214] Foucault, "Discipline and Punish," 252.
[215] Ibid., 253.
[216] Ibid., 255.
[217] Ibid.
[218] Michel Foucault, *Politics, Philosophy, Culture. Interviews and Other Writings 1977-1984*, ed. by Lawrence Kritzman (London: Routledge, 1988), p. 257.
[219] Ronald Walter Greene, "Rhetoric (Dis)Appearing," *Communication and Critical/Cultural Studies* 10, no. 2/3, (2013), 261.
[220] Dave Tell, "Rhetoric and Power: An Inquiry into Foucault's Critique of Confession," *Philosophy and Rhetoric* 43(2), 2010: 95-117.
[221] Ibid., 114.
[222] Ibid., 99.
[223] Ibid., 102.
[224] Michel Foucault, "Truth and Juridical Forms" in *Power. Essential Foucault*, ed. Paul Rabinow and Nikolas Rose (New York: The New Press, 2000), 57.
[225] Tell, "Rhetoric and Power," 105.
[226] Ibid., 108.
[227] Ibid.
[228] Ibid.
[229] Foucault, "Discipline and Punish," 252.
[230] Shaw and others, "Insider Risk Evaluation and Audit," 4.
[231] Ibid., 22.
[232] Ibid., 23.
[233] Ibid.
[234] Ibid.
[235] "Department of Defense Directive 55240.06," *Defense Technical Information Center*, May 17 2011, 20, http://www.dtic.mil/whs/directives/corres/pdf/524006p.pdf.
[236] James Ball, "Xbox Live Among Game Services Targeted by US and UK Spy Agencies," *The Guardian*, December 9, 2013, http://www.theguardian.com/world/2013/dec/09/nsa-spies-online-games-world-warcraft-second-life.
[237] Michel Foucault, *History if Sexuality Vol. 1*, trans. Robert Hurley, (New York: Vintage Books, 1990), 100.
[238] Foucault, "Discipline and Punish," 22-23.
[239] Ibid., 27.
[240] Ibid., 27.
[241] Silowash and others, ""Common Sense Guide."
[242] Computer Emergency Response Team (CERT) at the Carnegie Mellon University Software Engineering Institute.
[243] "National Threat Assessment Center - Insider Threat Study," *United State Secret Service*, http://www.secretservice.gov/ntac_its.shtml
[244] Foucault, "Discipline and Punish," 252.
[245] Shaw and others, "Insider Risk Evaluation and Audit," 21-22.
[246] Ibid., 22.

[247] Donovan Conley and William O. Saas, "Occultatio: The Bush Administration's Rhetorical War," *Western Journal Of Communication* 74, no. 4 (July 2010): 329-350.
[248] Shaw and others, "Insider Risk Evaluation and Audit," 24-25.
[249] Ibid., 26.
[250] Foucault, "Discipline and Punish," 306.
[251] Shaw and others, "Insider Risk Evaluation and Audit," 26.
[252] Ibid., 27.
[253] Ibid., 15.
[254] FL Greitzer, CF Noonan, LJ Kangas, and AC Dalton "Identifying at-Risk Employees: A Behavioral Model for Predicting Potential Insider Threats," prepared by the Pacific Northwest National Laboratory for the United States Department Of Energy, September 30, 2010, 2.3, http://www.pnl.gov/main/publications /external/technical_reports/PNNL-19665.pdf
[255] Greitzer and others, "Identifying at-Risk Employees," 2.3.
[256] Foucault, "Discipline and Punish," 256.
[257] Greitzer and others, "Identifying at-Risk Employees," 2.5.
[258] Ibid.
[259] Foucault, "Discipline and Punish," 19.
[260] (a) research to further characterize data and indicators to support behavioral profiles that help to differentiate between accidental misuse and true malicious insider activities; (b) research to establish a greater understanding of the motivations of malicious insiders and related precursors or indicators of imminent insider attacks; (c) research on testing/evaluation methods to verify and validate proposed insider threat detection or prediction methods; (d) collection of useful data sets to support evaluation studies; and (e) a continuing responsibility to examine social issues, privacy and ethical issues, and legal considerations surrounding the deployment of insider threat monitoring, analysis, and mitigation systems that balance these public/human rights issues with the needs and responsibilities of organizations, enterprises, and governments in conducting business productively, safely, and securely." Greitzer and others, "Identifying at-Risk Employees," 9.29.
[261] Greitzer and others, "Identifying at-Risk Employees," 9.28.
[262] Foucault, "Discipline and Punish," 28.
[263] Ibid., 202-03.
[264] Greitzer and others, "Identifying at-Risk Employees," 3.8.
[265] Foucault, "Discipline and Punish," 170.
[266] Ibid., 205.
[267] Ibid., 205.
[268] Silowash and others, "Common Sense Guide," 21.
[269] Foucault, "Discipline and Punish," 184.
[270] Ibid.
[271] "Department of Defense Directive 55240.06," 14.
[272] "Army Regulation 381–12," 4.
[273] "Army Regulation 381–12," 6.
[274] Ibid., 7.
[275] Foucault, "Discipline and Punish," 201.
[276] Ibid., 202-203.
[277] Foucault, "Discipline and Punish," 202.
[278] Ibid., 297.
[279] Ibid., 303.
[280] Greitzer and others, "Identifying at-Risk Employees," 7.25.
[281] Ibid.
[282] Foucault, "Discipline and Punish," 304.
[283] Greitzer and others, "Identifying at-Risk Employees," 7.26.
[284] Foucault, "Discipline and Punish," 204.

[285] Ann E. Marimow, "A Rare Peek Into A Justice Department Leak Probe," *The Washington Post*, May 19, 2013, http://www.washingtonpost.com/local/a-rare-peek-into-a-justice-department-leak-probe/2013/05/19/0bc473de-be5e-11e2-97d4-a479289a31f9_story.html.
[286] The full quote is: "Remember, remember, the Fifth of November, the Gunpowder Treason and Plot. I know of no reason why the Gunpowder Treason should ever be forgot... But what of the man? I know his name was Guy Fawkes and I know, in 1605, he attempted to blow up the Houses of Parliament." *V for Vendetta*, directed by James McTeigue (2005: Burbank, CA: Warner Home Video, 2006), Blue-ray.
[287] Ed Pilkington "Chelsea Manning Rejects 'Pacifist' Label in First Statement since Sentencing," *The Guardian*, October 9, 2013, http://www.theguardian.com/world/2013/oct/09/chelsea-manning-not-a-pacifist.
[288] While Julian Assange is a key player, his self-portrayal was excluded from this project as he himself is not a leaker.
[289] George Orwell, *Animal Farm and 1984*, (New York: Harcourt Inc., 1945), Kindle edition.
[290] Bradley Manning, "Sometimes You Have to Pay a Heavy Price to Live in a Free Society," *Democracy Now*, August 21, 2013, http://www.democracynow.org/blog/2013/8/21/bradley_manning_sometimes_you_have_to_pay_a_heavy_price_to_live_in_a_free_society
[291] Ibid.
[292] Ibid.
[293] Ibid.
[294] Ibid.
[295] Ibid.
[296] Ibid.
[297] Ibid.
[298] Ibid.
[299] Edward Snowden, interview by Laura Poitras and Glenn Greenwald, Part I, *The Guardian*, June 9, 2013, http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video.
[300] Ibid.
[301] Ibid.
[302] Ibid.
[303] Barton Gellman "Code Name 'Verax': Snowden, In Exchanges with Post Reporter, Made Clear He Knew Risks," *The Washington Post*, June 9, 2013, http://www.washingtonpost.com/world/national-security/code-name-verax-snowden-in-exchanges-with-post-reporter-made-clear-he-knew-risks/2013/06/09/c9a25b54-d14c-11e2-9f1a-1a7cdee20287_story.html
[304] Ibid.
[305] Edward Snowden, interview by Hubert Seipel, *ARD German TV*, January 29, 2014, http://www.liveleak.com/view?i=f93_1390833151
[306] Ibid.
[307] Ibid.
[308] Ibid.
[309] Ibid.
[310] Ibid.
[311] Edward Snowden, interview by Laura Poitras and Glenn Greenwald, Part II, *The Guardian*, June 9, 2013, http://www.theguardian.com/world/video/2013/jul/08/edward-snowden-video-interview.
[312] "Snowden delivers Channel 4's Alternative Christmas Message," *Channel 4 News*, 25 December 2013, http://www.channel4.com/news/edward-snowden-nsa-gchq-whistleblower-surveillance-spying.
[313] Ibid.
[314] Ibid.
[315] Snowden, interview by Hubert Seipel.
[316] Ibid.
[317] Siobhan Gorman, "NSA Officers Spy on Love Interests," *The Wall Street Journal*, August 23, 2013, http://blogs.wsj.com/washwire/2013/08/23/nsa-officers-sometimes-spy-on-love-interests/

[318] Snowden, interview by Hubert Seipel.
[319] Ibid.
[320] Ibid.
[321] Ibid.
[322] Paige Lavender, "Edward Snowden Receives Sam Adams Award (VIDEO)," *The Huffington Post*, October 12 2013, http://www.huffingtonpost.com/2013/10/12/edward-snowden-video_n_4088780.html.
[323] Ibid.
[324] Bentham, "On Publicity."
[325] Glenn Greenwald and Ryan Gallagher, "Snowden Documents Reveal Covert Surveillance and Pressure Tactics Aimed at WikiLeaks and Its Supporters," *The Intercept* February 18, 2014, https://firstlook.org /theintercept /article/2014/02/18/snowden-docs-reveal-covert-surveillance-and-pressure-tactics-aimed-at-wikileaks-and-its-supporters/
[326] "What is Wikileaks?", July 5, 2011, https://wikileaks.org/About.html.
[327] Ibid.
[328] Habermas, "The Public Sphere," 49.
[329] Ibid., 49.
[330] Ibid.
[331] Ibid.
[332] Ibid., 55.
[333] Jürgen Habermas, *The Structural Transformation of the Public Sphere*, (Cambridge: The MIT Press, 1991), XII.
[334] Ibid.
[335] "What is Wikileaks?"
[336] Hubertus Buchstein, "Bytes that Bite: The Internet and Deliberative Democracy," *Constellations* 4, no. 2 (1997): 250.
[337] Diogenes Laertius, "Lives of Eminent Philosophers," http://www.perseus.tufts.edu/hopper/text?doc =Perseus%3Atext%3A1999.01.0258%3Abook%3D6%3Achapter%3D2#note-linka
[338] Michel Foucault, *The Courage of Truth (The Government of the Self and Other II)*, edited by Frederic Gros, (New York : Palgrave Macmillan, 2011), 2-3.
[339] Pilkington "Chelsea Manning Rejects 'Pacifist' Label."
[340] "Chelsea's Guardian Statement," *The Law Offices of David E. Coombs Blog*, October 9th, 2013, http://www.armycourtmartialdefense.info/2013/10/chelseas-guardian-statement.html.
[341] Snowden, interview by Laura Poitras and Glenn Greenwald, Part I.
[342] Foucault, *The Government of the Self*, 43.
[343] Michel Foucault, *Fearless Speech*, edited by Joseph Pearson, (Los Angeles: Semiotext(e), 2001), 22.
[344] Robert W. Wallace, "The Power to Speak —and not to Listen— in Ancient Athens," in *Free Speech in Classical Antiquity*, edited by Ineke Sluiter & Ralph M. Rosen, (Boston: Brill, 2004), 221.
[345] Ibid.
[346] Sarah Monoson, *Plato's Democratic Entanglements. Athenian Politics and the Practice of Philosophy*, (Princeton: Princeton University Press, 2000), 52.
[347] Arlene W. Saxonhouse, *Free Speech and Democracy in Ancient Athens*, (Cambridge: University Press, 2006), 89.
[348] Monoson, *Plato's Democratic Entanglements*, 65-66.
[349] Ryan K Ballot, "Free Speech, Courage, and Democratic Deliberation" in *Free Speech in Classical Antiquity*, edited by Ineke Sluiter & Ralph M. Rosen, (Boston: Brill, 2004), 233.
[350] Marlein Van Raalte, "Socratic Parrhesia and its Afterlife in Plato's Laws" in *Free Speech in Classical Antiquity*, edited by Ineke Sluiter & Ralph M. Rosen, (Boston: Brill, 2004), 280.
[351] J.J Mulhern, "IIAPPHIIA in Aristotle" in *Free Speech in Classical Antiquity*, edited by Ineke Sluiter & Ralph M. Rosen, (Boston: Brill, 2004), 314.
[352] David R. Novak, "Engaging Parrhesia in a Democracy: Malcolm X as a Truth-teller," *Southern Communication Journal* 71(1) 2006: 41.

[353] Pat J. Gehrke, Susan C. Jarratt, Bradford Vivian & Arthur E. Walzer, "Forum on Arthur Walzer's 'Parrēsia, Foucault, and the Classical Rhetorical Tradition,'" *Rhetoric Society Quarterly* 43, no. 4 (2013): 360.
[354] Monoson, *Plato's Democratic Entanglements*, 53.
[355] Ibid., 54.
[356] Ibid.
[357] Ibid., 55.
[358] Ibid., 237.
[359] Ibid., 62.
[360] Ibid., 52.
[361] Elizabeth Markovits, *The Politics of Sincerity. Plato, Frank Speech, and Democratic Judgment*, (University Park: The Pennsylvania State University Press, 2008), 68.
[362] Foucault, *Fearless Speech*, 19.
[363] Ibid., 12.
[364] Foucault, *The Courage*, 219.
[365] Ibid., 220.
[366] "What is Wikileaks?"
[367] Foucault, *Fearless Speech*, 12.
[368] Trevor Timm and Rainey Reitman, "Freedom of the Press Foundation Publishes Leaked Audio of Bradley Manning's Statement," Freedom fo the Press, March 12, 2013, https://freedom.press /blog /2013/03/fpf-publishes-leaked-audio-of-bradley-mannings-statement.
[369] Foucault, *Fearless Speech*, 17.
[370] Ibid.
[371] Ibid., 18.
[372] Monoson, *Plato's Democratic Entanglements*, 53.
[373] Ibid.
[374] Ibid..
[375] Ibid., 66.
[376] Saxonhouse, *Free Speech*, 86.
[377] Ibid., 88.
[378] Manning, "Sometimes You Have to Pay."
[379] Gellman, "Code name 'Verax.'"
[380] Snowden, interview by Laura Poitras and Glenn Greenwald, Part I.
[381] Ibid.
[382] Daniel Ellsberg answering a reporter in 1971. Ashley Fantz, "Pentagon Papers leaker: 'I was Bradley Manning,'" *CNN*, March 21, 2011, http://www.cnn.com/2011/US/03/19/wikileaks.ellsberg.manning/.
[383] Richard Nixon and John Mitchell, "Nixon Conversation 006-021 on 29 June 1971," *Presidential Recording Program*, http://millercenter.org/presidentialrecordings/rmn-006-021.
[384] "Sign Daniel Ellsberg's petition to free Bradley Manning," *The Chelsea Manning Support Network*, August 1, 2012, http://www.chelseamanning.org/news/sign-daniel-ellsbergs-petition-to-free-bradley-manning.
[385] Hillary Rodham Clinton, "Remarks to the Press on Release of Purportedly Confidential Documents by Wikileaks," U.S. Department of State, November 29, 2010, http://www.state.gov/secretary/20092013clinton/rm/2010/11/152078.htm
[386] Ewen MacAskill, "Julian Assange like a hi-tech terrorist, says Joe Biden," *The Guardian*, December 19, 2010, http://www.theguardian.com/media/2010/dec/19/assange-high-tech-terrorist-biden.
[387] Foucault, *Fearless Speech*, 19.
[388] Markovits, *The Politics of Sincerity*,65-66.
[389] Snowden, interview by Laura Poitras and Glenn Greenwald, Part I.
[390] Ibid.
[391] Barton Gellman. "Edward Snowden, after months of NSA revelations, says his mission's accomplished," *The Washington Post*, December 23, 2013, http://www.washingtonpost.com/world/national

-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html.
[392] Ibid.
[393] Snowden, interview by Laura Poitras and Glenn Greenwald, Part I.
[394] Ibid.
[395] Ibid..
[396] Ibid..
[397] Ibid..
[398] Snowden, interview by Hubert Seipel.
[399] Ibid.
[400] Barton, "Edward Snowden."
[401] Snowden, interview by Hubert Seipel.
[402] Saxonhouse, *Free Speech*, 96.
[403] Snowden, interview by Hubert Seipel.
[404] Ibid.
[405] Barton, "Edward Snowden."
[406] Foucault, *Fearless Speech*, 17.
[407] Snowden, interview by Laura Poitras and Glenn Greenwald, Part I.
[408] Barton, "Edward Snowden."
[409] Ibid.
[410] Edward Snowden, "Statement from Edward Snowden," *ACLU*, November 4, 2013, https://www.aclu.org/blog/national-security/statement-edward-snowden.
[411] Foucault, *Fearless Speech*, 17.
[412] Barton, "Edward Snowden,"
[413] Ibid.
[414] Ibid.
[415] Snowden, interview by Hubert Seipel.
[416] Ibid.
[417] Bradley Manning, "Bradley Manning's full statement," transcript by Alexa O'Brien, *Salon*, March 1, 2013, http://www.salon.com/2013/03/01/bradley_mannings_full_statement/.
[418] Ibid.
[419] Ibid.
[420] Ibid.
[421] Ibid.
[422] Ibid.
[423] Ibid.
[424] Manning, "Bradley Manning's full statement."
[425] Ibid.
[426] Chelsea Manning, "Unfortunately, I can't go back and change things," *The Guardian*, August 14, 2013, http://www.theguardian.com/world/2013/aug/14/bradley-manning-statement-sentencing-trial.
[427] Ibid.
[428] Manning, "Unfortunately, I can't go back and change things."
[429] Foucault, *The Courage*, 24.
[430] Foucault, *Fearless Speech*, 15-16.
[431] Ibid., 15.
[432] Foucault, *The Government of the Self*, 56.
[433] Ibid., 65.
[434] Ibid..
[435] Ibid., 67
[436] Ibid., 66.
[437] Monoson, *Plato's Democratic Entanglements*, 55.
[438] Ibid.

[439] Ibid., 55-56.
[440] Markovits, *The Politics of Sincerity*,66.
[441] Ibid., 65-66.
[442] Ballot, "Free Speech," 234.
[443] Greenwald and Gallagher, "Snowden Documents."
[444] Manning, "Sometimes You Have to Pay."
[445] Ballot, "Free Speech," 234.
[446] Ibid., 243.
[447] Ibid., 247.
[448] Ibid.
[449] Ibid.
[450] Gellman, "Code name 'Verax.'"
[451] Ibid.
[452] Ibid.
[453] Ibid.
[454] *V for Vendetta*, directed by James McTeigue.
[455] Julian Assange and Slavoj Žižek, interview by Amy Goodman, *Democracy Now*, July 5, 2011, http://www .democracynow.org/2011/7/5/exclusive_julian_assange_of_wikileaks_philosopher.
[456] James Ball, "GCHQ Captured Emails of Journalists from Top International Media," *The Guardian*, January 19, 2015, http://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post.
[457] Assange and Zizek, *Democracy Now*.
[458] Foucault, "The Discourse," 216.
[459]
[460] Greene, "Another Materialist," 22.
[461] Snowden, interview by Laura Poitras and Glenn Greenwald, Part I.
[462] Gaonkar, "Foucault on Discourse."
[463] Gehrke and others, "Forum.".
[464] Susan C. Jarratt, "Untimely Historiography? Foucault's "Greco-Latin Trip,"" *Rhetoric Society Quarterly* 44, no. 3 (2014): 220-233.
[465] Carole Blair and Martha Cooper, "The Humanist Turn In Foucault's Rhetoric of Inquiry," *Quarterly Journal of Speech* 73, no. 2 (1987): 151-171.
[466] Raymie E. Mckerrow, "Critical Rhetoric: Theory and Praxis," *Communication Monographs* 56, no. 2 (1989): 91-111.
[467] Biesecker, "Michel Foucault."
[468] Ronald Walter Greene, "Y Movies: Film and the Modernization of Pastoral Power," *Communication & Critical/Cultural Studies* 2, no. 1 (2005): 20-36.
[469] Danya Greenfield "The Case Against Drone Strikes on People Who Only 'Act' Like Terrorists," *The Atlantic*, August 19 2013, http://www.theatlantic.com/international/archive/2013/08/the-case-against-drone-strikes-on-people-who-only-act-like-terrorists/278744/

Bibliography

5 U.S.C. 552 (2006). http://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012 -title5-partI-chap5-subchapII-sec552.pdf.

Abrams v. United States. 250 U.S. 616 (1919).

Agamben, Giorgio. *Homo Sacer: Sovereign Power and Bare Life*. Translated by Daniel Heller-Roazen. Stanford: Stanford University Press, 1998.

An Act to amend section 552 of title 5, United States Code, to codify the provisions of Public Law 89-187. Public Law 90-23. *United States Statutes at Large* 81 (1967): 54 – 56.

An Act to Amend Section three, title one, of the Act entitled 'An Act To punish acts of interference with the foreign relations, the neutrality, and the foreign commerce of the United States, to punish espionage, and better to enforce the criminal laws of the United States, and for other purposes.' H.R. 8753. *United States Statutes at Large* 40 (1919): 553– 554. http://www.constitution.org/uslaw/sal/040_statutes_at_large.pdf.

An Act to Prevent the Disclosure of National Defense Secrets. H.R. 26656. *US Statues at Large* 34 (1909 - 1911): 1084-1085. http://www.constitution.org/uslaw/sal/036 _statutes _at_large.pdf.

An Act To Punish Acts Of Interference With The Foreign Relations, The Neutrality, And The Foreign Commerce Of The United States, To Punish Espionage, And Better To Enforce The Criminal Laws Of The United States, And For Other Purposes. H.R. 291. *United States Statutes at Large* 40 (1919): 217 – 231. http://www.constitution.org/uslaw /sal/040_statutes_at_large.pdf

"Army Regulation 381–12: Threat Awareness and Reporting Program." *Army Publishing Directorate*. October 2010. http://www.apd.army.mil/pdffiles/r381_12.pdf.

Assange, Julian and Slavoj Žižek. Interview by Amy Goodman. *Democracy Now*. July 5, 2011. http://www.democracynow.org/2011/7/5/exclusive_julian_assange_of _wikileaks _philosopher.

Ball, James. "Xbox Live Among Game Services Targeted by US and UK Spy Agencies." *The Guardian*. December 9, 2013. http://www.theguardian.com/world/2013/dec/09/nsa-spies-online-games-world-warcraft-second-life.

___. “GCHQ Captured Emails of Journalists from Top International Media.” *The Guardian*. January 19, 2015. http://www.theguardian.com/uknews/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post.

Ballot, Ryan K. “Free Speech, Courage, and Democratic Deliberation.” In *Free Speech in Classical Antiquity*. Edited by Ineke Sluiter & Ralph M. Rosen. Boston: Brill, 2004.

Barton Gellman “Code Name ‘Verax’: Snowden, In Exchanges with Post Reporter, Made Clear He Knew Risks,” *The Washington Post*, June 9, 2013, http://www .washingtonpost .com/world/national-security/code-name-verax-snowden-in-exchanges-with-post-reporter-made-clear-he-knew-risks/2013/06/09/c9a25b54-d14c-11e2-9f1a-1a7cdee20287_story.html

Bentham, Jeremy. “Chapter II, Of Publicity” in “An Essay On Political Tactics, Or Inquiries Concerning The Discipline And Mode Of Proceeding Proper To Be Observed In Political Assemblies: Principally Applied To The Practice Of The British Parliament, And To The Constitution And Situation Of The National Assembly Of France.” *The Works of Jeremy Bentham*, published under the Superintendence of his Executor, John Bowring (Edinburgh: William Tait, 1838-1843). 11 vols. Vol. 2. http://oll.libertyfund.org/titles/192.

Biesecker, Barbara. "Michel Foucault and the Question of Rhetoric." *Philosophy & Rhetoric* 25, no. 4 (Fall 1992): 351-364.

___. "Rethinking the Rhetorical Situation from Within the Thematic of Différance." *Philosophy & Rhetoric* 22, no. 2 (Spring 1989): 110-130.

Bitzer, Lloyd F. "The Rhetorical Situation." *Philosophy & Rhetoric* 1, no. 1 (1968): 1-14.

Blair, Carole, and Martha Cooper. "The Humanist Turn In Foucault's Rhetoric Of Inquiry." *Quarterly Journal Of Speech* 73, no. 2 (1987): 151-171.

Bravin, Jess. “Supreme Court to Hear Case on Whistleblower Protection for Air Marshal.” *Wall Street Journal*, May 19, 2014. http://www.wsj.com/articles/SB10001424052702304422704579571850297006192

Buchstein, Hubertus. “Bytes that Bite: The Internet and Deliberative Democracy.” Constellations 4, no. 2 (1997): 248-263.

Carter, Jimmy. "National Security Information Statement on Issuing Executive Order 12065." June 29, 1978. Edited by Gerhard Peters and John T. Woolley, *The American Presidency Project*. http://www.presidency.ucsb.edu/ws/?pid=31008.

"Charge Sheet." *The New York Times*. Accessed June 6th, 2014. http://graphics8.nytimes.com/ packages/ pdf/politics/20110302-manning.pdf

Charney, David L. "IV. Insights into the Profession. The Psychology of the Insider Spy." *Office of the Director of National Intelligence*. http://www.ncix.gov/issues/ithreat /docs/Charney-PsychologyofInsiderSpyAFIO-INTEL_Fall-Winter2010.pdf

Clinton, Hillary Rodham. "Remarks to the Press on Release of Purportedly Confidential Documents by Wikileaks." *U.S. Department of State*. November 29, 2010. http://www.state.gov/secretary/20092013clinton/rm/2010/11/152078.htm

Conley, Donovan, and William O. Saas. "Occultatio: The Bush Administration's Rhetorical War." *Western Journal Of Communication* 74, no. 4 (July 2010): 329-350.

Deacon, Roger. "Theory As Practice: Foucault's Concept of Problematization." *Telos: A Quarterly Journal Of Critical Thought* 118, (December 1, 2000): 127-142.

Debs V. United States. 249 U.S. 211 (1919).

"Defense Intelligence Agency assessment of damage done by Edward Snowden leaks– read the report," *The Guardian*. May 22, 2014. http://www.theguardian.com /world/interactive/2014/ may/22/pentagon-report-snowden-leaks-damage-report.

Deleuze, Gilles. "What is a Dispositif?" in *Michel Foucault Philosopher*, trans. by Timothy J. Armstrong, 159-168. New York: Harvester Wheatsheaf, 1992.

DeLuca, Kevin. "Articulation Theory: A Discursive Grounding for Rhetorical Practice." *Philosophy & Rhetoric* 32, no. 4 (1999): 334-348.

"Department of Defense Directive 55240.06." *Defense Technical Information Center*. May 17 2011. http://www.dtic.mil/whs/directives/corres/pdf/524006p.pdf.

Ellsberg, Daniel, Ben Wizner, Andrew McCarthy, James Woolsey, and John Donvan. "Snowden Was Justified." *Intelligence Squared U.S.*. February 12, 2014. http:// intelligencesquaredus.org/images/debates/past/transcripts/021214%20Snowden.pdf.

Executive Order 12065 of June 28, 1978, National Security Information. *Homeland Security Digital Library*. https://www.hsdl.org/?abstract&did=457386.

Executive Order 12356 of Apr. 2, 1982, Classified National Security Information. *National Archives*. http://www.archives.gov/federal-register/codification /executive-order/12356.html

Executive Order 12958 of Apr. 17, 1995, Classified National Security Information. *Weekly Compilation of Presidential Documents* Volume 31, Issue 16 (April 24, 1995): 634-651. http://www.gpo.gov/fdsys/pkg/WCPD-1995-04-24/pdf/WCPD-1995-04-24-Pg634.pdf.

Executive Order 13292 of March 25, 2003. Further Amendment to Executive Order 12958, as Amended, Classified National Security Information. Weekly Compilation of Presidential Documents Volume 39, no. 13 (March 31, 2003): 359-376. http://www.gpo.gov/fdsys/pkg/WCPD-2003-03-31/pdf/WCPD-2003-03-31-Pg359.pdf.

Executive Order 13526 of December 29, 2009. Classified National Security Information. *Compilation of Presidential Documents*. http://www.gpo.gov/fdsys/pkg/DCPD-200901022/pdf/DCPD-200901022.pdf.

Executive Order 13587 of October 07, 2011, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information. *Code of Federal Regulations*, Title 3 (2011): 276-280. http://www.gpo. gov/fdsys/pkg/CFR-2012-title3-vol1/pdf/CFR-2012-title3-vol1-eo13587.pdf.

Fantz, Ashley. "Pentagon Papers leaker: 'I was Bradley Manning.'" *CNN*. March 21, 2011. http://www.cnn.com/2011/US/03/19/wikileaks.ellsberg.manning/.

FOIA Oversight and Implementation Act of 2014. H. R. 1211, 113th Cong., 2nd sess. *Congressional Record* 160, no. 31. (February 25, 2014): H 1887- 1891.

Foucault, Michel. *The Archeology of Knowledge*. New York: Vintage Books, 2010.

___. "Confession of the Flesh," in *Power/Knowledge Selected Interviews & Other Writings 1972-1977*, edited by Colin Gordon, 194-228. New York: Pantheon Books. 1980.

___. *The Courage of Truth (The Government of the Self and Other II).* Edited by Frederic Gros. New York : Palgrave Macmillan, 2011.

___. *Discipline and Punish. The Birth of the Prison*. Translated by Alan Sheridan. New York: Vintage Books, 1995.

___. "The Discourse on Language." in *The Archeology of Knowledge*, 215-237. New York: Vintage Books, 2010

___. *Fearless Speech*, Edited by Joseph Pearson. Los Angeles: Semiotext(e), 2001.

___. "Foucault replies to questions from the audience at Berkeley's History Department in 1983."transcribed by Arianna Bove, http://www.generation-online.org/p/fpfoucault4.htm.

___. *The Government of Self and Others: Lectures at the College de France, 1982-1983*. Edited by Frederic Gros. Translated by Graham Burchell. New York: Picador, 2011.

___. *The Government of the Self and Others*. New York: Picador, 2010.

___. *History if Sexuality Vol. 1*. trans. Robert Hurley. New York: Vintage Books 1990.

___. "Polemics, Politics, and Problematizations." in *Essential Foucault; Selection from The Essential Works of Foucault 1954-1984*, edited by Paul Rabinow and Nikolas Rose, 18-24. New York: The New Press, 2003.

___. *Politics, Philosophy, Culture. Interviews and Other Writings 1977-1984*. Edited by Lawrence Kritzman. London: Routledge, 1988.

___. "Technologies of the Self" in *Ethics: Subjectivity and Truth*, edited by Paul Rabinow, 223-251. New York: The New Press, 1997.

___. "Truth and Juridical Forms." *Power. Essential Foucault.* ed. Paul Rabinow and Nikolas Rose. New York: The New Press, 2000.

Frohwerk v. United States. 249 U.S. 204 (1919).

Gaonkar, Dilip Parameshwar. "Foucault on Discourse: Methods and Temptations," *Journal of American Forensic Association* 18, (1982): 246-257.

Gaonkar, Dilip Parameshwar and Robert J. McCarthy Jr., "Panopticism and Publicity: Bentham's Quest for Transparency," *Public Culture* 6 (1994): 547-575.

Gehrke, Pat J., Susan C. Jarratt , Bradford Vivian & Arthur E. Walzer. “Forum on Arthur Walzer's ‘Parrēsia, Foucault, and the Classical Rhetorical Tradition.’” Rhetoric Society Quarterly 43, no 4 (2013): 355-381.

Gellman, Barton. “Edward Snowden, after months of NSA revelations, says his mission’s accomplished.” *The Washington Post*. December 23, 2013. http://www.washingtonpost .com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html.

Gillum, Jack. “Top Obama Appointees Using Secret Email Accounts.” *Associated Press*. June 4, 2013. http://bigstory.ap.org/article/emails-top-obama-appointees-remain-mystery.

Gorman, Siobhan. “NSA Officers Spy on Love Interests.” *The Wall Street Journal*. August 23, 2013. http://blogs.wsj.com/washwire/2013/08/23/nsa-officers-sometimes-spy-on-love-interests/.

Government in the Sunshine Act. Public Law 94-409. *United States Statutes at Large* 90 (1967): 1241 – 1248.

Greene, Ronald Walter. "Another materialist rhetoric." *Critical Studies In Mass Communication* 15, no. 1 (March 1998): 21-40.

___. “Rhetoric (Dis)Appearing.” *Communication and Critical/Cultural Studies* 10, no. 2/3. (September 2013): 259-264.

___. "Y Movies: Film and the Modernization of Pastoral Power." Communication & Critical/Cultural Studies 2, no. 1 (2005): 20-36.

Greenfield, Danya. “The Case Against Drone Strikes on People Who Only 'Act' Like Terrorists.” *The Atlantic*. August 19 2013. http://www.theatlantic.com /international/archive/2013/08/the-case-against-drone-strikes-on-people-who-only-act-like-terrorists/278744/.

Greitzer. FL, CF Noonan, LJ Kangas, and AC Dalton. “Identifying at-Risk Employees: A Behavioral Model for Predicting Potential Insider Threats.” Prepared by the Pacific Northwest National Laboratory for the United States Department Of Energy. September 30, 2010. http://www.pnl.gov/main/publications/external /technical_reports/PNNL-19665.pdf

Greenwald, Glenn and Ryan Gallagher. “Snowden Documents Reveal Covert Surveillance and Pressure Tactics Aimed at WikiLeaks and Its Supporters.” *The Intercept*. February 18, 2014. https://firstlook.org/theintercept/article/2014/02/18/snowden-docs-reveal-covert-surveillance-and-pressure-tactics-aimed-at-wikileaks-and-its-supporters/.

Gunn, Joshua, and Dana L. Cloud. "Agentic Orientation as Magical Voluntarism." *Communication Theory* 20, no. 1 (February 2010): 50-78.

Habermas, Jurgen, Sara Lennox, and Frank Lennox. "The Public Sphere: An Encyclopedia Article (1964)." *New German Critique* no. 3 (1974): 49-55.

___. *The Structural Transformation of the Public Sphere*. Cambridge: The MIT Press, 1991.

Hosenball, Mark. “U.S. officials don't know how much secret material Snowden took.” *Reuters*. June 24, 2013. http://www.reuters.com/article/2013/06/24/us-usa-security-material-idUSBRE95N1F820130624.

“H.R. Report 92-1419: Administration of the Freedom of Information Act.” *Union Calendar* no. 738. 92nd Congress, 2nd sess., 1972. http://www.loc.gov/rr/frd/Military_Law/pdf/FOIA-1974.pdf.

Jarratt, Susan C. "Untimely Historiography? Foucault’s “Greco-Latin Trip”." *Rhetoric Society Quarterly* 44, no. 3. (2014): 220-233.

Lundberg, Christian, and Joshua Gunn. “‘Ouija Board, Are There Any Communications?’ Agency, Ontotheology, and the Death of the Humanist Subject, or, Continuing the ARS Conversation." *Rhetoric Society Quarterly* 35, no. 4 (Fall 2005): 83-105.

MacAskill, Ewen. “Julian Assange like a hi-tech terrorist, says Joe Biden.” *The Guardian*. December 19, 2010. http://www.theguardian.com/media/2010/dec/19/assange-high-tech-terrorist-biden.

Mckerrow, Raymie E. "Critical Rhetoric: Theory and Praxis." *Communication Monographs* 56, no. 2 (1989): 91-111.

Manning, Bradley. “Sometimes You Have to Pay a Heavy Price to Live in a Free Society.” *Democracy Now*. August 21, 2013. http://www.democracynow.org/blog/2013/8/21/bradley_manning_sometimes_you_have_to_pay_a_heavy_price_to_live_in_a_free_society

___. “Bradley Manning’s full statement,” transcript by Alexa O'Brien, *Salon*, March 1, 2013, http://www.salon.com/2013/03/01/bradley_mannings_full _statement/.

Manning, Chelsea. “Unfortunately, I can't go back and change things.” *The Guardian*. August 14, 2013. http://www.theguardian.com/world/2013/aug/14/bradley-manning-statement-sentencing-trial.

___. “Chelsea's Guardian Statement.” *The Law Offices of David E. Coombs Blog*. October 9, 2013. http://www.armycourtmartialdefense.info/2013/10 /chelseas-guardian-statement.html.

Marimow, Ann E. “A Rare Peek into a Justice Department Leak Probe.” *The Washington Post.* May 19, 2013. http://www.washingtonpost.com/local/a-rare-peek-into-a-justice-department-leak-probe/2013/05/19/0bc473de-be5e-11e2-97d4-a479289a31f9_story.html.

Markovits, Elizabeth. *The Politics of Sincerity. Plato, Frank Speech, and Democratic Judgment*. University Park: The Pennsylvania State University Press, 2008.

Miller, Carolyn R. “*Kairos* in the Rhetoric of Science.” In *A Rhetoric of Doing: Essays on Written Discourse in Honor of James L. Kinneavy*, edited by Stephen P. Witte, Neil Nakadate, and Roger D. Cherry, 310–327. Carbondale: Southern Illinois UP, 1992.

Monoson, Sarah. *Plato’s Democratic Entanglements. Athenian Politics and the Practice of Philosophy*. Princeton: Princeton University Press, 2000.

Mulhern, J.J. “IIAPPHIIA in Aristotle.” In *Free Speech in Classical Antiquity*. Edited by Ineke Sluiter & Ralph M. Rosen. Boston: Brill, 2004.

Mudd, Philip. Interview by Stephen Colbert. “The Colbert Report.” *Comedy Central*. September 12, 2013. http://thecolbertreport.cc.com/videos/cm16zd/philip-mudd.

“National Insider Threat Policy,” *Office of the Director of National Intelligence*, http://www. ncix. gov/ nittf/docs/National_Insider_Threat_Policy.pdf

“National Threat Assessment Center - Insider Threat Study,” *United State Secret Service*, http://www.secretservice.gov/ntac_its.shtml

Nixon, Richard and Charles W. Colson. “Nixon Conversation on June 17, 1971,” *Presidential Recording Program*. http://millercenter.org/presidentialrecordings /rmn-005-109.

Nixon, Richard and John Mitchell. “Nixon Conversation on 29 June 1971.” *Presidential Recording Program*. http://millercenter.org/presidentialrecordings/rmn-006-021.

Novak, David R. “Engaging *Parrhesia* in a Democracy: Malcolm X as a Truth-teller.” *Southern Communication Journal* 71, no. 1 (2006): 25-43.

O'Farrell, Clare. *Michel Foucault.* London: SAGE, 2005.

Openness Promotes Effectiveness in our National Government Act of 2007. Public Law 110-175. *United States Statutes at Large* 121 (2007): 2524 – 2531.

Orwell, George. *Animal Farm and 1984.* New York: Harcourt Inc., 1945. Kindle edition.

Paige Lavender, “Edward Snowden Receives Sam Adams Award (VIDEO),” *The Huffington Post*, October 12 2013, http://www.huffingtonpost.com/2013/10/12/edward-snowden-video_n_4088780.html.

Pilkington, Ed. “Chelsea Manning Rejects 'Pacifist' Label in First Statement since Sentencing.” *The Guardian*. October 9, 2013. http://www.theguardian.com/world/2013/oct/09/chelsea-manning-not-a-pacifist.

Privacy Act of 1974. Public Law 93-579. *United States Statutes at Large* 88 (1974): 1896 – 1910.

Reidy, Patrick. “Combating the Insider Threat at the FBI: Real-world Lessons Learned.” *YouTube* video. 59:40. November 19, 2013. https://www.youtube.com/watch?v=38M8ta13K0Q.

“S. 743 Report of the Committee on Homeland Security and Governmental Affairs United States Senate.” *Union Calendar* no. 358. April 19, 2012. 112th Congress 2nd sess. http://www.gpo.gov/fdsys/pkg/CRPT-112srpt155/pdf/CRPT-112srpt155.pdf.

Sanchez, Julian. “Edward Snowden: Pentagon report on 'grave' threat is gravely overblown.” *The Guardian*. 22 May 2014. http://www.theguardian.com/commentisfree/2014/may/22/pentagon-report-snowden-grave-threat-overblown.

Saxonhouse, Arlene W. *Free Speech and Democracy in Ancient Athens*. Cambridge: University Press, 2006.

Schenck v. United States. 249 U.S. 47 (1919).

Schroeder, Gerald A. "An Overview of Executive Order 12356." *FOIA Update* III, no. 3. 1982. http://www.justice.gov/oip/foia_updates/Vol_III_3/page6.htm.

Shaw, Eric D., Lynn F. Fischer and Andrée E. Rose. "Insider Risk Evaluation and Audit." *The Defense Personnel and Security Research Center*. August 2009. http://www.dhra.mil/perserec /reports/tr09-02.pdf.

Shimabukuro Jon O. and L. Paige Whitaker. "Whistleblower Protections under Federal Law: An Overview." *Congressional Research Service*. September 13, 2012. https://www.fas.org/sgp/crs/misc/R42727.pdf.

Silowash, George, Dawn Cappelli, Andrew Moore, Randall Trzeciak, Timothy J. Shimeall, and Lori Flynn. "Common Sense Guide to Mitigating Insider Threats," 4th ed. December 2012. *National Counterintelligence and Security Center*. http://www.ncix.gov/issues/ithreat/docs/Common_Sense_Guide_to_Mitigating_Insider_Threats.pdf.

Sloop, John M. *The Cultural Prison: Discourse, Prisoners, And Punishment*. Tuscaloosa: University of Alabama Press, 1996.

Snowden, Edward. Interview by Laura Poitras and Glenn Greenwald. *The Guardian*. June 9, 2013. http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video.

___. Interview by Laura Poitras and Glenn Greenwald. Part II. *The Guardian*. June 9, 2013. http://www.theguardian.com/world/video/2013/jul/08/edward-snowden-video-interview.

___, Interview by Hubert Seipel. *ARD German TV*. January 29, 2014. http://www.liveleak .com/view?i=f93_1390833151

___. "Statement from Edward Snowden." *ACLU*. November 4, 2013. https://www.aclu .org/blog/national-security/statement-edward-snowden.

"Snowden delivers Channel 4's Alternative Christmas Message." *Channel 4 News*. December 25, 2013. http://www.channel4.com/news/edward-snowden-nsa-gchq-whistleblower-surveillance-spying.

"Supreme Court Vacates Exemption 1 Decision." *Foia Updated* XX, no 1. January 1, 1999. http://www.justice.gov/oip/blog/foia-update-supreme-court-vacates-exemption-1-decision.

Swartz, Arron. “Guerrilla Access Manifesto.”*Archive.org*. Accessed February 1st, 2015. http://archive.org/stream/GuerillaOpenAccessManifesto/Goamjuly2008_djvu.txt.

Tarabay, Jamie. “Obama and Leakers: Who are the eight charged under the Espionage Act?” *Aljazeera America*. December 5, 2013. http://america.aljazeera.com/articles/2013/12/5/obama-and-leakerswhoaretheeightchargedunderespionage act.html

Taylor, Marisa and Jonathan S. Landay. “Obama’s crackdown views leaks as aiding enemies of U.S.” *McClatchy DC*. June 20th, 2013. http://www.mcclatchydc.com /2013/06/20/194513/obamas-crackdown-views-leaks-as.html#storylink=cpy

Tedford, Thomas L. and Dale A. Herbeck. *Freedom of Speech in the United States*. 5th ed. State College: Strata Publishing Inc., 2005.

Tell, Dave. “Rhetoric and Power: An Inquiry into Foucault’s Critique of Confession.” *Philosophy and Rhetoric* 43, no. 2 (2010): 95-117.

The Electronic Freedom of Information Act Amendments of 1996. Public Law 104-231. *United States Statutes at Large* 110 (1996): pages 3048 –3054.

"The Nation: A Gallery of the Guilty." *Time* 105, no. 2 (1975).

Timm, Trevor and Rainey Reitman. “Freedom of the Press Foundation Publishes Leaked Audio of Bradley Manning’s Statement.” *Freedom of the Press.* March 12, 2013. https://freedom.press/blog/2013/03/fpf-publishes-leaked-audio-of-bradley-mannings-statement.

Totenberg, Nina. “Supreme Court Rules in Favor of Air Marshal Whistleblower,” *NPR*, January 21, 2015. http://www.npr.org/2015/01/21/378905657/supreme-court-rules-in-favor-of-tsa-whistleblower.

“U.S. vs. Edward J. Snowden criminal complaint.” *The Washington Post*. Accessed February 7th, 2015. http://apps.washingtonpost.com/g/documents/world/us-vs-edward-j-snowden-criminal-complaint/496/

V for Vendetta. Directed by James McTeigue. 2005. Burbank, CA: Warner Home Video, 2006. Blue-ray.

Van Dyk, Jere. “Who were the 4 U.S. citizens killed in drone strikes?” *CBS NEWS*. May 23, 2013. http://www.cbsnews.com/news/who-were-the-4-us-citizens-killed-in-drone-strikes/

Van Raalte, Marlein. “Socratic *Parrhesia* and its Afterlife in Plato’s Laws.” In *Free Speech in Classical Antiquity*. Edited by Ineke Sluiter & Ralph M. Rosen. Boston: Brill, 2004.

“Verdict Special Findings.” *The Freedom of the Press Foundation*. Accessed June 6th, 2014. https://pressfreedomfoundation.org/sites/default/files/Manning-verdict-special-findings.pdf

Wallace, Robert W. “The Power to Speak —and not to Listen— in Ancient Athens.” In *Free Speech in Classical Antiquity*. Edited by Ineke Sluiter & Ralph M. Rosen. Boston: Brill, 2004.

“Welcome to PERSEREC.” *The Defense Personnel and Security Research Center*. Accessed February 7th, 2015. http://www.dhra.mil/perserec/index.html.

Wemple, Erik. “Greenwald to Colbert: Next NSA story will make ‘biggest impact.’” *The Washington Post*, May 13, 2014. http://www.washingtonpost.com/blogs/erik-wemple/wp/2014/05/13/greenwald-to-colbert-next-nsa-story-will-make-biggest-impact/.

“What is FOIA?” accessed February 1st. 2015. http://www.foia.gov/.

“What is Wikileaks?”, July 5, 2011, https://wikileaks.org/About.html.

Wilson, Woodrow. "Third Annual Message, December 7, 1915”. *The American Presidency Project*. Edited by Gerhard Peters and John T. Woolley. Accessed February 7, 2015. http://www.presidency.ucsb.edu/ws/?pid=29556.