UNIVERSITY OF CALIFORNIA

Los Angeles

Making Secret(s): The Infrastructure of Classified Information

A dissertation submitted in partial satisfaction

of the requirements for the degree Doctor of Philosophy

in Information Studies

by

Stacy Elizabeth Wood

2017

ABSTRACT OF THE DISSERTATION

Making Secret(s): The Infrastructure of Classified Information

by

Stacy Elizabeth Wood

Doctor of Philosophy in Information Studies

University of California, Los Angeles, 2017

Professor Safiya U Noble, Chair

This dissertation defines and analyzes the infrastructure of classified information including the sites, systems, objects and discourses that enable the creation, maintenance, management and destruction of classified information. Seeking to situate classified information as something other than a mere absence of information or an impediment to knowledge, this dissertation focuses on what kinds of records, documents, evidence and knowledge are created through the daily practices of official secrecy at the federal level. The increasing complexity of overlapping technical infrastructures and organizational standards requires thinking about records infrastructurally, re-framing individual documents as systems, if we are to begin thinking of future use and access.

This dissertation examines records within the infrastructure of classified information by contextualizing the need for research into these records as objects of great complexity that eschew easy distinctions between open and closed. It utilizes a research framework oriented around four elements: Standards, Economies, Rupture and Culture. Using methods from infrastructure studies, archival studies and critical discourse analysis, it analyzes the field of creation within socio-technical systems and identifies materiality as a matter of paramount importance for the maintenance of evidential value within overlapping systems of trust.

This dissertation illustrates the paucity of nuanced understandings of networked records in federal agencies and exposes a number of areas for further research and challenges for those who work in archival studies and information policy. This dissertation finds that a vital rethinking of the role of archival work and thinking could lead to an integration of archival processes into daily government work instead of traditional modes of custodial transfer.

The dissertation of Stacy Elizabeth Wood is approved.

Anne J. Gilliland

Michelle Caswell

Lisa Parks

Safiya U Noble, Committee Chair

University of California, Los Angeles

2017

Table of Contents

List of Figures

STACY WOOD
Department of Information Studies
University of California Los Angeles

EDUCATION

PhD	University of California, Los Angeles Information Studies	Anticipated 2017
MLIS	University of California, Los Angeles Archival Studies	Anticipated 2017
BA	University of California, Los Angeles English and World Literature, Gender Studies, Media Studies	2007

SELECTED AWARDS

Aimee Dorr Fellowship for Public Policy University of California Los Angeles	2015
Distinguished Teaching Award University of California Los Angeles	2015

PUBLICATIONS

Peer-Reviewed Journal Articles

2016 Wood, S. Police body cameras and professional responsibility. *Preservation, Digital Technology & Culture.* Forthcoming.

2016 Cifor, M. and Wood, S. Critical feminism in the archives. *Journal of Critical Library and Information Studies.* Forthcoming.

2014 Wood, S. et. al. Mobilizing records: re-framing archival description to support human rights. *Archival Science.* 10.1007/s10502-014-9233-1

2014 Kelty, C., Panofsky, A., Erickson, S., Currie, M., Crooks, R., Wood, S., Garcia, P., Wartenbe, M. Seven dimensions of contemporary participation disentangled. *Journal of the American Society for Information Science and Technology*. doi: 10.1002/asi.23202

Book Chapters

2016 Wood, S. Police body cameras: Emotional mediation and the economies of visuality. *Emotions, Technology, and Design.* Ed. Safiya U. Noble and Sharon Y. Tettegah. Elsevier; UK.

2014 Wood, S. Collective Intimacies. *Making Invisible Histories Visible: A Resource Guide to the Collections.* Ed. K. McHugh, B. Johnson-Grau and B. Sher. UCLA Center for the Study of Women.

Book Reviews

2011 Wood, S. Book Review: Narrating from the Archives: Novels, Records, and Bureaucrats in the Modern Age by Marco Codebò. InterActions: UCLA Journal of Education and Information Studies, 7(2), Article 12.

INVITED TALKS

Wood, S. (2017) Police Body Camera Footage: Public Records and Private
Evidence Memory Work, Black Bodies, and Social Justice
University of Michigan Institute for the Humanities and the University of Michigan School of Information

Wood, S. (2015) Classified Information Infrastructure and Archival Concerns
Library and Information Studies Alumni Association Annual Colloquium
University of California Los Angeles Department of Information Studies

RECENT CONFERENCES AND WORKSHOPS

Wood, S. (2017) Citizen Documentation and Police Body Cameras. Paper presented at the Personal Digital Archiving Conference.

Wood, S. (2016) Un/Natural Silences: Donor Requested Destruction in the Mazer Archives. Paper presented at the American Studies Association meeting.

Wood, S. (2016) Police Body Cameras and the Privatization of the Chain of Evidence. Paper presented at the Conference and School on Authority, Provenance, Authenticity, Evidence (APAE) University of Zadar.

Wood, S. (2016) Conspiracy Theories and Classified Information Infrastructure. Paper presented at the Summer School on Controversies and Conspiracies, SciencesPo.

Wood, S. (2016) Navigating Public Records Law and Police Body Camera Evidence. Paper presented at the Archival Education Research Institute, Kent State University.

Wood, S. and Cifor, M. (2016) Critical Feminism in the Archives. Paper presented at the Archival Education Research Institute, Kent State University.

Introduction

"Doesn't the act of noticing matter as much as what's noticed?" – Harry Mathews, The Journalist

In a series of documents declassified and released by James Clapper and the Office of the Director of National Intelligence in November of 2013, one might have noticed a few curiosities with respect to redaction. A number of them had their dates of filing and signing redacted, including a document signed by Reggie B. Walton, a judge of the United States Foreign Intelligence Surveillance Court. This particular ruling document exposed some of the persistent mistakes and challenges presented by managing information across agencies, platforms, standards and contexts. Firstly, although the date was redacted in the released document itself, the date of the ruling remained in it's URL. Additionally, the document had already been declassified and released with entirely different redactions. Adobe's Portable Document Format (PDF) has consistently presented challenges for redaction with government officials and contractors alike. In a filing for a lawsuit over AT&T's alleged compliance with the warrantless wiretapping program of the National Security Agency (NSA) in 2006, a redacted PDF contained text underneath the redactions that anyone could read by selecting the text and copying it into Microsoft Word. This document, presented in Hepting, et al. v. AT&T, 439 Supp. 2d 974 (N.D. Cal. 2006), listed a multiplicity of possible reasons for AT&T's use of a secret switching room that was designed with the capability to monitor telephone calls and internet transmissions. To make matters more absurd, this PDF "accident" occurred just a few months after the NSA published the guide "Redacting with Confidence: How to Safely Publish Sanitized Reports Converted from Word to PDF."[1]

[1] National Security Agency. (2005) *Redacting with Confidence: How to Safely Publish Sanitized Reports Converted from Word to PDF.* Report #1333-015R-2005. Ft. Meade, MD: National Security Agency.

In setting forth to define and analyze the sites, systems, objects and discourses that enable the creation, maintenance, management and destruction of classified information, this dissertation attempts to hold still the moving target of official secrecy as it functions at the federal level in the United States. These mistakes and accidents make visible the complexities of managing massive interconnected systems that rely on radically different levels of technological literacy, institutional norms that might be at odds, and incompatible standards or challenges of interoperability, just to name a few challenges. Attempting to define the infrastructure of classified information, this work is concerned with the operations that result in a particular kind of record, and how shifting technological arrangements affect those records. Classified information has predominantly been understood as representing an absence of information and an absence of content. This dissertation seeks to situate classified information as something other than what Peter Galison has called an "anti-epistemology,"[2] and in fact contends that classified information is a generative category of information. Replacing the question "what don't we know" with "what does it do" allows us to move beyond considering government structures as "institutional frames"[3] within which document production and transmission occurs, and instead fosters an understanding of the immensely productive and formative qualities of a vast infrastructure.

This dissertation responds to the research need for the study of classified information infrastructure within the context of Information Studies by demonstrating the centrality of infrastructural layers for creation and maintenance of records; for the formation of knowledge communities; for the evaluation of evidence; and to ongoing challenges presented by networked information to access, use and preservation. It utilizes a research framework for studying

[2] Galison, P. (2010). Secrecy in three acts. *social research*, 941-974.
[3] Wolter, U. (1995). Institutional frames. *Recent Trends in Data Type Specification*, 469-482.

complex, infrastructural, socio-technical arrangements and the records they produce. This framework has four elements: (1) Standards, (2) Economies, (3) Ruptures, (4) Cultures. Employing techniques and methods from infrastructure studies, media studies and archival studies, it illustrates the generativity of classified information infrastructure. In turn, it exposes the material conditions and restraints of classified information as networked records that present epistemological and political challenges for archival functions such as transparency and accountability, and challenges to archival principles such as creator or fonds.

Secrecy and Bureaucracy

Secrecy, when applied to government affairs, tends to be held in contrast to openness and transparency. Claire Birchall traces the roots of transparency movements within the United States in the tenets of liberal democratic concepts of the public sphere, and critiques its alliances with the neoliberal values of individualism and voluntary regulation.[4] These debates correspond to activist engagements in Archival Studies which contrast the liberal ethos of open access with cultural protocols emerging from different systems of value.[5] The rhetoric of transparency and accountability from within the United States government perpetually characterizes secrecy as a balancing act, a necessary evil that holds certain classes of information secret to temper their potential harm or their volatility. Dennis Thompson has characterized this balancing act as something like the Heisenberg uncertainty principle as it applies to information, the ability of the citizen to evaluate a policy or process would itself disturb that policy or process.[6] The rhetoric of transparency conceives of something as either secret or transparent, however secrecy functions in

[4] Birchall, C. (2011). Introduction to ‘Secrecy and Transparency’ The Politics of Opacity and Openness. *Theory, Culture & Society*, *28*(7-8), 7-25.

[5] Withey, K. C. (2012). Does information really want to be free? Indigenous knowledge systems and the question of openness.

[6] Thompson, D. F. (1999). Democratic secrecy. *Political Science Quarterly*, *114*(2), 181-193.

multiple ways. With respect to government secrecy, its functionality relies on what Braditch has referred to as the "spectacular deployment of secrecy."[7] This picks up on one of the features of secret in its etymological history, that secrets are forever active, they require maintenance and their status only remains secret when we name them as such, "…take concealment, or hiding, to be the defining trait of secrecy."[8] There is no natural relationship between the contents of a secret and its status as secret.

State secrets require a substantial apparatus and infrastructure to maintain their protected status. Because these secrets are not typically unidirectional but implicate different adjacent hierarchies and knowledge communities, their status must be legible and recognizable. For their status to remain acceptable by a public invested in the politics of liberal democracy and accountability, these secrets must also be legible and visible outside of their institutions of origin. The moment of revelation is just as important as their original classification, because the contents are assumed to justify their previous hidden-ness. Classified information infrastructure then is the public means by which the state creates and maintains secrets. Justifications and revelations perform the balance between the assumption that the first amendment is meant to foster and protect the access of the public to information necessary for engagement in public debate, and the notion of national security. Temporal constraints and considerations are integral elements of Executive Orders dealing with classified information. These constraints structure relationships between agencies, information seekers and the information itself while serving an ameliorative function, positioned as a necessary barrier between secrecy and public access to information. References to specific and even general temporal markers within Executive Orders act as an appeal to normative, shared symbols of accountability and stability, as well as creating

[7] Bratich, J. (2006). Public secrecy and immanent security: a strategic analysis. *Cultural Studies*, *20*(4-5), 493-511.
[8] Ibid.

a persistent state of information control through the development of infrastructure that transcends individual agencies, practices and behaviors. As legal documents that derive their justification from Constitutional powers, Executive Orders represent breaks from or expansions of legal precedent, a legal manifestation of temporal inertia. Justification for the entire classified information infrastructure has relied on assumptions about the future uses or potential uses of information, from its roots as a specific and somewhat narrowly conceived piece of military strategy to its present day status as a piece of sprawling totalizing information policy. As the apparatus became more elaborate and the enumerative powers became more detailed, temporal constraints and benchmarks for the status of classified information followed suit. Descriptions of the imagined future uses or potential uses of information, however, remain similarly pointed in the causal relationship between information and eventual harm. Classified information then always already contains within it an accompanying time based omen about its potential uses as well as its eventual uselessness. The status of its potential for risk is linked to contingent political and military contexts, most pointedly expressed by the term "declassifying event."[9] This declassifying event signifies the end of the information's sensitivity and thus its usefulness strategically. The declassifying event could be anything, but it is important to acknowledge that the bureaucratic language that dominates legal documents such as Executive Orders allows for the transformation of violent acts into the euphemistically benign "declassifying event”; to say nothing of the tension between the strategic usefulness of information and its life as public or historical knowledge.

Temporal resources in this instance are not just the future, past and present, they invoke their imaginative properties, all oriented around the potential for disaster or, as the differentiated

[9] Brooks, N. (2006). The Protection of Classified Information: The Legal Framework. *National Security Issues*, 139.

justifications for the classes of information imply, oriented around the potential for grave damage, serious damage or simply damage. In much of his more recent work, David Hoy[10] has discussed elements of Foucault's work on disciplinary regimes and power, highlighting how mechanisms for discipline (both from the state as well as from the self) rely on a shared concept of the future. This future orientation can be expressed in utopian terms of peace or those of a deterrent alternative, either way the future is shared and requires a "constant disciplinary state of becoming" stemming from both the logic and language of its imagination.[11] *In A Thousand Plateaus*, Deleuze and Guattari characterize every secret as a collective assemblage, a project that requires constant social reproduction and a shared sense of what is, can, should or cannot be known.[12]

The history of archives and archival work cannot be disentangled from the history of bureaucratic organization in general, and the role of secrecy in bureaucracy has represented a challenge to goals of citizen access to both contemporary and historical information. Critiques and concerns about the overreach of government secrecy have accompanied each subsequent expansion of the classification system. As early as 1956, the Defense Department Committee on Classified Information issued a report stating that “overclassification has reached serious proportions,”[13] and concerns that classification was having consequences outside of its original intent, such as undermining transparency and inter-agency cooperation or assisting in covering up abuses and mistakes.[14] In 1958, Max Weber outlined the characteristics of an “ideal type” of

[10] Hoy, D. C. (1981). Power, repression, progress: Foucault, Lukes, and the Frankfurt school. *Triquarterly*, *52*, 43.

[11] Costas, J., & Grey, C. (2014). The temporality of power and the power of temporality: Imaginary future selves in professional service firms. *Organization Studies*, *35*(6), 909-937.

[12] Deleuze, G., & Guattari, F. (1987). A thousand plateaus.

[13] DEF. DEP'T COMM. ON CLASSIFIED INFO., REPORT TO THE SECRETARY OF DEFENSE BY THE COMMITTEE ON CLASSIFIED INFORMATION 6 (1956), available at http://www.thememoryhole.org/foi/coolidge-committee.pdf

[14] Report of the commission on Protecting and Reducing Government Secrecy, S. Doc. No. 105-2 (1997).

bureaucratic organization. A bureaucracy is hierarchically organized, and is oriented around shared and standardized rules that govern operations. In addition it is dependent upon technical prowess and continuity.[15] He also draws an explicit connection between bureaucratic institutions and their investment in secrecy, both official and unofficial, framing secrecy as a form of regulation. Sarangi and Slembrouck assert that these basic features of bureaucracy necessarily rely on information exchange,[16] as management of people is done by proxy through information about them and interactions between citizens and public bureaucracy is dependent upon processes of information seeking and exchange.

The expansion of the classified information system represents a form of bureaucratic path dependency,[17] which assumes that once an institution of a certain size establishes a standard, the institution will grow, expand and contract according to that particular path barring some kind of disastrous fall into dysfunctionality.[18] This path then acts as the path of least resistance, a primary characteristic of the dispersed agency that characterizes bureaucratic processes. Authority then lies in the daily reproduction of individual functions, the maintenance of the path. The growth of bureaucratic forms of government that characterized the development of states throughout the 19th and 20th centuries relied on the ability to function across micro and macro levels in a standardized way. The contemporary disparaging of the usage of bureaucracy, as both Kafka and DuGay[19] pointed out, exists alongside this proliferation of processes and

[15] Weber, M.(1958). Bureaucracy. In H.H. Gerth (translated). From Max Weber: Essays in Sociology. New York: A Galaxy Book.

[16] Sarangi, S. and Slembrouck, S. (2014) Language, Bureaucracy, and Social Control. New York: Routledge.

[17] Mahoney, J. (2000) Path Dependency in Historical Sociology, Theory and Society, 29, 507-548.
Peters, B.G. (2006) Path Dependency and Public Sector Reform, Paper presented at conference on Path Dependency Theory, Roskilde University, Denmark.

[18] Peters, B.G. (2009) The Politics of Bureaucracy: An Introduction to Comparative Public Administration. 6th Ed. New York: Routledge.

[19] Kafka, B. (2012) The Demon of Writing: Powers and Failures of Paperwork. Cambridge: MIT Press.
DuGay, P. (2000) In Praise of Bureaucracy: Weber – Organization – Ethics. London: Sage.

idiosyncrasies. However, David Graeber reminds us that while these processes might multiply to the point of absurdity, an essential element of their success is the persistent possibility of violence from the state itself to regulate and punish noncompliance, which is meted out along lines of racial, sexual, gender and class privileges.[20] What makes classified information infrastructure distinct as a form of regulation and organization is that it is a system of information organization with explicit threat as both its justifying cause and its system of enforcement.

The work bureaucracy brings to mind a world of paper, containers, stamps and organizational aids, forms in triplicate and the expectation of deferral, a slow moving process anathema to efficiency. While the association of bureaucracy with paperwork is strong in the popular imagination, scholarly investigations into the relationship between documents and bureaucracy are relatively few. In his review of anthropological literature concerning bureaucracies, Matthew Hull[21] points to several reasons this could be, including that anthropologists as researchers produce an abundance of documents themselves and as such do not confer specialized status onto them. He also addresses the "container" assumption, that documents are simply a way of communicating their contents, rather than having meaning in their material specificity. David Graeber also points out that paperwork is boring, a stand in for tedium.

Studying the state, however, as Philip Abram's aptly titled essay demonstrates, is difficult, namely because it is particularly invested in keeping certain aspects of its work

[20] Graeber, D. (2015) The Utopia of Rules: On Technology, Stupidity, and the Secret Joys of Bureaucracy. New York: Melville House.

[21] Hull, M. (2012) Documents and Bureaucracy. The Annual Review of Anthropology. Vol 41, 251-67.

hidden.[22] One element of the broadly based justification for this hidden-ness is the public interest or public good, that the individual need for information or access is outweighed by the commitment to the whole. In his description of these difficulties, Abrams has a radical proposition, that they are just as much a product of researchers as the state itself. Possibly, he suggests, there is no such thing as "the state" and we have but to refuse "the legitimating account of it that political theorists and political actors so invitingly and ubiquitously hold out to us."[23] This power then is an ideological one, one that gets reproduced through processes and "illusory common interest"[24] To bring together Hull and Abrams, the key to studying the state as it presents itself is to study the processes that bolster its cohesiveness. If documents and information exchange are an integral part of how interactions with the public bureaucracy of the state occur, understanding the expression of state power requires attention to these processes and the layers of hiddenness implied by the general work of state power and the explicit work of classified information; infrastructure requires not just attention to processes but also to structure.

Processes and structure mutually reinforce one another, establishing and justifying shared stakes and identity. In this way, this dissertation also argues that classified information infrastructure operates as a form of cultural technique. Geoffrey Winthrop-Young has traced three different emergent uses of the term cultural techniques ranging from its initial deployment as an agricultural term borrowing from the Latin root colere (to cultivate, tend). As a wordrelated to the planning and implementation of agricultural systems, it is through these cultural techniques that land becomes "habitable."[25] The second incarnation of cultural techniques

[22] Abrams, P. Notes on the Difficulty of Studying the State. Paper delivered at the 1977 British Sociological Association. University of Durham.
[23] Abrams Ibid.
[24] Marx, K. and Engels, F. (1965) The German Ideology. London: Lawrence and Wishart. P. 42
[25] Winthrop-Young, G. (2013). Cultural techniques: Preliminary remarks. *Theory, Culture & Society,* 30, 3-19.

emerged as a strategy to contend with new media spaces and technologies, this meaning shares some kinship with another concept, media literacy, which considers ones' own repository of skills and techniques for understanding and inhabiting new and different media. This second formulation most importantly foregrounded the persistent debate concerning the agency of the user pitted against the constraints and affordances of particular media and technologies.

The third, contemporary usage of cultural techniques refers less to a particular set of skills, media or technologies, and instead refers to a "complex technical, social and administrative mediation" process. Cultural techniques erase their own making, their status stands for itself, their operations coalescing "into entities that are subsequently viewed as the agents or subjects running these operations."[26]As a strategy, this strain of thought seeks, through attention to the materialities of technologies and processes, to bring attention to the "constitutive media dependent ontic operations" [27] that underlie our most basic methods of distinction and identification. Cultural techniques do not refer to all of the influences and mechanisms of culture, but are rather self-legitimating and self-referential[28]; in this context we can identify classified information as cultural technique, since classified information is information that is determined to be in need of classification and classification is the process whereby information is determined to need classification. In his description of cultural techniques, Thomas Macho invokes the "technologies of the self" defined by Foucault, curiously ignoring three other techniques by which Foucault claims humans can understand and regulate themselves.[29] Technologies of production, sign systems, power and self are never isolated, instead gaining

[26] Vismann, C. (2013). Cultural techniques and sovereignty. *Theory, Culture & Society,* 30, 83-93.

[27] Winthrop-Young, G. Ibid.

[28] Macho, T. (2013). Second order animals: Cultural techniques of identity and identification. *Theory, Culture & society,* 30, 30-47.

[29] Macho, T. Ibid.

purchase through their interdependence. In his use of Foucault, Macho attempts to bridge the historical (archaeological) mode of Foucault with the material and technical analysis of media archeology. Media cannot arrive spontaneously and ahistorically just as history has to be recognized as a process that happens within and across media technologies.

The cultural technique of classified information requires the acknowledgment of all four of Foucault's technologies. Executive Orders are clearly products of a sign system, expressions of and agents of power, regulatory policies governing and shaping production and constituting particular knowledge communities that produce the self. Just as classified information defines itself in terms of its status as information that needs to be classified, so too do government officials self-identify according to their access to or ability to regulate information, as do members of the public with stakes of varying degrees of intimacy in the revelation or maintenance of classified information. Classified information infrastructure defines classified information, sets its terms and consequences, and justifies its own existence through the creation of shared community stakes.

Research Questions

My dissertation begins by asking three broad research questions:

(1) What are the elements and characteristics of the infrastructure of classified information within the United States federal government?

In order to understand how classified information is produced and maintained by socio-technical arrangements, it is necessary to identify the layers of infrastructures including the standards, devices, platforms, software, network architecture, policy, regulation and professional practices that make classified information possible. Being able to identify these elements both individually and collectively can help understand the challenges and barriers to future archival work with respect to classified information.

(2) How does a material understanding of classified information infrastructure affect archival expectations such as transparency, accountability, description and access of and to archival resources?

Here, I am engaging with specific archival functions and practices. As technologies and policy change, contradict and/or complicate each other, how does this present difficulties for those attempting to preserve and provide access to an evolving historical record?

(3) How does a material understanding of classified information infrastructure challenge evolving definitions of information elements (document, data, metadata, record)?

This question attempts to situate classified information as a category of information that interacts uniquely with shifting definitions from within Information Studies. Elements of information are defined across legislative, organizational and executive documentation and these definitions build on each other as often as they contradict each other. The consequences of this definitional work are myriad, clumsy definitions or exclusive interpretations have often led to legal challenges or overreach.

Method

In this dissertation I use mixed-methods in order to get at the complexity of the interconnected layers of classified information infrastructure. I use methods outlined in infrastructure studies, historical analysis, case study and multi-modal critical discourse analysis to think through a variety of layers and scales of classified information.

Infrastructure has long been defined as a set of physical arrangements or networks that enable, "a collective term for the subordinate parts of an undertaking."[30] The term "critical infrastructure" was introduced with the President's Commission on Critical Infrastructure Protection (PCCIP) in July of 1996 under President Bill Clinton. The PCIIP's 1997 report highlighted increased vulnerabilities for cyber security infrastructures stemming from a growing indistinguishability between commercially available technology and technology used by the government. Their core recommendation sought to increase and strengthen cooperation between the federal government and the private sector. [31] Clinton followed this report with Presidential Decision Directive No. 63, integrating representatives from the private sector into the daily work of critical infrastructure protection.[32] The Directive also called for critical infrastructure preparedness within individual federal agencies specifically and as a broad agenda item by assigning a Chief Infrastructure Assurance Office (CIAO) to each federal agency and setting up a National Infrastructure Assurance Council. The Directive proposed the establishment of the Federal Intrusion Detection Network (FIDNET) in order to detect and respond to cyber attacks and vulnerabilities quickly and flexibly. FIDNET was ultimately abandoned as privacy and inter-agency security concerns were raised and the comparable EINSTEIN program was introduced. Operated through the Department of Homeland Security, the current program, EINSTEIN 3 enlists the aid of internet service providers (ISPs) analyzing federal network traffic.[33]

[30] Infrastructure [Def. 1] n.d. In *Oxford English Dictionary*, Retrieved September 10, 2016 from http://www.oed.com/view/Entry/95624?redirectedFrom=infrastructure&

[31] Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection. October 1997.

[32] The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. White Paper, May 22, 1998.

[33] Privacy Impact Assessment for EINSTEIN -3 – Accelerated. U.S. Department of Homeland Security. April 19, 2013.

The language and priorities of critical infrastructure continued in the text of the USA Patriot Act of 2001, meaning systems and assets "so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[34] If we understand infrastructure to be the subordinate parts of an undertaking, then this new definition that makes some infrastructure critical, also makes the disentanglement of the state and infrastructure a categorical impossibility. In 2013, the Office of the White House Press Secretary released the details of President Barack Obama's Presidential Policy Directive – Critical Infrastructure Security and Resilience [35] which designated critical infrastructure sectors as: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare, information technology, nuclear reactors, transportation systems, and water and wastewater systems. In addition, this policy directive identified improved information exchange and management as a key strategic objective for defending critical infrastructure. The outlining of these critical infrastructure sectors acknowledges the shifting understandings of the boundaries of what can be considered infrastructure. Much like classified information, they are defined in this instance as priorities through future threat. But classified information moves throughout each of these critical infrastructures, operating across agencies and contexts and requiring both coordinated and uncoordinated cooperation through the application of standards and shared technological protocols.

Work in infrastructure studies has enabled researchers to explore and understand technological arrangements used for labor, economic activity, social and cultural connection and

[34] USA Patriot Act of 2001, 42 U.S.C. . § 5195 c – e.

[35] Presidential Policy Directive. Critical Infrastructure Security and Resilience. PPD-21. February 12, 2013.

communication. For this dissertation, the methods most salient are infrastructural inversion[36] and scales of analysis, in order to be able to capture multiple layers of activity and interactivity. Infrastructural inversion proposes a figure/ground switch in which the researcher looks past the product or process that emerge through infrastructure and instead focuses on the structures and activities in their constituent parts. Rather than understanding transportation infrastructure as a series of roadways then, infrastructural inversion would enable the understanding of infrastructure as a series of technical standards, legal constraints, interaction between public and private economies, geographic cultures and habit – everything from the concrete to traffic algorithms work together to make traffic happen. Scales of analysis[37] is an adaptation of Thomas Misa's scales of society analysis by Paul Edwards, in which studying infrastructure at different scales gives one a different vantage point on how infrastructure develops and functions. The micro scale is the individual level, the ways in which an individual operates within infrastructure each day. If we extend the traffic example, this would be a person's daily commute. The meso scale operates at the institutional level, allowing us to capture larger trends across society in small amounts of time. The macro scale captures epochal infrastructural shifts. Historical analysis relies on the interpretation of historical events, documents and processes as a series of negotiated narratives. This method not only asks why and how a particular event occurred, but how and why the evidence we use to understand the event was created. Therefore an attention to the institution, collective or individual that produced a piece of evidence in conjunction with how it was used and how it is now considered are all vital matters of concern.

[36] Bowker, G. C., & Star, S. L. (2000). *Sorting things out: Classification and its consequences*. MIT press.

[37] Edwards, P.N. "Infrastructure and Modernity: Force, Time, and Social Organization in the History of Sociotechnical Systems," Modernity and Technology, T.J. Misa, P. Brey, and A. Feenberg, eds., MIT Press, 2004, pp. 185–225.
Misa, T.J. , "How Machines Make History, and How Historians (and Others) Help Them to Do So," Science, Technology, & Human Values, vol. 13, nos. 3–4, 1988, pp. 308–331

Critical Discourse Analysis is an interdisciplinary methodological approach that understands language as one form of social practice and situates that practice in a web of power relations. Critical Discourse Analysis focuses on the analysis of "opaque as well as transparent structural relationships of dominance, discrimination, power and control as manifested in language."[38]As alluded to earlier in this dissertation, discussions around policy often identify power as unidirectional from the policy document to the effect on the citizen. With respect to information policy, there is the temptation to understand the policy document as having direct and visible results, which may or may not be true. Critical Discourse Analysis attempts to understand the ways in which the more opaque aspects of communication and linguistic expression are co-constitutive of power relations. The core texts at the heart of this study each state an explicit purpose and operate on multiple levels not simply to address a logistical problem or information need, but to create differentiated knowledge communities with varied levels of access, serve as reference for day to day operations, and promote or advocate for particular technologies or techniques, to name a few. As a starting point, this project engages Norman Fairclough's three-dimensional framework for discourse analysis.[39] This involves considering each of the assembled texts[40] at three levels. At the discourse-as-text level, I will explore these texts for emergent rhetorical patterns, recurrent themes and structural elements. These texts are highly formalized and consistent, their structure indicating their intended purpose as well as gesturing to both transparency and legibility. At the discourse-as-discursive practice level, the eco-system of production will be considered. Returning here to previous sections concerning the

[38] Wodak, R. (1995). Critical Linguistics and Critical Discourse Analysis. Verschueren et. Al. 1995, pp. 204-10.

[39] Fairclough, N.and Holes, C. (1995). Critical Discourse Analysis: The Critical Study of Language. Longman.
Fairclough, N. (2001). Language and Power. Longman.
Fairclough, N.(2003). Analysing Discourse: Textual Analysis for Social Research. London: Routledge.

[40] For a complete listing of assembled texts, please see References.

context of this project, one might consider the different intended audience of each document type. While each of the texts assembled are publicly available, the method and logic of their production, dissemination and consumption vary greatly, as do their functionality. This also allows for the consideration of intertexuality not simply between the assembled texts, but also with their explicit stated function, standardization, conventions and resultant forms. At the discourse-as-social-practice level, the features of the assembled texts outlined above come into contact with broad socio-political processes, facilitating historical comparison and exposing key moments of rupture in discourse. My approach to Critical Discourse Analysis also relies on the developments of Wodak, specifically her foregrounding of historical methodologies. [41]

This project requires an extension of Critical Discourse Analysis to include Multi-Modal Critical Discourse Analysis. This method acknowledges the limitations of studying only textual sources and extends analysis to a multiplicity of media objects and artifacts. While Fairclough gets us to the level of understanding the circumstances of production and circulation, it is necessary to move beyond this to include mediation as a critical point of analysis. This is crucial to keeping archival questions in the foreground as media specificity plays a large part in not just the circulation and management of records, but also constrains the mechanisms for and conditions of future use. The infrastructure of classified information does not solely rely on a group of texts but also employs various media and technologies, that may or may not be standardized enabling interoperability and usability. The media involved in marking, transmitting and storing classified information are managed and regulated through information policy. However, within the texts assembled, there are varying degrees of media specificity. Executive Orders and Legislative Acts in general tend to treat media and technologies as generalizable and

[41] Wodak R, ed. 1989. Language, Power and Ideology. Studies in Political Discourse. Amsterdam: Benjamins. Wodak R. 1996. Disorders of Discourse. London: Longman.

abstract, what Lisa Gitelman has referred to as the mistake of treating media as a "unified entity."[42] The media involved in classified information infrastructure are complex objects, acting simultaneously as the means for accessing information and for obscuring it, as the means for signaling its status and signifying its political potentialities. These media and technologies can have the same effect as the genre of the manual, an assumption of both usefulness and transparency that elides their complexities and assumes their status to be nothing more than a vehicle for informational content. The media and technologies of classified infrastructure also present a challenge in the sense that new technological means of communication often become the justification for changing policy. Again invoking Gitelman in her introduction to *Always, Already New*, the approach of this dissertation includes the protocols and normative practices surrounding media as elements of their historical construction. Diplomatic pouches for example are defined by the United States Department of State as "any properly identified and sealed package, pouch, envelope, bag, or other container that is used to transport official correspondence, documents, and other articles intended for official use,"[43] and are considered inviolable by both national and international law.[44] As diplomatic entities, these containers are legally considered, much like embassies, to be a piece of the land and as such only under the jurisdiction of the sovereign nation to which it belongs. The Vienna Convention on Diplomatic Relations contains protocols for marking, storage and transmission and specifies the ways in which one might physically tamper with such a container, but one might imagine how elastic these definitions might be. While I do not contend that media or technology solely "determine our situation,"[45] it is vital methodologically not to abandon media specificity and media history

[42] Gitelman, L. (2006) Always Already New: Media, History and the Data of Culture. Cambridge: MIT Press.
[43] Vienna Convention on Diplomatic Relations (VCDR) Article 25
[44] Vienna Convention on Diplomatic Relations (VCDR) Article 27.3
[45] Kittler, F. (1999) Gramophone, Film, Typewriter. Stanford: Stanford University Press.

in favor of the linguistic alone. In her book *Files: Law and Media Technology*, Cornelia Vismann finds media materiality missing from many scholarly analyses of the law in fictional texts, an attention to the embodied encounters with bureaucracy litter the pages of Kafka and Melville[46]. This is true too across media.

This dissertation uses case study to center a wide-ranging analysis. Case study is appropriate when the boundaries are not clear between the phenomenon and the context.[47] I employed theoretical sampling, as the goal of the study is not comprehensiveness or representativeness but instead, information richness. Cases then are chosen purposefully rather than randomly and illustrative. Case study allows research to focus on processes and allows for the use of conceptual categories that guide research and analysis, allowing analysis to come from pre-existing analytical categories derived from Infrastructure Studies.

Limitations

There are some obvious and not-so obvious limitations to this project. The contours of this dissertation are necessarily shaped by my own limited access to the daily workings of classified information policy and implementation. While I can access publicly available documentation concerning these issues, they are all describing what is essentially an ideal type rather than particular instances. From the Statute down to the Manual, an ideal type of classified information is imagined and dealt with alongside a parallel work, employee and technical environment.

Throughout the process of conducting this project, people have persistently asked me about declassification. As declassification tends to be the forward-facing activity on the part of

[46] Vismann, C. (2008) Files: Law and Media Technology. Trans. Geoffrey Winthrop-Young. Stanford: Stanford University Press.
[47] Yin, R. K. (2013). *Case study research: Design and methods*. Sage publications.

the government and particularly on the part of archives when it comes to secrecy, it is often framed as our only intervention. It is both a boon and a limitation to this project that I have decided to (as much as possible) steer clear of declassification, its protocols and practices so as to remain focused on the making of secrets to begin with.

Roadmap

Through considering the infrastructure of classified information within each of these methodological frameworks, I derived four categories of analysis: standards, economies, rupture and knowledge cultures. In each chapter I consider one of these categories through a juxtaposition of micro, meso and macro layers, focusing on one object or set of documents for analysis within their historical and infrastructural context. The first chapter consider the most recent manual on the handling, marking, transmission and storage of classified information produced by the Department of Defense, published in 2012. In examining this manual within its historical context this chapter seeks to understand the ways in which the Department of Defense itself defines its records, how it attempts to move policy and protocol into organizational action, as well as the historical context of standards development with respect to classified information. The second chapter focuses on emergent economies of classified information infrastructure by zeroing in on a new category of approved mobile telephones, the DMCC-S or Defense Mobile Classified Communication – Secret. The challenges that have forestalled the development of mobile networked telephony in the field that can successfully receive, store and transmit classified information exposes the interconnected layers of infrastructure that both enables and disables the movement of information. The current program emerged within the context of generational economic partnerships between private industry and the federal government. The third chapter engages with a standard trope in infrastructure studies – that infrastructure is most visible upon breakdown. In examining the role of infrastructure in the recent scandal surrounding Hilary Clinton’s private email server during her tenure in the State Department, this chapter considers the role of breakdown and spectacle not just in exposing infrastructure but also its role in its ongoing success. Classified information as a manifestation of legal and codified ongoing secrecy requires a cyclical justification that must remain public. Leaking, mishandling and hacking happen often, but few cases receive sustained and widespread attention, and fewer still are formally investigated or prosecuted. Those cases that do often represent a political and legal flashpoint expose a critical flaw in the system of classified information and reify the rhetorical support behind its daily functioning. The fourth chapter explores the relationship between classified information and conspiracy theory generation and support. Secrecy, as a routine part of government work and the relationship between citizens and the government, plays a role in the formation of knowledge cultures. This chapter foregrounds the knowledge culture that has arisen around a set of documents with disputed provenance that have become integral to conspiracy theories concerning the cover up of UFOs by the United States government. These documents claim authority through the markings and formal qualities that align them with classified information infrastructure and benefit from a culture of generalized acceptance toward government secrecy. They have produced an economy of authentication across ufology circles that simultaneously mimics and critiques traditional modes of authentication. The conclusion of the dissertation is a challenge to think of classified information, and government records in general, infrastructurally and to confront the practical implications of that line of thinking in addition to outlining further work.

Chapter 1: Standards of/and Classification

Introduction

What do we mean by standards within the context of classified information infrastructure? The sheer number of standards involved in large scale networked technological systems would require a work unto itself, and while I can gesture to the complexity of the standards involved in order to create, maintain, transmit and destroy classified information, this chapter will predominantly be concerned with the legal standards and protocols for classified information,, and analyze the most recent training manual for marking and handling classified information produced and disseminated by the United States Department of Defense. Defining precisely what classified information *is* happens at a few different levels, through Executive Orders and Legislative Acts, whereas the standards for the daily work of processing and handling classified information occurs at an organizational level, and through training manuals and certification processes. We can understand these overlapping forms of enunciation as chains of reference, and while the laws governing the classification of information contract and expand rather than progress in a linear way, their current status is always built upon precedent. In his ethnographic work on the Conseil d'Etat, *The Making of Law*, Bruno Latour asserts that we should not view law as "mere wrapping for power relations,"[48] and instead urges us to understand the law as practice. Of course the law does not act unto itself, but requires operationalization. Thinking infrastructurally about law requires us to think about precedent in a broader sense, as a referent to an installed base. For their part Geoffrey Bowker and Leigh Star argued for standards to be considered material and political, emerging from past assumptions that we may or may not have access to and which are patently ubiquitous. [49]This is precisely why

[48] Latour, B. (2010). *The making of law: an ethnography of the Conseil d'État*. Polity. P 141

[49] Bowker, G. C., & Star, S. L. (2000). *Sorting things out: Classification and its consequences*. MIT press.

sometimes standards are hard to see, they are everywhere and typically embedded into the way we think and do things, and in ways that sometimes masquerade as intuitive. Bowker and Star see the key to unmasking this invisibility, this sense of the intuitive, by paying attention to the infrastructure of standards as well as the standards within infrastructure. Thinking in this way also requires an attention to law as a system, which in this case relies on a balance between consensus based (statute) and unilaterally based (Executive Orders) implementation that relies on an incredibly diffuse system of enforcement.

Executive Orders and Legislative Acts

Executive privilege and one of its most persistent manifestations, Executive Orders, are the source of much hand wringing in the current political climate. The Executive Order is routinely rhetorically leveraged against particular presidents as representative of their despotic influence or, conversely, as the action of a strong and decisive leader, often eschewing both the historical precedents that enabled their existence or the consequences of their language and directives. Precise definitions of what an Executive Order can be or has been vary greatly, the majority highlight their administrative and regulatory functions, and ability to craft statements "which are directed to, and govern actions of, governmental officials and agencies."[50] However, Executive Orders are responsible for some of the most profound policies governing civil rights, environmental policies, and privacy rights, which suggests that their strategic and practical value far exceeds their narrow conception as an executive administrative tool. Debates surrounding the validity of Executive Orders are intimately related to debates about executive power and privilege broadly conceived. Although Executive Orders are consistently supported and reaffirmed by the Supreme Court, their status represents ongoing debates about the

[50] Cash, R. (1963). Presidential power: Use and enforcement of executive orders. *Notre Dame Lawyer* 39(1), 44-55.

Constitutional basis for Executive power and the legal precedents that uphold Executive Orders as law.

Article II of the constitution opens with "The executive power shall be vested in the President of the United States of America," and this power is positioned against the independent judiciary and the collective power of Congress as a legislative body. As such, the power of all three branches are constituted mutually, challenged and reinforced by each other. The language of Article I, which described the power of Congress, is far more explicit and specific with regards to the limits and extent of its powers. As a result of this disparate Constitutional foundation, the executive branch "has undergone a process of development by practice and by judicial decision."[51] Logistically speaking, Executive Orders are far simpler to construct than large pieces of legislation and as a result, Congress typically occupies a reactionary position, forcing it to contend with a process that does not submit to the same kind of collective action as Congress must. While Article II is limited in its treatment of enumerated powers attributed to the Executive, the implied powers that derive simply from the vestment of executive power have been debated as everything from a vestment that does nothing but charge the president with maintaining the status quo,[52] to giving the president the ability to take various forms of independent action with or without the support of statute.[53]

There are no specific powers related to the president's ability to have unique access or control over information in the Constitution, these standards have been developed ad hoc through legal precedent and subsequent interpretation. The courts have agreed in several cases broaching the subject, that the President should indeed have both access to information not readily available

[51] Randall, J.G. (1951). Constitutional problems under Lincoln. University of Illinois Press,
35. [52] Fisher, L. (1995). Presidential war power. University Press of Kansas, 21.

[53] Mayer, K. (2001). With the stroke of a pen: Executive orders and presidential power. Princeton University Press, 43.

to the public as well as maintain a role in the management and development of an infrastructure including formalized secrecy.[54] Executive privilege has its genesis in the late 1790s, and has continued to the present day in a series of requests from Congress for access to information that the executive has denied. George Washington refused compliance with requests for information surrounding the failed St. Clair military expedition and the negotiation of the Jay Treaty [55] and Thomas Jefferson denied Congress information in the trial of Aaron Burr. However, the majority of cases that have set the precedent for executive privilege have arisen within the post WWII context, drastically tightening control on the ability of members of the Executive Branch to provide both testimony and documentation to Congress either voluntarily or under subpoena. Presidents Truman and Eisenhower blocked federal employees from testifying regarding internal decision making, conversations or written communications from within the White House itself. Although executive privilege had been asserted for generations, it became an explicitly constitutional issue in United States v. Nixon in 1974,[56] Nixon argued that executive privilege enables the president to refuse the release of information, claiming it is an implied element of Constitutional power vested in the Executive to control sensitive information. In this case the Supreme Court ordered Nixon to release subpoenaed tapes that would eventually shed light on the Watergate scandal. Having struggled since the first presidency[57] to define these boundaries it is a rarity that the courts challenged executive privilege directly.

While government information policy is the domain of all branches of government, the executive has almost singularly defined and set forth the protocols governing classified

[54] New York Times Co. v. United States, 403 U.S. 713, 728 (1971). Chicago and Southern Airlines v. Waterman Steamship Cor., 333 U.S. 103, 111 (1948).

[55]

[56] United States v. Nixon, 418 U.S. 683 (1974).

[57] In 1792, George Washington exerted the first version of executive privilege, refusing to give information to Congress regarding a failed military expedition.

information. Several key legislative endeavors have served to expand and augment the infrastructure of classified information, but the bulk of this infrastructure has been developed, implemented and regulated through executive orders.

The roots of the contemporary classification system can be traced to information control policies developed specifically for the United States War Department during World War I. Modeled on British and French systems of information policy and control, the system implemented by the War Department was the first agency wide system of classification and established the three-tier system (secret, confidential, restricted). With Executive Order 2954 Woodrow Wilson created the Creel Committee, a committee on public information with the authority to limit and disseminate publicity about military activity (later, the Office of Censorship). One of its most significant contributions was a code of wartime practices which identified information, the sensitivity of which required close consultation and subsequent approval for dissemination by government agencies. In the first of a series of Executive Orders that established what would become the elaborate infrastructure that characterizes the contemporary system of classified information, Franklin Roosevelt carefully defined the genres and types of information considered "vital" and therefore potentially subject to classification. The first to explicitly reference materials, Executive Order 8381, names materials such as books and pamphlets as well as their reproductions.

While the classification system is now one of inter-agency coordination with oversight emerging from the National Security Council as well as the Information Security Oversight Office, with Executive Order 9182 the classification system was brought entirely under a single organization, the Office of War Information. Executive Order 10104 (1950) established specific standards for each level of classification and Executive Order 10290 replaced the ad hoc system of widely varying sets of regulation in various departments with a White House controlled centralized system fully centralizing classified information infrastructure and bringing the system under one office. This Executive Order also more broadly alluded to justification, shifting the language from a national defense criteria to a national security criteria which would become the overriding logic of secrecy, balanced against the specter of individual privacy and eschewing larger social structures or collective experience. This brought with it a contraction of reach and an implementation of the first procedure for declassifying documents that no longer warranted protection. For the next several decades, the shift to classification infrastructure would occur outside of the Executive, affected predominantly by two legislative acts, the Atomic Energy Act of 1954 (accompanied by Executive Order 10865 which provided safeguards for classified information within industry) and the Freedom of Information Act of 1967. As a significant amendment to the Atomic Energy Act of 1946, the 1954 Act loosened restrictions on private enterprise related to nuclear energy or fissile materials. While it still upheld strict protocols for information control and its own hierarchical designation system (the highest being restricted data), its amendment signaled a shift in partnerships between contractors, private industry and the government. The Freedom of Information Act was the first legal protection against the abuse of the classification system which, while conceived as a wartime necessity had become a routinized and normative bureaucratic extension of government information management. Executive Order 11652 issued by Richard Nixon attempted to both reduce the level of classification and tighten enforcement of abuses. Reducing the number of agencies and personnel with the authority to classify documents at the "Top Secret" level and requiring quick and standardized declassification schedules, were part of a broader attempt to keep leaks from within agencies and Congress in check. This Order also extended the justification for classification to include the protection of information that had the potential to negatively affect foreign relations. Although the divisions between foreign and domestic information management and gathering are still some of the most contentious, this Order also attempted to bring all classified information, including that concerning diplomatic and foreign affairs, under the umbrella of a unified system.

President Carter continued the trend toward reduced secrecy, employing a stronger standard for classification which relied on 'identifiable damage' to national security and imposed for the first time a balancing test in declassification review requiring agency officials to weigh the public's interest in knowing against the potential damage from release. In an attempt to transcend the protracted struggle for power between Congress and the Executive, Executive Order 12065 was the first to even circulate as a draft to congressional committees seeking public comment and broadly based support. Executive Order 1256 was a drastic change in tone: discarding the balance test for classification; eliminating mandatory declassification procedures, allowing agencies to reclassify previously public information; imposing secrecy requirements on government contractors; and drastically attempting to limit the Freedom of Information Act as much as possible. The basic features of the classification system remained remarkably similar, relying at this point on entrenched protocols and institutional knowledge to mirror the policies of the Executive. Rather than bolster the system with legislation related to scientific knowledge and development, this period was defined by its relationship to Cold War era intelligence practices and methods. Shortly after Ronald Reagan issued Executive Order 1256, Congress passed the Intelligence Identities Protection Act in 1982, making it a federal crime to release or even seek to know the identities of intelligence officers. By 1995 the political tone had changed in the wake of revelations concerning activities of the Central Intelligence Agency throughout the Reagan administration. Attempts to build in safeguards against unitary Executive control over information policy and the tendency to use classification to cover up covert action regardless of sensitivity characterized Executive Order 12958, issued by Bill Clinton in 1995. Requiring the identification of the classifier attached to each classified piece of information alongside a justification, this Order built accountability into the system.

In 2003, the basic outlines of much of classified information infrastructure and its justifications shifted in the wake of 9/11. As legal protections for surveillance and intelligence gathering broadened, the classification process became even more fully entrenched within the Executive office. For the first time, Executive Order 13292, issued by George W. Bush, authorized the Vice President as an original classifying authority. This Order also expanded to categories of classifiable information to include infrastructures and "protection services," relying on ever more vague and flexible language to provide significant latitude for interpretation. The Archivist of the United States, who had heretofore had the role of managing declassified information as well as overseeing the beginning of declassification review processes, lost this power, which instead, was transferred to the Director of the Information Security Oversight Office. Barack Obama's 2009 revocation of this Order in reality maintained much of its language and changes. Executive Order 13526 strikes a different tone in its preamble, which is longer than the average and appeals to a "free flow of information" that must be balanced against the threats of "transnational terrorism." A departure from previous Orders is the creation of the National Declassification Center, which operates from within the National Archives somewhat independently, although still under the oversight of the ISOO and subject to the Interagency Security Classification Appeals Panel (ISCAP). As Executive Order 13526 is the current standard, I will spend a bit of time breaking it down.

Section 6.1 of Executive Order 13526 provides operational definitions for terms contained within the text of the executive order, including everything from “access” to “unauthorized disclosure,” and as these terms are legal terms they may or may not be synonymous with colloquial or other professional or disciplinary use of the terms. For example, the definition of records is stated as referring to “the records of an agency and Presidential papers or Presidential records, as those terms are defined in title 44, United States Code, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency’s control under the terms of the contract, license, certificate or grant.” Glossary and other definitions in government documents often refer the reader to a seemingly endless chain of referents. Instead of just quoting or reproducing the definition of records used in title 44 of the U.S.C., we have here a directive to visit another document. Classification is defined as tautology, as “the act or process by which information is determined to be classified information.” Classified then is an adjective and noun, it can describe the state of information as well as the process by which it is defined as such. E.O. 13526 generally describes two processes, classification and declassification. There are two kinds of classification, original and derivative. The standards for original classification fall back into a familiar tautology, “information can be originally classified under the terms of this order if…an original classification authority is classifying the information.” Further standards include the expectation that there is a reasonable expectation of threat and that the information is the property or under the control of the U.S. Government. This executive order maintains the standard three levels of classification:

(1) “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.

(2) “Secret” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

(3) “Confidential” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe

Each of these relies on the oft repeated “reasonable expectation” justification but also pairs it with the additional expectation of providing evidence of this reasonable expectation. Although the instruction here is vague, it is a key to the authority of classification. If a piece of information is classified, then a citizen might themselves have a reasonable expectation that it was classified as a result of someone identifying and describing a potential threat that is itself reasonable. Classification authority stems directly from the President and Vice-President, and moves down through the agency heads and officials appointed by or designated by the president. Top Secret classification authority stays at that level, whereas Secret and Confidential can also be at the level determined by an agency appointee whose job includes the administration of classified information policy, including regulatory practices and training and oversight. According to the most recent report by the Information Oversight Office (ISOO) published in 2014, there were 2,276 government officials with original classification authority. Together they made 46,800 original classification decisions, 11 percent of which were considered to be Top Secret. Each of these classification designations must be considered part of seven predetermined categories including: military plans, weapons systems or operations; foreign government information; intelligence activities (including covert action), intelligence sources or methods, or cryptology; foreign relations or foreign activities of the United States, including confidential sources; scientific, technological, or economic matters relating to the national security; United States Government programs for safeguarding nuclear materials or facilities; vulnerabilities or capabilities, systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or the development, production, or use of weapons of mass destruction. E.O. 13526 is material and format agnostic, meaning that it avoids referring to particular formats or materials. In fact, it carefully posits that "document" means "any recorded information, regardless of the nature of the medium or the method or circumstances of recording," leaving the determination of specific methods of marking up to agencies heads or other designees rather than providing general guidelines. The guidelines for marking remain at a fairly high level, specifying only that classified information should always contain one of the three classification levels: identity of the original classification authority as well as the agency and/or office of origin; declassification instructions; and a reason for classification. The majority of classified information becomes so due to Derivative Classification, which is the kind of classification that occurs when people reproduce or summarize previously classified information, or who are applying classification markings using a classification guide. In contrast to the numbers we see with original classification, derivative classification occurred over 75 million times in 2014. Those who apply derivative classification must receive training at least every two years, which can occur at the agency level or through external certification organizations. In rare circumstances, senior agency officials can provide a waiver for individuals who cannot participate in mandatory training. In addition, each agency with original classification authority must author a classification guide with an eye towards achieving uniformity and proper application of the standards.

Department of Defense

The United States War Department, the predecessor of the United States Department of Defense, was established by the first Congress in 1789. The War Department acted as the civilian administrative body overseeing the field army, gradually expanding to provide for recruitment and training as well as the administration of medical and financial resources. With each conflict, the powers and responsibilities of the War Department expanded, resulting in fragmentation and confusion concerning authority and accountability. With the War Powers Act of 1941, the Army Ground Forces, Army Air Forces and the Services of Supply were defined, further segmenting operations.

Following World War II, President Harry Truman proposed the consolidation of scattered and disparate military bodies into a single department housed in the Executive branch of the United States Government. Within the context of post-war prosperity, Congress debated the appropriate size and role of the military in American society, culture and political life, in addition to the entrenched struggle over the consolidation of power within the Executive.[58] In 1947, President Truman signed the National Security Act into law, setting up what would later be renamed as the Department of Defense in a 1949 amendment. Alongside Executive Order 9877, President Truman attempted a clear delineation of roles, missions and functions[59] of the military services and civilian command. The National Security Act also established the Joint

[58] Hogan, Michael J. (2000). A Cross of Iron: Harry S. Truman and the Origins of the National Security State, 1945-1954. Cambridge University Press. Pp. 37-38.

[59] A brief note on terminology here. Although these terms are sometimes used interchangeably, they can also act as vital shorthand in official documentation as well. Summarizing from the literature, the clearest differentiation of terms identifies roles as the broad purpose for which the specific body or organization was established. Missions however are more narrowly defined and strategically oriented, missions can span organizational boundaries. Functions remain as the specific and unique means by which an established body fulfills both its roles and missions.

Chiefs of Staff, the National Security Council and the Central Intelligence Agency, among other moves, to both compartmentalize and streamline channels of communication and authority along the chain of command. Centralization would soon become further entrenched with the Department of Defense Reorganization Act of 1958, which situated authority with the Joint Chiefs of Staff and the Secretary of Defense rather than the historical precedent of somewhat independent military departments and command.

The Secretary of Defense acts as the head of the Department of Defense. As this position is appointed by the President, its' authority is a direct derivation of the Constitutional authority of the President as it relates to matters of the military.[60] While the organizational structures shifts, contracts and expands according to the establishment of new subordinate or regulatory bodies, the first major revision of the Department of Defense (DoD) Directive (DoDD) pertaining to the functions of the DoD and its major components was signed by Defense Secretary Robert Gates in 2010. The original founding version of 5200.01 was issued in 1954, and was routinely amended and revisited until 1987, at which point a substantive transformation reflecting shifts in policy orientation and practical challenges occurred. In addition, this revision of the Directive can be partly attributed to the Goldwater-Nichols Defense Reorganization Act passed in 1986.[61]

Itself a result of political fallout and logistical challenges presented by the Vietnam War, the Act responded to a lack of cooperation and communication across the military services.[62] Signed by President Ronald Reagan, it significantly tightened the chain of command, providing for a direct

[60] 10 U.S.C 113

[61] Gaddis, J. L. (2002). A grand strategy of transformation. *Foreign Policy*, 50-57.

[62] Eilon, L. and Lyon J. (2010). White Paper: Evolution of Department of Defense Directive 5100.01 "Functions of the Department of Defnse and Its Major Components" Office of the Secretary of Defense Director, Administration and Management, Organizational Management and Planning. Revised (2014) by Jason Zaborski and Robin Rosenberger.

line from the President through the Secretary of Defense to Combatant Commanders.[63] The Act also considerably reorganized standard operator procedures for military action, reconfiguring them along strategic or geographic lines rather than by resource or expertise. Instead of silos of expertise individually strategizing, United States Central Command (USCENTCOM) would now allocate assets and resources according to objective. In addition, the Act allowed for shared technological and infrastructural resources, encouraging technological interoperability.

A key factor precipitating contention, competition and compartmentalization between agencies and governmental organizations is intelligence. Sharing information across organizational lines presents complex challenges partly due to the intricacies of information policy across levels of government and operations. The Department of Defense presents a unique case in terms of information management and sharing, as it derives its power from the Executive and acts as the clearinghouse for individual intelligence agencies and operations under the military services. The Department of Defense acts as a manager and coordinator of intelligence services, including geospatial intelligence(GEOINT), signals intelligence (SIGINT), human intelligence (HUMINT) and measurement and signature intelligence(MASINT). The Department of Defense also manages, coordinates and maintains the infrastructure for satellite assets in service of the intelligence agencies. A significant amount of information policy is devoted to regulating access to certain classes of information, either regulating the government's access to the information of citizens or, conversely, the citizen's access to government information. However, this statement, and much of the literature concerning access and open government, fails[64] to move beyond this one to one relationship. The assertion that policy dictates access does

[63] Again, note the terminology; Combatant Commanders marks a departure from military specific terminology, a move that acknowledges the increasing use of civilian contractors and extra-military services, characterizing contemporary United States military operations.
[64] Scassa, T. (2014). Privacy and open government. *Future Internet*, *6*(2), 397-413, 408.

not address the thick layers of bureaucratic control and management logic that regulates operations of intelligence agencies and government bodies. By concentrating on the Department of Defense, this research focuses on the space between policy and accessibility, and challenges the direct association between policy and action. Policy in this case, made up of both Executive Order and Legislative Acts, precipitates a series of institutional behaviors and mechanism that proliferate as policies, technologies and organizational structures shift. The relationship of record as command delineated by Cornelia Vismann,[65] and recently expanded by the scholarship of James Lowry,[66] involves not simply the production and circulation of the record itself, but also relies on a series of human activities and material practices as outlined by internal directives, manuals and instructions. The documents produced by the Department of Defense relating to information policy and control produce the very classes of information for which policy documents call.

The current organizational chart (Appendix B) for the Department of Defense illustrates its role in terms of operations and management. Chief Information Officer Terry Halvorsen, along with David De Vries, Principal Deputy Chief Information Officer, and Christopher E. Thomas, Administrator of the Defense Technical Information Center, are the principal information officers within the DoD shaping the ways in which policy becomes instrumentalized across the bureaucratic structure of the agency. Terry Halvorsen acts as the principal adviser to the Secretary of Defense concerning Information Management, Technology, and Assurance, as

Gasco-Hernandez, M. Ed. (2014) Open Government: Opportunities and Challenges for Public Governance. New York: Springer.
Peled, A. (2011) When Transparency and Collaboration Collide: The USA Open Data Program. JASIST. Vol. 61, 2085.
Gurstein, M. (2011) Open Data: Empowering the Empowered or Effective Data Use for Everyone? First Monday.

[65] Vismann, C. (2008). *Files: Law and Media Technology.* Trans. Geoffrey Winthrop-Young. Stanford: Stanford University Press.

[66] Citation forthcoming

well as infrastructure, including telecommunications, satellite communications, navigation, timing programs, and non-intelligence space systems. David De Vries also supports the Chief Information Officer. Christopher E. Thomas operates with a different mandate, as the Administrator of the Defense Technical Information Center (DTIC), his mission is to coordinate science and technology information (STINFO) policy across agencies for the Department of Defense. He is also the Chief Technology Officer for the DTIC and oversees the DTIC's operation of the DoD's Information Analysis Centers. During his tenure, DoDTechipedia was unveiled, allowing DoD scientists and researchers to share information and data within the Unclassified but Sensitive Internet Protocol Router Network, formerly the Non-secure Internet Protocol Router Net (NIPRNET), and the Secret Internet Protocol Router Network (SIPRNet).

The Information Security Oversight Office (ISOO)

Although professional archivists and archival scholars across the United Sates have been and are engaged in advocacy concerning issues of secrecy and access, there remains a division between the archival community in general and the National Archives specifically. The National Archivist is an appointed position and may or may not be someone with archival experience. The arm of the National Archives responsible for standardizing and assessing the "management of classified and controlled unclassified information through oversight, policy development, guidance, education, and reporting" is the Information Security Oversight Office, which acts as the liaison between accessions from agencies to public use and/or storage in the archives.[67] They are also responsible for the education and training of the agencies with respect to information security. The ISOO also deals with regulatory functions and sees to appeals; contained within the ISOO are the Interagency Security Classification Appeals Panel (ISCAP), the National Industrial

[67] Presidential Libraries also work with agencies on an individual basis on declassification.

Security Program (NISP), the National Industrial Security Program Policy Advisory Committee (NISPPAC), the Classification Management Working Group (CMWG) and the State, Local, Tribal, and Private Sector Policy Advisory Committee (SLTPS-PAC). The director of the ISOO is also the acting executive for the ISCAP. Established with Executive Order 12958, ISCAP acts as an intermediary and appeals to authority for classification challenges, exemptions from declassification protocols and declassification requests.

Established in 1978 by Executive Order 12065 and signed by President Jimmy Carter, the ISOO was meant to replace an Interagency Classification Review Committee (ICRC), itself established through Executive Order in 1972 by President Richard Nixon. The ICRC was assembled by representatives from various departments and commissions acting on behalf of their particular constituencies, whereas the ISOO was meant to act as an independent office enacting oversight and mediating interagency issues and disputes. John P. Fitzpatrick is the current Director of the Information Security Oversight Office, his explicit mandate being to both adhere to executive commitments to openness and transparency in balance with the protection of information vital to 'national security.'

The Manual as Genre

The oldest known manual can be traced back to the Sumerian civilization, approximately 1375 B.C.E. The text is inscribed on clay tablets by Kikkuli, the squire of the King of the Hittites Suppiluliuma and outlines the proper care and training of horses.[68] The program is outlined in detail, setting forth standards for ration amounts; periods of rest and training schedules; and creating standard regimen across a burgeoning military force increasingly reliant upon horses. The text has become a boon to researchers interested in a multitude of subjects, but also provides

[68] RAULWING, P. (2009). The Kikkuli Text. Hittite Training Instructions for Chariot Horses in the Second Half of the 2nd Millennium BC and Their Interdisciplinary Context.

insight into an antecedent of a genre typically associated with bureaucratic organizational structure, professionalization or personal technology. While the manual is a genre of organizational communication it is also characterized by a "socially recognized communicative purpose and common aspects of form."[69] Rather than represent individual communicative practices, a genre in this sense operates within a community, formally defining a set of common priorities and reinforcing cohesion.[70] The commonly understood purpose of a training manual is to train, to teach and to inform a constituency of how to perform a particular set of skills in a standardized fashion. In this way, changes in organizational policies and priorities can be communicated consistently, and all members of the organization can share a common referent. While organizations function within a genre repertoire,[71] rather than relying on a single communicative or document genre, the manual serving as a reference text positions it as a more static genre compared to a memo or single task related document. Additionally, manuals are meant to simplify. Typically, a genre has characteristic and recognizable form, and relies on a shared sense of both understanding and purpose. However, manuals are also dynamic[72], they do nothing on their own. In order for them to function, you must already possess a great deal of knowledge about the subject, and must identify either externally or internally as a member of a specialized community of knowledge and practice. Crucially though, manuals are also meant as reference texts to be consulted rather than wholly internalized, and apart from initial training are typically sought out when an individual recognizes a gap in their own knowledge or confront an issue on which they need guidance. Guides for dealing with classified information are many and

[69] Yates, J., & Orlikowski, W. J. (1992). Genres of organizational communication: A structurational approach to studying communication and media. *Academy of management review*, *17*(2), 299-326.
[70] Manuals are not the only information genres that achieve this purpose.
[71] Orlikowski, W. J., & Yates, J. (1994). Genre repertoire: The structuring of communicative practices in organizations. *Administrative science quarterly*, 541-574.
[72] Gitelman, L. (2014). *Paper knowledge: Toward a media history of documents*. Duke University Press. P. 2.

are produced by agencies themselves, external training services and offices. An individual worker who may deal with classified information incidentally or infrequently might have three manuals and sixteen laws governing her behavior, and internal audits have found consistently that training on these issues is minimal and ineffective.[73] However, the distribution of the manual fulfills the minimum requirements set forth by law, that agencies train and inform their employees of proper protocols, and can more often be a tool of indemnity rather than knowledge or skill transfer. Manuals maintain a curious relationship to what Michel Foucault has called the "author function."[74] Foucault writes that an individual author's name "manifests the appearance of a certain discursive set and indicates the status of this discourse within a society and a culture,"[75] and sets authored texts apart from anonymous texts, guarantors and other more remote entities. This concept of author arises as texts are placed within complex economies, apportioning both responsibility and ownership over particular ideas and discourses. The author itself is a subject position constituted in relation to the author-function. Although outside of the literary debate between Barthes and Foucault[76] concerning the function and role of the author in postmodernity, manuals offer a unique test case for disrupting the boundaries of authorship and discursive position. Manuals rely on an author-function that transcends the particularities of their writing and instead identifies a broader entity as author, in this case a particular government agency. The agency's author-function activates the text as discourse that communicates not just

[73] United States Department of State Office of Inspector General. (1999). *Security and Intelligence Oversight Audit: Protecting Classified Documents at State Department Headquarters.* SIO/A-99-46.
United States Department of State and the Broadcasting Board of Governors Office of Inspector General. (2013) *Evaluation of Department of State Implementation of Executive Order 13526, Classified National Security Information.* AUD-SI-13-22.

[74] Foucault, M. (1979). *What is an Author?*. na.

[75] Foucault, M. (1979). *What is an Author?*. na.

[76] Barthes, R. (1994). 11 The Death of the Author. *Media Texts, Authors and Readers: A Reader*, 166.

its position as an extension of executive power but as a mandate for individual responsibility of agency employees, a real explication of bureaucratic and legal power as practice.

Standards in Action, a Proliferation of Training and Instruction Manuals

The current Department of Defense Manual Number 5200.01 Volumes 1-4 were published in 2012[77] and comprise the most comprehensive overview of the classification program, its authorities and currently sanctioned practices with respect to classified information. Each of the four volumes has its own purpose: Volume 1 provides an overview of the DoD Information Security Program; Volume 2 outlines the methods and standards for marking classified information; Volume 3 outlines means of the protection of classified information; and Volume 4 deals exclusively with a category of information called "Controlled Unclassified Information." In its entirety it contains three hundred and sixty-two pages, each volume containing its own glossary in order to decipher not only acronyms but to act as a guide to organizational priorities and structure. The glossary is an extension of the stated purpose of each volume of the manual, and gives a broad picture of the ways in which classified information is placed at the center of overlapping discourses concerning United States "national security." National Security runs throughout these documents, performing multiple functions as it has in policy discourse for the last several decades. The National Security Act[78] was passed in 1947, embedding a nebulous concept of national security into foreign policy. The Act created the National Security Council, the Central Intelligence Agency and the precursor to the DoD.

[77] Department of Defense. (2012) *DoD Information Security Program: Overview, Classification and Declassification*. 5200.01, Volume 1.
Department of Defense. (2012) *DoD Information Security Program: Marking of Classified Information.* 5200.01, Volume 2.
Department of Defense. (2012) *DoD Information Security Program: Protection of Classified Information.* 5200.01, Volume 3.
Department of Defense. (2012) *DoD Information Security Program: Controlled Unclassified Information (CUI).* 5200.01, Volume 4.

[78] National Security Act of 1947, 50 U.S.C. 3002

However, the Act did not define what it meant by national security, leaving it as a broad umbrella under which to house any conceivable threat. In an essay entitled "The Legitimate Claims of National Security," General Maxwell Taylor outlined an expansive vision of national security:

> The national valuables in this broad sense include current assets and national interests, as well as the sources of strength upon which our future as a nation depends. Some valuables are tangible and earthy; others are spiritual or intellectual. They range widely from political assets such as the Bill of Rights, our political institutions and international friendships, to many economic assets which radiate worldwide from a highly productive domestic economy supported by rich natural resources. It is the urgent need to protect valuables such as these which legitimizes and makes essential the role of national security.[79]

These manuals reflect the priorities and ideologies expressed in President Barack Obama's National Security Strategy. [80] Obama emphasized security as one of four enduring national interests, which when considered together conceptualize a totalizing brand of American exceptionalism that places U.S. interests at the heart of international peace and security and asserts the U.S. as a protector of universal values. By describing these four interests as inextricable, Obama ties activities justified with national security rhetoric to each of these other priorities. Interestingly, the DoD manual itself defines national security along much more narrow lines as "the national defense or foreign relations of the United States. National security includes defense against transnational terrorism."[81] Although this definition is narrow in the glossary, it is deployed as the primary justificatory principle throughout the manuals, suggesting a larger ideological footprint than defense and terrorism. The manuals also invoke prior authorizing bodies and documents through a comprehensive list of references to directives, memos, statutes,

[79] Taylor, M. D. (1973). The legitimate claims of national security. *Foreign Aff.*, *52*, 577.

[80] Obama, Barack (2010) National Security Strategy. Office of the President of the United States, White House. P. 17

[81] Department of Defense. (2012) *DoD Information Security Program: Overview, Classification and Declassification*. 5200.01, Volume 1. P. 80.

executive orders, instructions and of course, other manuals. Volume 3 references 63 of these documents alone. These manuals take as their overriding precedent Executive Order 13526 which attempts to set broad standards for a "uniform system for classifying, safeguarding and declassifying national security information, including information relating to defense against transnational terrorism."[82] The language of the Executive Order couches this goal within a larger system that purportedly aligns "democratic principles" with a generalized prioritization of freedom of the circulation of and access to information. Classified information is then defined as extraordinary, an exception to routine practices. Additionally, the application of uniformity throughout this document and its proliferating manuals, directives and instructions are framed as another mechanism for ensuring transparency and accountability of government activities. The Executive Order is divided into six parts: original classification; derivative classification; declassification and downgrading; safeguarding; implementation and review; general provisions. Original classification identifies the entities that possess classification authority as well as provides a framework for determining what exactly should be classified. Again, this determination is framed in broad terms relying on a generalized investment in national security as a governing principle. The very foundations for considering information classifiable rely on a stated understanding of this principle, "Information shall not be considered for classification unless its authorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security…"[83] In addition to reaching the nebulous standards of identifiable and describable, the information must also pertain to at least one of the following things: military plans, weapons systems, or operations; foreign government information; intelligence activities, sources and methods; foreign relations or foreign activities of the United

[82] Exec. Order 13526. 75 C.F.R. 707 (2009).

[83] Exec. Order 13526. 75 C.F.R. 707 (2009).

States; scientific, technological, or economic matters relation to national security; United States Government programs for safeguarding nuclear materials or facilities; vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to national security; or the development, production or use of weapons of mass destruction.[84] Volume 1 of the manual is a much more detailed description of principles outlined in the Executive Order including descriptions of who can possess Original Classification Authority (OCA), how they can get it and the procedures for applying for exemptions to automatic declassification. This Volume also includes guidance on the production and circulation of the manuals themselves. E.O. 13526 requires Agency heads to provide guidance as well as periodically review the guidance they produce regarding classified information. The manual specifies this review as every 5 years and requires their classification guides to be distributed to organizations covered by the guide. Each published piece of classification guidance must also be sent to the Defense Technical Information Center as long as the guide does not itself contain any proprietary or classified information. DTIC then indexes and provides online, searchable access to the guides.

Volume 2 provides granular instructions for marking classified information. This goes beyond general markings and extends into even more specifically formed and regulated communities of information. Apart from generalized categories of classified information, there are two additional areas in which further protocols and standards are outlined: Special Access Programs (SAPs) and Intelligence Information. The Intelligence Community (IC) has developed its own specific standards of classification and control through the IC Directive (ICD) 710, "Classification and Control Markings System," which is issued by the Office of the Director of

[84] Exec. Order 13526. 75 C.F.R. 707 (2009).

National Intelligence (ODNI) in conjunction with standards outlined by the Special Security Center (SSC), Controlled Access Program Coordination Office (CAPCO), and the CAPCO Register and Manual for guidance on marking and dissemination of classified and unclassified intelligence information. These IC designations are included in the banner line along with the prevailing classification level. For example, a Top Secret intelligence document might say in the banner "TOP SECRET/IMCON," which signifies that it is considered Top Secret as an original classification and has the additional control standard of "Controlled Imagery," which governs sources and methods used by geospatial intelligence.[85] As this manual is specifically concerned with the application of uniformity prioritized by E.O. 13526, this section is perhaps its most vital component. It provides a comprehensive and uniform guide to control markings. Information control (nee) bibliographical control has long been a central concern to those in Information Studies. In his foundational essay "Two Kinds of Power," Patrick Wilson explores the conceptual challenges of bibliographic control as a distinct practice. He posits bibliographic control as a form of power and in fact, a kind of power over power, given the assumption that knowledge somehow leads to power itself. [86] As a functional term, control then is something that we can implement over a set of resources. The relationship between control and organization, which Wilson describes as contingent instead of necessary, comes to the fore in classified information. We might see the infrastructure of classified information as operating within the transitional space identified by Gilles Deleuze in his essay "Postscript on the Societies of Control."[87] In this essay, Deleuze describes what he sees as the transition of society from a Foucauldian disciplinary one to one of control, meaning that previous, formally controlled spaces

[85] Department of Defense. (2012) *DoD Information Security Program: Marking of Classified Information.* 5200.01, Volume 2.

[86] Wilson, P. (1968). *Two kinds of power: An essay on bibliographical control*. Univ of California Press.

[87] Deleuze, G. (1992). Postscript on the Societies of Control. *October*, *59*, 3-7.

are broken apart, and power is reconstituted through perpetually moving barriers and mechanisms of control. Within government information environments, classified information operates as a mechanism of control. Control here facilitates ease of communication within close information communities, control markings signaling immediately to the reader whether or not they are allowed to go forward and read. This form of control fundamentally requires everyone to agree to its terms and act accordingly, and access and boundaries can shift at any point. In terms of classified information, control is multi-directional, operating through detailed protocols within government environments and outside of government information environments. Analyses and understandings of control proliferate across disciplinary and professional boundaries. James Beniger's book, *The Control Revolution: Technological and Economic Origins of the Information Society*,[88] posits control at the heart of all economic and social behavior through the 21st century. Control permeated the strategic and rhetorical registers of the United States military and cybersecurity. "Command and control" has become a stock phrase across agencies with multiple definitions. The Department of Defense Dictionary of Military and Associated Terms define command and control as "the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission."[89] A 2006 report expanded this definition to include: establishing intent (the goal or objective); determining roles, responsibilities, and relationships; establishing rules and constraints (schedules, etc.); and monitoring and assessing the situation and progress.[90] This

[88] Beniger, J. (2009). *The control revolution: Technological and economic origins of the information society*. Harvard university press.

[89] Command and Control [Def.1] n.d. In DoD Dictionary and Terminology Repository. Retrieved February 12, 2017.
http://www.dtic.mil/doctrine/dod_dictionary/data/c/3226.html

[90] Alberts, D. S., & Hayes, R. E. (2006). *Understanding command and control*. ASSISTANT SECRETARY OF DEFENSE (C3I/COMMAND CONTROL RESEARCH PROGRAM) WASHINGTON DC. P. 35

report situates these traditional mechanisms of command and control as problematic within the "Information Age," which requires flexibility of ability and authority to make immediate decisions while maintaining a consistent intent across entities. The relationship between networked communication and information hierarchies that characterize traditional bureaucratic and military structures is consistently figured as a crisis. Although there is debate concerning the exact time-period of its writing, Sun Tzu's *The Art of War*[91] is considered the oldest manual for war strategy. The gathering, dissemination and control of information is at the heart of the text, as the key to maintaining advantage and avoiding violence. The text contains specific instructions for intelligence gathering and deception. Although he does expose techniques and describe the centrality of strategy, the emphasis always remains "foreknowledge" as amount of information means nothing without appropriate timing. The temporality of information organization, standards and classification all rely on this same assumption, the more knowledge is not necessarily better, but well timed and strategic knowledge is key to success in military contexts. Control is intertwined with structural maintenance and manifests differently in diverse structures of government and power. In their analysis of the transition away from the fixed stratification of the state defined by bureaucratic norms, to what they dub the speedy and flexible "war machine," Deleuze and Guattari identify secrecy and speed as the heart of the successful war machine.[92] A disjuncture occurs, then, in the creation, maintenance and proliferation of standards. As information is framed as one of the primary resources that keeps the United States safe and information controls function to ensure that safety, and enable communication across agencies, then classified information infrastructure is always already about the deferral of harm.

[91] Tzu, S. (1963). The Art of War. Translated by Samuel B. Griffith. *New York: Oxford University*, *65*.

[92] Guattari, F., & Deleuze, G. (2000). *A thousand plateaus: capitalism and schizophrenia*. London: Athlone Press. Reid, J. (2003). Deleuze's War Machine: Nomadism Against the State. *Millennium*, *32*(1), 57-85.

Paranoia about information getting where it is not supposed to be leads to overclassification and overly complex policies that subsequently result in the dilution of how important a particular classification can be. In testimonies before Congress, a handful of government officials have estimated that as much as fifty percent of defense information may be improperly classified.[93] Emerging from what Lawrence Halloran has called a cultural bias against information sharing that characterized Cold War domestic and foreign policy, practices of overclassification have ossified within agency standards.[94] In the flurry of post 9/11 diagnostics concerning intelligence communities, overclassification and compartmentalization were often cited as major roadblocks.[95] Nevertheless, classification and additions to the classification system have proliferated, rendering the movement of information from classified to declassified all but inert as the resources and time to declassify information has not been met with similar funding and attention.

The complexity and length of manuals and training programs have led to a secondary economy made up of external training programs. In addition to the Department of Defense's own manual, the Center for Development of Security Excellence also produced a shorter, more concise manual in 2014 that is used in their certification program.[96] Written for both Department

[93] *See Too Many Secrets: Overclassification as a Barrier to Information Sharing: Hearing Before the Subcomm. on National Security, Emerging Threats, and International Relations of the H. Comm. on Government Reform*, 108th Cong., at 82 (Aug. 24, 2004) (statement of Carol A. Haave, Deputy Secretary of Defense for Counterintelligence and Security); Donald Rumsfeld, *War of the Worlds*, Wall St. J., July 18, 2005, at A12 (acknowledging "too much material is classified across the federal government as a general rule").

[94] Halloran, L. (2005). *Briefing Memorandum for the Hearing "Emerging Threats: Overclassification and Pseudo-Classification,"* Memorandum for the Members of the Subcommittee on National Security, Emerging Threats, and International Relations.

[95] *The 9/11 commission report: Final report of the national commission on terrorist attacks upon the United States*. Government Printing Office, 2011.

[96] Center for Development of Security Excellence. (2017) Marking Classified Information: JOB AID.

of Defense employees, and also taking into account both classified and uncontrolled controlled information, the manual attempts to summarize practices and justifications for a range of classification practices with the goal of simultaneous protection of information and information sharing across necessary constituencies. Whereas the language of both executive orders and legislative acts are relatively lacking in detail, this manual specifies that information regarding original classification should be shown in standardized ways across documentation, identifying standard marking elements as: banner lines, portion marks, agency, office of origin, date of origin, and classification authority block, specifying down to the format for the declassification date.[97] If a document contains derivative classification of information from multiple sources (either original or derivative), the classification level will defer to the highest used in any of the source material.

The Information Security Oversight Office published its rules and regulations for classified information in the Federal Register in 2010 and revised in 2014, giving a much more comprehensive view on the day to day handling of classified information than could be found in either executive orders or legislative acts. Most saliently, the ISOO provides guidance for marking and handling classification in the "electronic environment,"[98] including guidance on classified email, web pages, URLS, relational databases, blogs, wikis, instant messaging and chats, and attached files. The prevailing concern with respect to the electronic environment is its traceability to original classification authorities. Information that is considered dynamic in nature presents a challenge for security, and especially for traditional means of marking and handling classified information. The instructions regarding relational databases exhibits a deep discomfort with the ways in which information combines and displays according to query. Indeed, the

[97] Center for Development of Security Excellence. (2017) Marking Classified Information: JOB AID.
[98] 32 C.F.R. Parts 2001 and 2003 Classified National Security Information.

guidance provided defaults to the highest level of classification of any individual informational element for the entire database. The database itself must provide the user with a warning attached, transferring the onus for discerning over-classification on the user who is encouraged to make further inquiries on individual elements. Wikis and email on the other hand, forms that could be considered dynamic, are not considered dynamic by the ISOO, their instructions consider the email string or wiki as a whole instead of breaking it down into its constituent parts. Therefore, the overall classification designation and declassification instructions for the entire string, or for the entire wiki, should prevail. In addition, wikis should be portion marked and keep a log of different users and the changes they make.

We should be aware too of the shifts in classified information infrastructure that have brought on an expansion of categories and classifications that extend secrecy beyond the three-tiered system. This extension is so profound that one of the four volumes of the Department of Defense manual is entirely devoted to Controlled Unclassified Information (CUI). In a Presidential memorandum sent to Heads of Departments and Agencies in 2008, George W. Bush created the category of CUI, and placed the National Archives in charge of implementation, oversight and management of the CUI framework. This memo was an attempt to harness the over one hundred different information designations across government agencies for unclassified information considered critical or sensitive, and as a result, under strict controls. A lack of standardization and information sharing across these agencies made policies a moving target. The National Security Archive conducted a government-wide audit of policies regarding unclassified but sensitive information, the results of which resulted in Congressional hearings on information controls and policies.

In 2010, President Barack Obama issued Executive Order 13556 specifically targeting the disarray represented by the proliferation of control classification and markings, and attempted to mandate both uniformity and openness with respect to the system's application. Making Controlled Unclassified Information the government-wide designation, this Executive Order kept the management of CUI under control of NARA and prompted agency heads to review all markings used for designating unclassified information and submit a catalogue of proposed categories within 180 days of the issuance of the order. Within one year of the order, each agency was to maintain a public registry of all categories, which would come up for review each year for five years and every two years after that. NARA issued a final rule setting guidelines for federal agencies regarding the protection, release and disposal of CUI. One of the major implications for this rule was the burden placed on contractors dealing with CUI in their dealings with government agencies. In its response to public comments and final publication of the rule governing CUI, NARA did not mince words,

> the dispositive issues are not who protects the information, whether it is difficult or costly to protect it, or even how one goes about protecting it; the dispositive issue is that certain laws or similar authority require the Government, and by extension, those who handle or receive it, to protect this information.[99]

The rule goes on to describe the balance between information need and management and explicitly denies the reduction of regulations for any entity. The current definition of Controlled Unclassified Information (CUI) is

> Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information …or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Law, regulation, or Government-wide policy may require or permit safeguarding or dissemination controls in three ways: Requiring or permitting agencies to control or

[99] C.F.R. Part 2002

> protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify.[100]

Before CUI, the most common term for information that did not qualify as needing to be classified but still required sensitivity regarding its circulation and management was Sensitive but Unclassified (SBU). The term only appeared in the late 1970s, but came to encompass a whole range of information outside of formal classification structures, including proprietary data, law enforcement information, health information etc. It would eventually become even more expansive, covering information that was exempt from disclosure under FOIA or information that came under the Computer Security Act of 1987.[101] When Bush issued his CUI memorandum, he was attempting to bring together all of the disparate categories that had popped up through the decades, but the slow pace at which any new information control policy is implemented results in splintering of use and cooperation. The current CUI registry contains 24 categories with 85 subcategories. While the manual for marking and classifying information published in 2012 by the Department of Defense is technically still active, its guidance is moot in the face of new CUI streamlining regulations and there is currently no specific training for DoD employees or agencies regarding CUI, all of which would be through NIST or NARA. The DoD

[100] C.F.R. Part 2002

[101] Knezo, G. J. (2006, November). Sensitive but Unclassified Information and Other Controls: Policy and Options for Scientific and Technical Information. LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE.

had in fact publicly stated its resistance to change in between the issuance of the memorandum or Executive Order, and to a coherent and decisive interagency policy.[102]

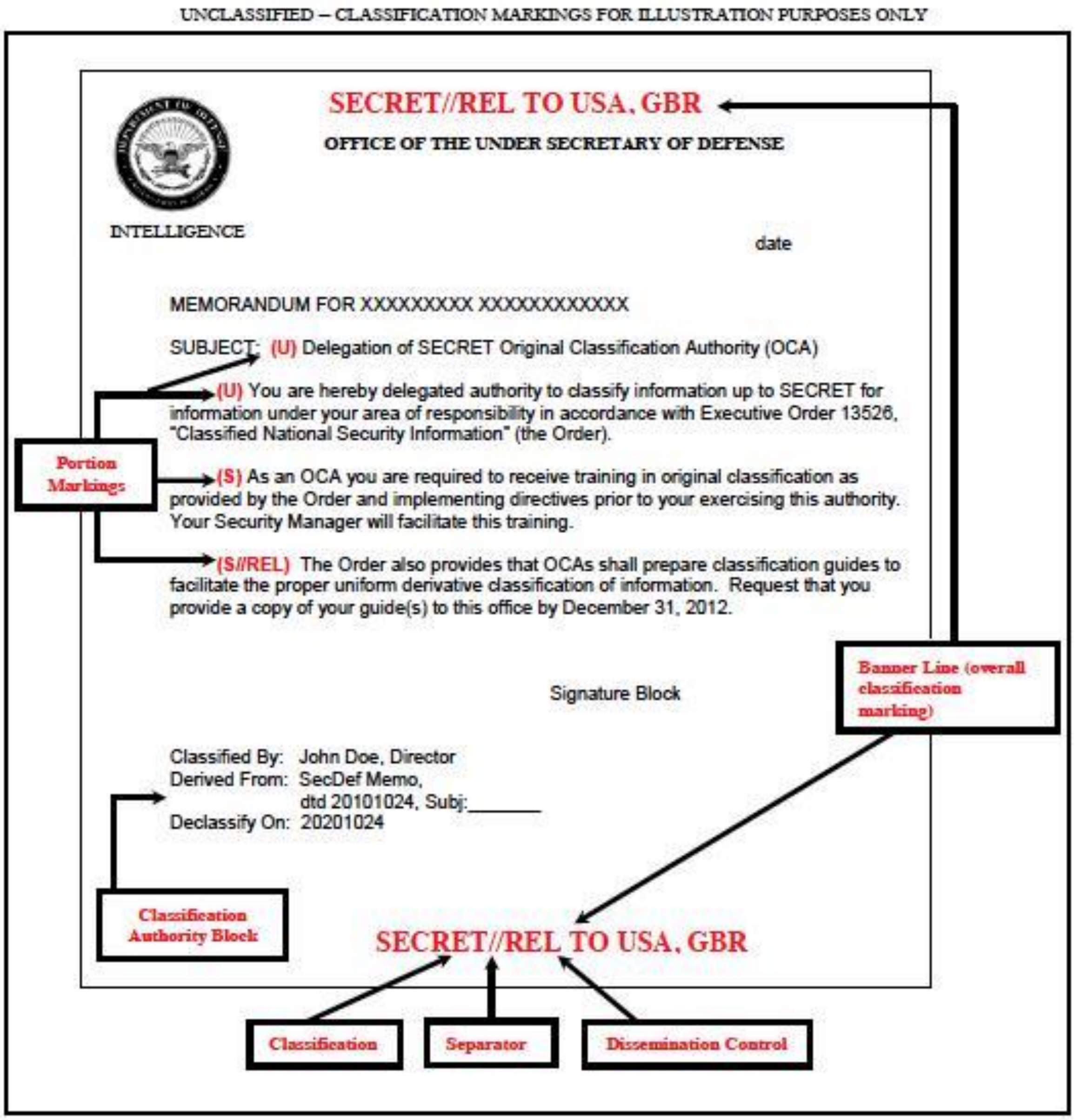
Secrecy as Standard and the Standards of Secrecy

The infrastructure of classified information presents an interesting case for analyzing standards and classification. Bowker and Star define classification as “a spatial, temporal or spatio-temporal segmentation of the world,” and a classification system as “a set of boxes, metaphorical or not, into which things can be put in order to then do some kind of work-bureaucratic or knowledge production.” Bowker and Star go on to define standard as “any set of agreed-upon rules for the production of (textual or material) objects.”[103] Classified information infrastructure as a system is one of classification insofar as it separates knowledge according to potential for damage and to particular levels of access according to role. It is also, however, a standard as it governs the production of specific textual objects. Classification is often talked about as something that is done *to* a document, but it is fundamentally also the production of a new document and an entirely new record. Vital to any discussion of standards and systems of classification is a definition of the community. If standards must be agreed upon, then they must be agreed upon by somebody, and if a classification system is to be useful, the kind of work it is doing must be fairly easy to identify. As this Chapter has shown, who agrees upon the standards is cyclical and often oppositionally defined, and starts with an overgeneralized singular directive that is then subject to more deliberative and consensus based processes. The kind of work the classified information infrastructure is doing is often less easy to identify. The work is justified

[102] Under Secretary of Defense (2009). *Memorandum on Clarification of Current DoD Policy on Controlled Unclassified Information (CUI).*

[103] Bowker, G. C., & Star, S. L. (1996). How things (actor-net) work: Classification, magic and the ubiquity of standards. *Philosophia*, *25*(3-4), 195-220.

through the implication of potential harm caused by the possession of information by another entity and what it does is situate information within a system of risk. Take for example the two documents reproduced here, which are both found in the DoD Manual, and meant to illustrate the proper implementation and display of marking standards and techniques.



UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

SECRET//REL TO USA, GBR

OFFICE OF THE UNDER SECRETARY OF DEFENSE

INTELLIGENCE

date

MEMORANDUM FOR XXXXXXXXX XXXXXXXXXXXX

SUBJECT: (U) Delegation of SECRET Original Classification Authority (OCA)

(U) You are hereby delegated authority to classify information up to SECRET for information under your area of responsibility in accordance with Executive Order 13526, "Classified National Security Information" (the Order).

(S) As an OCA you are required to receive training in original classification as provided by the Order and implementing directives prior to your exercising this authority. Your Security Manager will facilitate this training.

(S//REL) The Order also provides that OCAs shall prepare classification guides to facilitate the proper uniform derivative classification of information. Request that you provide a copy of your guide(s) to this office by December 31, 2012.

Signature Block

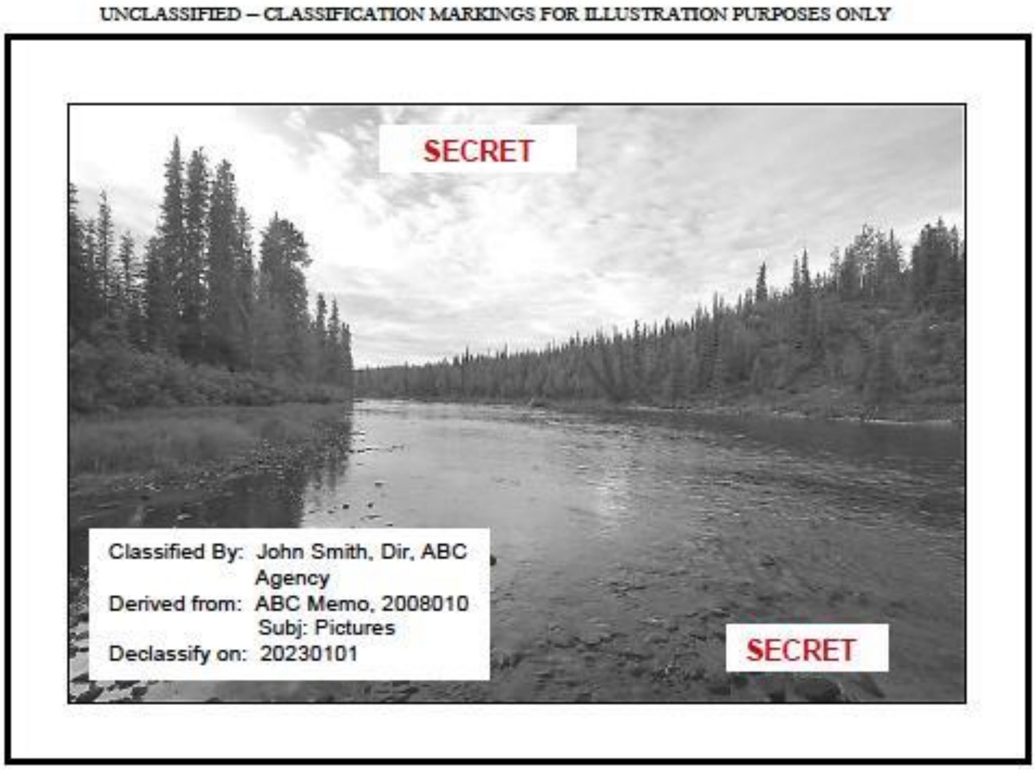
Classified By: John Doe, Director
Derived From: SecDef Memo,
dtd 20101024, Subj:_______
Declassify On: 20201024

SECRET//REL TO USA, GBR

Portion Markings
Banner Line (overall classification marking)
Classification Authority Block
Classification
Separator
Dissemination Control

1: "Figure 4. Example of Derivatively Classified Document" from DoDM 5200.01-V2, February 24, 2012

The first document we recognize as a bureaucratic document, it’s a memorandum, containing basic elements of a widely-circulated document: a date, a heading, a subject line, a body, a signature. The classification markings follow and in this example we see that the information can be segmented out in part or in whole, but that entering into the classified system requires document elements that immediately identify it as separate from other circulating information. Bold boxes outline the elements of classification: portion markings, banner line, classification authority block, classification, separator, dissemination control. Classified information then is visually different and immediately recognizable, becoming a new document and a new record identifying a separate set of organizational actions than the informational content of the previous document.


UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY
SECRET
SECRET

Classified By: John Smith, Dir, ABC Agency
Derived from: ABC Memo, 2008010 Subj: Pictures
Declassify on: 20230101

Figure 2: "Figure 22. Markings on Photographs" from DoDM 5200.01-V2, February 24, 2012

The second document we see is doing something different. It is displaying proper classification markings for photographs and contains a much more streamlined set of markings, a classification authority block and banner line. Exactly what is being classified here however forces us to be more specific about the separation between content and context, and asks for critical separation of information and documentation. There are limits to control within artificially controlled information environments. This artificiality is exposed periodically by the paradoxes inherent in the assumptions embedded within the classification system. In 2010, internal memos within the Navy and the Marine Corps warned troops against accessing WikiLeaks directly or through published media sources, essentially barring them from access to public knowledge.[104] This classified photograph or similarly classified geolocation data belies the same artificiality of closed systems, as the physical space itself cannot be classified but its representation can. Even the most expansive understandings of documentation, such as Suzanne Briet's focus on functionality,[105] do not collapse the distinctions between representations and abstractions. The futility expressed by the WikiLeaks memo demonstrates this failure, as it tries to assert the form of classified document over the circulation of knowledge outside of its own closed system. Commercial entities can be relatively quick to recognize the failure of a standard. Failed standards and formats for audio-visual materials are multitudinous, and the relative speed of adoption and rejection depends on overlapping factors but rarely have anything to do with what is "better."[106] Within a classified information infrastructure, arguably failed standards and classifications are plagued with inertia as the competing temporal registers of law, policy and

[104] Shachtman, N. (2010). Pentagon to Troops: Taliban Can Read Wikileaks, You Can't. Wired Magazine.

[105] Briet, S., Day, R. E., Martinet, L., & Anghelescu, H. G. (2006). *What is documentation?: English translation of the classic French text*. Scarecrow Press.

[106] Sterne, J. (2012). *MP3: The meaning of a format*. Duke University Press.

technology impede one another and expectations of control turn justification into paradox. One of the great challenges of a classified information infrastructure involves the increased dependence on networked communication and information technologies provided through government contracts, partnerships that require rethinking standards and classifications system-wide.

Chapter Two: Public Records, Private Phones

Introduction

On February 13, 2013, President Barack Obama issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." The text of this Executive Order extended and solidified practices and policies concerning the working relationships between private sector entities and the United States government that in the past thirty years have become increasingly inseparable and incredibly lucrative for individuals and corporations alike. Expressing great urgency, Obama stressed the dire need for cooperation between the federal government, intelligence agencies and the corporations that create, own or maintain cyber and communications infrastructure in order to both defend and gain access to sensitive and critical information. A subsequent proposed framework to be adopted by "agencies with responsibility for regulating the security of critical infrastructure,"[107] asserted the inextricability of such rhetorically and politically hefty concepts as Homeland Security, Counterterrorism, Economic Affairs, National Security and private information infrastructure.

Three years later, the Defense Information Systems Agency (DISA) has begun to roll out one part of the Pentagon's Joint Information Environment Plan, mobile devices for use in the field by persons with Secret clearance, that is operating under the name, Department of Defense

[107] Exec. Order 13636 78 C.F.R. 11737 (2013).

Mobility Classified Capability – Secret or DMCC-S. These devices and their related software, apps, standards and protocols will replace the now defunct Secure Mobile Environment Portable Electronic Device System. Reliant upon private infrastructure and contracts for the program's success, this transitional moment offers a window into understanding how the what, where, when and why of a classified record is shifting dramatically in the face of new socio-technical configurations. This chapter focuses on this transition to think through these questions, situating this program within a longer history of contracts between the federal government and the private sector.

Private Contracts and the United States Government: Setting the Neoliberal Stage

The use of contractors by the United States Government is hardly new, these contractors are such an integral part to the daily workings of government that they are often referred to as a "shadow government," and their effectiveness and cost is notoriously difficult to track. The Office of Budget and Management has estimated that 70% of the Department of Defense's annual budget is spent on contractors. The definition of contractor is as expansive as their activities and engagements with operations of government. For the purposes of this discussion, an expansive definition is useful in order to capture the ways in which the shifting boundaries of public and private work have been reconfigured, therefore we can consider any private company producing goods or offering services to the federal government under contract. Government contractors for the most part have been divided into two general types: those whose goods and services are separated out under a project management organizational model, and those that are used to supplement the daily needs of government under both long and short term contracts. Contemporary contracts with the private sector that involve networked technologies represent a third type of contract which makes short term engagement increasingly difficult, as the private sector owns the infrastructure so crucial to contemporary operations. The ability of the government to continue to do business with private entities relies on what Daniel Guttman has referred to as three co-existing constitutional models of accountability.[108] The "presumption of regularity/public law" model places the onus of accountability with the government entity or official who contracts with the private sector, assuming that the entity or official will be responsible for keeping the contractor on the right track. Extending any oversight to the contractor would be seen as an unnecessary overreach. The common law model is based on the belief that regulations and oversight in place for public officials and activities should also follow private contractors engaging in work on behalf of or paid by the public. The mechanisms of accountability and oversight come from the contractor, and are seen as one of many ways of evaluating past work and negotiating future contracts. The governance/accountability model is invested in incentivizing compliance and leveraging market forces and competition to course correct.

The United States federal government has contracted with private entities since its inception, but the unprecedented expansion of government that characterizes the second half of the twentieth century was bolstered by similarly unprecedented reliance on government contracts. Prior to World War II, the most prevalent use of private contractors came in the form of entities like the Institute for Government Research (which would eventually become The Brookings Institute). Private donations fueled what the organization's original 1918 charter stated as "scientific investigations into the theory and practice of governmental administration…to carry on such inquiries, directly or with the cooperation of governments, learned societies, institutions of learning or other agencies and individuals and to make public

[108] Guttman, D. (2003). Contracting United States government work: Organizational and constitutional models. *Public Organization Review*, *3*(3), 281-299.

the results of its investigations."[109] This and other privately funded research institutions have held and do hold great influence over government reform. While relatively little attention has been given to this constellation of think tanks and interest groups as a system rather than on specific institutional histories, what is easily established is the growth of their numbers and their influence. Claiming to produce reliable and unbiased research for the improvement of government function and accountability, organizations such as the Institute for Government Research have been identified as directly leading to the passage of the Budgeting and Accounting Act in 1921, creating both the budget bureau and the congressional accounting offices.[110]

The buildup to World War II required a new set of tools and relationships in service of preparedness and mobilization. This period saw the growth and development of the Manhattan Engineer District, later nicknamed the "Manhattan Project," focused on the successful and expedient development of the atomic bomb, as well as the Office of Scientific Research and Development (OSRD) which maintained oversight of a host of research and development initiatives. President Franklin Roosevelt allowed his then science advisor Vannevar Bush to "contract out most of its (OSRD's – authors parentheses) programs to universities, de-emphasizing federal laboratories…"[111] This period set the standard of operations for large scale government projects. The Manhattan Project was managing much more than individual research projects; they also were in charge by default and then by contract of the cities that housed the projects, creating a micro-economic system. Acknowledging this growing trend, President John

[109] Willoughby, W.F. 1918. The Institute for Government Research. *The American Political Science Association.* 12 (1). Pp. 49-62.

[110] Roberts, A. S. (1994). *The rhetorical problems of the management expert* (Doctoral dissertation, Harvard University Cambridge, Massachusetts).

[111] McDougall, W. A. (1985). Heavens and the earth: a political history of the space age. P. 67.

F. Kennedy issued a Letter to the Director of the Bureau of the Budget in 1961 referencing a recently issued Budget Circular No. A-49 which outlined federal policies for issuing contracts for government activities. The Circular and the subsequent letter both emphasized that activities considered “inherently governmental” should always be in official hands, not in the hands of contractors. Debates about what exactly should be considered inherently governmental are constant. Currently, arguments over this inherency tend to be focused on private contractors in military zones or extending military activities. More specifically, inherency comes up in discussions about the protocols governing drone operations, both as a means of surveillance and in active mission scenarios.[112] The strict definition of inherently governmental is a teleological one – activities that are inherently governmental are those that are as a matter of law and policy, considered to be confined to public employees, thus garnering public oversight and accountability. The prescience of Kennedy’s 1961 letter has less to do with the logistical context of military or scientific need of the time, and more to do with building the infrastructure of government research and technological expertise, not only in partnership with private entities but in deference to them. The Manhattan Project recruited contractors to engage not just in research but in sustained “life-cycle” support of nuclear projects which took place on government property and in government facilities. A specific contract became the model for this and subsequent projects for years, the management and operating (M & O) contract. While there was little to no movement on the legislative side to substantively confront the complexities or potentialities of this heavy reliance on contracting, “the preference for private enterprise conduct

[112] Luckey, J. R., Grasso, V. B., & Manuel, K. M. (2009, June). Inherently governmental functions and Department of Defense operations: background, issues, and options for Congress. LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE.
Clanahan, K. D. (2013). Wielding a Very Long, People-Intensive Spear: Inherently Governmental Functions and the Role of Contractors in US Department of Defense Unmanned Aircraft Systems Missions. *AFL Rev.*, *70*, 119.
Tiefer, C. (2013). Restrain 'Risky Business': Treat High-Risk Private Security Contractors as Inherently Governmental.

of U.S. weapons development and production work…is essentially an unwritten law."[113] Support for the protraction of these relationships came in the form of financial justifications of course, but importantly, also relied on the assertion that the success of such programs were not alone due to the scientists involved but in the management expertise and business acumen of their parent companies. Vannevar Bush pointed out the obvious when he reflected that "it was soon possible to gather together committees on various aspects of the problem, for the men who could contribute were already working together."[114] This period solidified the connections that comprised President Eisenhower's vision of the "military-industrial complex," think tanks such as RAND were established, technology projects on a massive scale were almost entirely out of direct government hands and oversight, and contractors became intimately involved in congressional decision making and policy development. The position of think tanks and policy institutes outside of the government allowed them to advocate for their interests to Congress without any official improprieties. The Aerospace Corporation saw the development of the intercontinental ballistic missile system concurrently with the development of the computerized air defense system developed by the Mitre Corporation.

At least one government entity was created and operated from the beginning with the assumption of government business by contract. Following the launch of Sputnik in 1957, the National Aeronautics and Space Administration was established and its engagement with contractors for all levels of its operations was unprecedented. Reconceiving the governmental function as one of project management, NASA immediately relied upon private aerospace manufacturers like Boeing to build its rockets and invested in contract research organizations

[113] Peck, M. J., & Scherer, F. M. (1962). THE WEAPONS ACQUISITION PROCESS; AN ECONOMIC ANALYSIS.

[114] Bush, V. Pieces of the Action (New York: William Morrow, 1970). *Bush198Pieces of the Action1970*, 198-199.

like the Jet Propulsion Laboratory (JPL). Right up to the present, contractors dominate construction, research, training and mission control for all NASA flights. NASA was in fact the first such agency to become publicly embroiled in a law suit alleging that its hiring practices were violating laws governing civil service, as well as the federal employee's union's collective bargaining agreement. Although the 1978 lawsuit Lodge 1858 American Federation of Government Employees v. Webb brought attention to how prevalent these dependencies were, NASA was ultimately vindicated due to the very conditions of its founding. The National Aeronautics and Space Act of 1958 was passed establishing the agency as entirely civilian in nature, rather than military, skirting arguments about what might be inherently governmental. The law stipulated that the basic work of NASA would be done by federal employees, but also acknowledged the need for and provided for the use of contractors. The law also capped the number of federal employees to be hired by NASA at any given time, placing limits on growth and expansion before it even began. In what would become a familiar story, contractors emerged as a way of operating outside of both federal pay caps and hiring freezes.

This period also witnessed the establishment and growth of several new civilian governmental bodies including the Environmental Protection Agency and the Department of Transportation. These too were established with pay and personnel caps which made their staffing inadequate as their responsibilities and services continued to grow. Many of these new agencies in turn created their own versions of RAND, policy and research institutes that could ameliorate the pressures of their work, but was also a means of bringing the perceived management skill and expertise of the private sector to bear on public social problems. Perhaps most egregiously, the Office of Education brought in military contractors, including Westinghouse, to mimic the Department of Defense's management style within public schools.

When the rhetorical promise of small government emerged in the 1980's, the patterns were already established and the prevalence of privatization, deregulation, and public-private partnerships as positive goals became familiar terrain. Seen as a counterweight to the familiar complaints leveraged against bureaucracy and its relative sluggish tempo of activity, public-private partnerships were meant to automatically be more responsive and much more in tune with market forces. The problem of bureaucracy, it seemed, was that it was not subject to the kinds of competition that produced the best work. Ronald Reagan's 1987 budget proposal included more proposals for privatization than any president had ever put forth including the federal sale of satellites, airports and power agencies.[115] Richard Fink, then president of Citizens for a Sound Economy was quoted as saying, "It's going to be the greatest effort to return the provision of goods and services to the private sector that we've seen in this country,"[116] and although the Administration had limited success in its budget agenda, it led the president to create the President's Commission on Privatization which depicted a broad and far-reaching vision for the privatization of everything from the U.S. Postal Service to prisons to Medicare and low-income housing. This too made little progress, but signified the beginnings of an organized and expansive coalition of lobbyists, researchers and politicians focused on expanding privatization; piggybacking on ideas contained in both Stuart Butler's Privatizing Federal Spending and Madsen Pirie's Dismantling the State.[117] Butler advocated for a complete reconceptualization of the relationships between special interests, lobbyists and government work.

[115] Cohen, D. The History of privatization: How an Ideological and Political Attack on Government became a Corporate Grab for Gold. Talking Points Memo. Retrieved August 8, 2016. http://talkingpointsmemo.com/features/privatization/one/

[116] Ibid.

[117] Butler, S. M. (1985). *Privatizing Federal Spending. A Strategy to Eliminate the Deficit*.
Pirie, M. (1985). Dismantling the State. *Dallas: National Center for Policy Analysis*, 20-21.

> Conditions must be created in which the demand for government spending is diverted into the private sector. This is the beauty of privatization. Instead of having to say ‘no’ to constituencies, politicians can adopt a more palatable approach to cutting spending. They can reduce outlays by fostering private alternatives that are more attractive to voters, thereby reducing the clamor for government spending. Changing the political dynamics of government spending in this way is the secret of privatization.[118]

This wholesale reconfiguration led to a re-conceptualization of public good(s), as Robert Poole of the Reason Foundation, a libertarian think tank, stated:

> most local services have few attributes of true public goods. Most of them – garbage collection, park and recreation services, libraries, airports, transit, and aspects of police and fire protection – have specific, identifiable users, who are the services’ beneficiaries.

Rather than an investment in public trust or collective will, the dependence on contractors represents a cynicism about engagement in public work that assumes limited motivation and short-term investment. Perhaps the most curious thing about the language of reinvention was its complete and utter ignorance of the very entrenched traditions and policies that were now being presented as characteristic of radical reinvention. In their 1992 book, *Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector*, David Osborne and Ted Gaebler[119] could not ignore that many of their innovative strategies had already been integrated into the public sector for years. The title of the book became a kind of motto for the Administration of Bill Clinton. Together and individually they would go on to write several books introducing strategies for individuals to reinvent government at various levels of engagement, as well as books on management style and the evils of bureaucracy. Both the catalog of Osborne and Gaebler and the policy adoption on the part of the Clinton

[118] Butler, S. M. (1985). *Privatizing Federal Spending. A Strategy to Eliminate the Deficit*.

[119] Osborne, D., & Gaebler, T. (1992). Reinventing government: How the entrepreneurial spirit is transforming government. *Reading Mass. Adison Wesley Public Comp*.

Administration focused on not just the increased use of private contracts for the sake of efficiency but also argued for the "blurring" of the very lines between public and private.

In many ways, the Clinton Administration represented the successful adoption of previous administrations' failed policy interventions with respect to privatization, implementing the National Performance Review, an intergovernmental task force geared toward efficiency and downsizing of federal programs and spending. While the National Performance Review identified programs that could be eliminated, privatized or reinvented, and the results were widespread, the most significant shift of this period concerns ideological and rhetorical shifts; a wholesale acceptance and promotion of neoliberal policy; embedding competition into the foundation of government service provision; and development and recasting citizens as consumers, which individualized exchange between individual people and the government at large. By transforming public goods into burgeoning new private markets, government services shifted from the provision of necessities to markets that to some extent rely on dependency. The Welfare Reform Law of 1996 signified a substantive change in the ways that corporations interacted with the public sector by transitioning from a product development and exchange model, to one in which corporations were able to make decisions and shape policy; in this instance determining what qualified individuals for welfare assistance, how they should be tracked and managed and what the services consisted of.

George W. Bush made privatization a more explicit part of his overall vision of the work of government and specifically a larger part of his platform stating, "Government should be market-based – we should not be afraid of competition, innovation and choice. I will open government to the discipline of competition."[120] Although initial efforts to privatize Social

[120] Bush, G. W. (2001). *The President's Management Agenda, Fiscal Year 2002*. EXECUTIVE OFFICE OF THE PRESIDENT WASHINGTON DC.

Security fizzled out due to opposition, his Administration focused on sectors of the government less prominent in the public eye including the Forest Service and large part of the intelligence community. Remarkably, this period saw rapid expansion of the use of contractors in war zones. As of 2007, contractors outnumbered troops in Iraq by twenty-thousand and in 2009, the Congressional Research Service reported that contractors made up over half of the troops in Afghanistan.[121] Contractors had become such an essential part of the U.S. military that Secretary of Defense Donald Rumsfeld included them in his definition of the Department's Total Force as described in the 2006 Quadrennial Defense Review. Most recently, the Barack Obama Administration represented a kind of push-pull when it came to the place of private contractors in the public sector. While thousands of jobs, specifically those in the intelligence and defense sector, were insourced over the past decade, there was also massive support for the privatization of schools through charter and voucher programs. This trajectory, that marks a re-definition of public good and a reconceptualization of how to get there, follows the development of neoliberalism as an ideology in a broader sense. Neoliberalism is a comprehensive political and economic ideology that positions individuals as economic agents and equates efficiency and profitability with success and well-being.[122] This philosophy swallows the very possibility of inherent governmental functions as it prioritizes corporate models of management that emphasize the responsibility and agency of individuals and de-emphasizes both the actual and potential roles of government in life.

Public Records and Private Contractors

[121] Schwartz, M. (2009) Department of Defense Contractors in Iraq and Afghanistan: Background and Analysis. 7-5700-R40764.

[122] Harvey, D. (2007). Neoliberalism as creative destruction. *The annals of the American academy of political and social science*, *610*(1), 21-44.

As resources for public work contracts and the opportunities for private contracts grow, so follows public records, archival work and records management. This has presented challenges to practices of accountability and transparency, as regulations regarding the retention and access to public records may or may not apply to records held by private agencies. Additionally, private corporations fundamentally share and prioritize different values. Government entities do not necessarily have to be profitable or accountable to shareholders and private corporations do not necessarily have to be accountable to the public. The Freedom of Information Act (FOIA) was signed into law in 1966, and its commitment to facilitating access to government information for the sake of accountability and transparency has met legal and logistical challenges since its signing. One of many unforeseen challenges was that the definition of agency records remains inadequate considering the growth and expansion of the privatization of government work. In recent years, even the work of providing access to public records has been contracted out to private companies. In 2012, at least twenty-five agencies were outsourcing parts of the FOIA process. The arguments for this are familiar, the rhetorical situating of efficiency as driving force, claiming that privatization can lead to a reduction in backlogs and financial savings. Private companies are operating at each stage of the FOIA process, including correspondence with requestors and submitting recommendations for exactly what to redact.[123] This activity is directly at the heart of what becomes defined as inherently governmental, and increasing compartmentalization of activities creates a moving target of inherency. CACI International Inc., represents another potential conflict of interest or point of departure for appropriate FOIA work. CACI provided translation services at the Abu Ghraib prison and is also one of the major recipients of FOIA contracts; therefore CACI could be in a situation in which they were

[123] Hogan C. (2011) The Outsourcing of Federal FOIA Services: Some are Concerned about Lack of Information on Contract Workers. Reporters Committee for Freedom of the Press. Retrieved August 9, 2016.

reviewing documents involving their own employees. In an essay about the rise of private prisons and the challenges they present, legal scholar Nicole Casarez discusses the side effects of skirting FOIA laws within private contracts, as prison officials have a uniquely powerful position from which to "abuse the public trust or prisoners' rights."[124] She even goes so far as to warn against the possibility of the federal government intentionally circumventing transparency and accountability measures outlined by FOIA. Between 1996 and 2007, FOIA defined a record as "any information that would be an agency records subject to the requirements of the [FOIA] when maintained by an agency in any format, including an electronic format." This definition was amended in 2007 to include the previous definition and "any information described under subparagraph (A) that is maintained for an agency by an entity under Government contract, for the purposes of records management.[125] While this change specifically acknowledges the need for a more expansive definition in reaction to new forms of government labor, it also makes for difficult work, since the responsibility for compiling records still falls to agencies. As records management and archival work has become increasingly networked and records are created in and accessed through multiple formats and platforms, these issues have become even more complex. In 2015, InfoReliance won a contract to provide Cloud Managed Services[126] to the National Archives and Records Administration, entrenching commercial services within the heart of the work of the National Archives. NARA has been using contractors for a myriad services for years, but this contract represents a point of no return in terms of infrastructural investment. Private corporations not only do not have the same relationship to transparency and

[124] Casarez, N. B. (1995). Furthering the accountability principle in privatized federal corrections: the need for access to private prison records.

[125] Open Government Act of 2007, Pub. L. No. 110-175, 121 Stat. 2524 amended subsection (f)(2) of the Freedom of Information Act (FOIA).

[126] InfoReliance (2015) InfoReliance wins NARA Cloud Managed Services Contract. Retrieved July 16, 2016. http://www.inforeliance.com/about-us/news-events/inforeliance-wins-nara-cloud-managed-services-contract

accountability expectations but in this instance, a five-year contract operates on an entirely different timescale than the National Archives, which focuses on the lifecycle of the record from its creation to its use.

Regulations for Contractors

While agencies retain the responsibility for keeping track of and procuring records produced by contractors, the contractors themselves are increasingly bearing the burden of implementing security controls in compliance with government standards. To aid in this there are two main points of reference for standards and protocols: the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS). The FAR system regulates the ways in which executive agencies[127] of the United States federal government contract for services, projects and goods. The system has three phases: need recognition and acquisition planning; contract formation; contract administration and the details of the process are within the Code of Federal Regulations.[128]The explicit purpose of FAR is to provide clear cut, uniform standards for those soliciting government contracts. Contractors are expected to perform due diligence and know the details of FAR in order to comply. With the passage of the Office of Federal Procurement Policy Act of 1974, the FAR was established alongside the authority to maintain and issue its parameters. This authority lies with the Secretary of Defense, the Administrator of the National Aeronautics and Space Administration (NASA) and the Administrator of General Services and all issuances must be jointly approved by the Administrator of Federal Procurement Policy.[129] There is one section of the FAR that deals explicitly with classified information, "Subpart 4.4 – Safeguarding Classified Information Within

[127127] Two agencies are exempt from this system, the Federal Aviation Administration and the United States Mint. 49 U.S.C. 40110, 48 C.F.R. 1201.104, 31 U.S.C. 5136, 48 C.F.R. 1001.104

[128] 48 C.F.R. 31

[129] 41 U.S.C. 421 (c)(1), 41 U.S.C. 405

Industry,"[130] its text consisting of a series of cascading citations to other statutes, protocols, manuals and procedures that require layers of research for compliance officers or parties negotiating on behalf of contractors. Once establishing that the authority of this particular section of the FAR is precipitated by the signing of Executive Order 12829 in 1993 or the National Industrial Security Program (NISP), a program to safeguard classified information that is released to contractors, licensees or grantees of the United States Government was outlined. Executive Order 12829 amended Executive Order 10909 signed in 1961 and Executive Order 10865. The requirements laid out in these Executive Orders are given more specific shape in the National Industrial Security Program Operating Manual (NISPOM) which is maintained and issued by The Secretary of Defense. In addition to NISPOM, the DOD also details protocols in Industrial Security Regulation[131] and in Part 27 of the FAR which covers policy and procedures for safeguarding classified information in both patents and patent applications.

While the FAR does outline responsibilities of contractors for all three phases of acquisition, there are few specifics beyond a general missive to refer to both agency specific protocols (if the agency being contracted with is exempt from NISP) and NISPOM as the onus is on the contractor to implement security measures. In addition, contractors must submit a form containing information about their needs and requirements with respect to clearance and classification authorities. Form DD 254[132] specifies details concerning such issues as facility clearance and storage/safeguarding requirements as well as general contact information for responsible and appropriate contacts for the contractor. Facility clearance is one of the largest hurdles as it requires sponsorship by a government contracting activity (GCA) or another cleared

[130] Edwards, D. F. (2010). OCIs in Construction Contracting: Bumps in the Road Ahead. *Procurement Law.*, *46*, 4.
[131] DoD 5220.22-R
[132] DD Form 254 Retrieved July 16, 2016. http://www.dtic.mil/whs/directives/forms/eforms/dd0254.pdf

agency or company, approval by the Defense Security Services, comprehensive understanding and implementation of both the Facility Security Clearance (FCL) Orientation Handbook and NISPOM, as well as registering for a Commercial and Government Entity Code (CAGE Code) designating a potential Facility Security Officer (FSO), clearing necessary personnel and disclosing foreign investment or activities. As a warning, the Checklist for New Facility Clearance furnished by the Defense Security Service states that alone, "Becoming familiar with the NISPOM will take a great deal of time and will, likewise, require a determined effort."[133]

The FAR takes an agnostic stance with respect to types of controlled unclassified information, the details of which are reserved for the DD 254 which requires both contractors and subcontractors to specify whether or not they will be using or dealing with Communications Security Information (COMSEC), which includes controlled cryptographic items (CCI), Restricted Data, Critical Nuclear Weapon Design Information (CNWDI), Formerly Restricted Data, Intelligence Information, Special Access Information, NATO Information, Foreign Government Information, Limited Dissemination Information and For Official Use Only Information. If a contractor needs or intends to deal in anyway with classified information, this form also requires a granular explanation of what (producing, receiving, storing, exchanging) the facility or contractor will be doing with that information, and exactly which security protocols have been put into place and whether or not their operations are limited spatially to the United States and its territories. Mutual exchange of information with the Defense Technical Information Center (DTIC) must also be disclosed and outlined, and the use of the Defense Courier Service (DCS) must be justified and established. This is also the forum for a contractor to specify their need for TEMPEST as defense or not, requiring both a NATO certification and

[133] U.S. Department of Defense Defense Security Service. Checklist for a New Facility Clearance. Retrieved July 16, 2016. http://www.dss.mil/isp/fac_clear/fac_clear_check.html

NSA specifications for both spying and protection against spying on information systems through radio, electrical signals, vibrations and/or sounds.

There is more known about protection standards (which are also referred to as emissions security (EMSEC) than the NSA's spying techniques for fairly obvious reasons, and their general methods include shielding, filtering, masking and strategic distance between walls and devices. In their outline of security levels, NATO defines each of the three levels through a measure of proximity.[134]

Additional guidance and requirements for contractors are outlined in DFARS. Sections 204.470 parts 1-4 refer to guidance on classified information for contractors, mostly by referring to other documentation and protocols. Significantly, part 2 outlines a "National Security Exclusion," which allows for the circumvention of inspection protocols detailed in FARS "for activities, or locations, and associated locations or information with direct national security significance."[135] This section specifically interacts with the U.S. International Atomic Energy Agency Additional Protocol (U.S. IAEA AP), and exempts work of national security concern from what is otherwise considered a required disclosure of nuclear activities. The determination of whether or not something meets the standards for reporting or the standards for the National Security Exclusion is up to a DoD Program Manager whose determination is to be guided by yet another DoD Instruction, 2060.03, which itself implements policy established in DoD Directive 2060.1 which represents agreed upon exclusions to agreements reached by the United States and the IAEA.

[134] Secure Systems & Technology. TEMPEST Standards. Retrieved July 16, 2016. http://sst.ws/tempest_standards.php

[135] DFARS 294.470-2

All government contractors that are granted a security clearance for access to classified information are required by Executive Order 13292 to sign a Classified Information Nondisclosure Agreement, or Standard Form 312, as are government employees. The form, issued by the Information Security Oversight Office of NARA, replaced earlier versions of the form such as SF 189 or SF 189-A. Everyone who signs has also undergone a background check, a personnel security investigation. This form operates as a contract between the signer and the U.S. Government in which the signer agrees to not disclose information to any unauthorized person, and provides the signer not only with an outlining of their responsibilities but also with a description of the consequences should they disclose information. It allows the federal government to pursue civil charges against those who disclose information in addition to any criminal charges. The form derives its authority not just from Executive Order 13292 but also from U.S.C. 18 § 793, 641, 794, 952; U.S.C. 50 § 783; U.S.C. 5 § 2302, 7211; U.S.C. 10 § 1034; U.S.C. 6 § 601-606 to name a few. A key element of this form too, is providing the limits of liability, stating that the signer is only liable if their actions result in unauthorized disclosure, safeguarding against liability in a situation in which classified information is classified retroactively or unbeknownst to the signer. At first glance, this document might seem a curious one, as criminal liability is already ensconced within statute. However, this document makes possible civil liability and opens the door for citizen lawsuits when no criminal charges have been filed or government action is seen to be inadequate. One side effect of this nondisclosure agreement manifests in customary prepublication reviews for federal employees or contractors, under which they can submit publishable work for review to ensure compliance.

Cell Phones in the DoD

Although cellular telephone service was introduced in the United States in 1983, the Department of Defense introduced its first piece of definitive domestic policy regarding the use of cellular telephones within Department facilities on June 12, 2002 in two documents, *Policy for Use of Cellular Telephones and Personal Digital Assistants (PDAs) Within Department Buildings*[136] and 5 FAM 526.2 *Restrictions for Cellular Telephones Usage*[137]. In these documents the primary security requirements outlined are that cellular telephones (both personal and those issued by the United States government) must be turned off in areas where classified information is discussed or processed and that they must not (in any state) be placed within ten feet of classified processing equipment. Additionally, phones that possess either or both still picture and video capturing functionality are not allowed inside of Department of State domestic facilities. This guidance, in conjunction with the Director of Central Intelligence Directive (DCID) 6/9, *Physical Security Standards for Sensitive Compartmented Information Facilities* (SCIFs) and the Intelligence Community Policy Memorandum (ICPM) 2005-700-1 attachment 1 (Annex D) and attachment 2 and 12 FAH-6 H-531.1 *Cellular Telephone Standards*, outlined the guiding protocols governing government agencies both in domestic and non-domestic contexts for the better part of a decade.

In a 2007 review conducted by the Office of the Inspector General, it was found that zero out of ten bureaus/offices examined could be considered “fully compliant” with all prevailing protocols, three out of ten were found to be “partially compliant,” and seven were found to be “noncompliant.”[138] The most common reasons cited for this state of affairs were a general lack of

[136] United States Department of State and the Broadcasting Board of Governors Office of inspector General. (2007) Report of Inspection: Review of Department Headquarters’ Implementation of Cellular Telephone Security Policies. SIA-I-07-01.

[137] 5 FAM 526.2

[138] United States Department of State and the Broadcasting Board of Governors Office of inspector General. (2007) Report of Inspection: Review of Department Headquarters’ Implementation of Cellular Telephone Security Policies.

awareness of protocols and compliance standards as well as a persistent and overriding need to use cellular telephones in day to day and real-time working contexts, including areas in which classified information was accessed and processed. In addition, interviewees expressed the need to use cellular telephones for emergency and/or familial reasons. Levels of training and security briefing vary from bureau to bureau, employee to employee, and the general introductory security briefing does not include cellular telephone usage in its training on the processing, handling, and storage of classified information. In the current Department of Defense manual concerning the marking, processing and handling of classified information, there are scant suggestions or missives of guidance concerning the use of telephones with respect to classified information and communication.

> c. Telephone. Only approved secure telephones, including cell phones and phones integral to personal electronic devices, authorized by the Director, NSA pursuant to paragraph 3.b of this enclosure, may [be used] for telephone transmission of classified information. Users must ensure the secure connection is at the appropriate level of classification for the information being discussed. [139]

> 11. USE OF SECURE COMMUNICATIONS. In accordance with the requirements of Enclosure 4, classified information shall be transmitted only over secure communications circuits approved for transmission of information at the specified level of classification. This includes communication by telephone, facsimile, e-mail and other forms of

[139] Department of Defense Manual. (2012) Information Security Program: Protection of Classified Information. 5200.01 Volume 3. P. 61.

electronic communications (e.g., messages, websites). See Volume 2 of this Manual for guidance on required markings. [140]

j. Security Incidents Involving Improper Transfer of Classified Information. Any activity that receives classified information that has been improperly handled, addressed, packaged, transmitted, or transported shall make a determination as to whether the information has been subjected to compromise. If the activity determines that the classified information has been subjected to compromise, the receiving activity shall immediately notify the sending activity, which shall be responsible for initiating an inquiry or investigation, as appropriate. The receiving activity shall share information generated regarding the incident with the sending activity. The sending activity is responsible for required notifications (e.g., to the OCA). Classified information shall be considered as having been subjected to compromise if it has been handled through foreign postal systems, its shipping container has been damaged to an extent that the contents are exposed, or it has been transmitted (e.g., telephone, facsimile, message, e-mail, computer or data links) over communications circuits that are not appropriate for transmission or classified information. If the receiving activity determines that classified information was not in fact compromised, but was nevertheless improperly prepared or transferred, the receiving activity shall report the discrepancy to the sending activity. [141]

[140] Department of Defense Manual. (2012) Information Security Program: Protection of Classified Information. 5200.01 Volume 3. P. 20.

[141] Ibid 91

> (2) FUOU[142] information and material may be transmitted via first class mail, parcel post, or, for bulk shipments, via fourth class mail. Whenever practical, electronic transmission of FOUO information (e.g., data, website, or e-mail) shall be …approved secure communications systems or systems utilizing other protective measures such as Public Key Infrastructure (PKI) or transport layer security (E.g., https). Use of wireless telephones should be avoided when other options are available. Transmission of FOUO by facsimile machine (fax) is permitted; the sender is responsible for determining that appropriate protection will be available at the receiving location prior to transmission (e.g., machine attended by a person authorized to receive (FOUO; fax located in a controlled government environment).

The guidance espoused here then is tied to device rather than practice, limited to using approved devices in approved spaces. As late as 2012, when these manuals were produced, there were no cellular telephones approved for use on secure, classified networks or for the storage or communication of classified information. BlackBerry, long the company that dominated the market for government contracts due to the level of security of their devices, had several devices

[142] FOUO or For Official Use Only, was a protective marking applied to unclassified information when disclosure to the public of that particular record, or a portion thereof, would reasonably be expected to cause a forseeable harm to an interest protected by one or more provisions of the Freedom of Information Act. There are 9 exemptions from the Freedom of Information Act including: information that is currently and properly classified; information that pertains solely to the internal rules and practices of an agency; information specifically exempted by a statute establishing particular criteria for withholding; information such as trade secrets or is otherwise privileged or confidential and would result in competitive harm if released; inter- or intra-agency memorandums or letters containing information considered privileged in civil litigation; information that would be reasonably expected to constitute an unwarranted invasion of personal privacy upon release; records compiled for law enforcement purposes that would identify a confidential source, deprive a person of a right to a fair trial, would interfere with law enforcement proceedings, could constitute an invasion of privacy, could disclose investigative techniques and procedures or could be expected to endanger the life or physical safety of an individual; certain records of agencies responsible for supervision of financial institutions; geological and geophysical information (including maps) concerning wells. FOUO was one category of classified information that was replaced by the category Controlled Unclassified Information in 2008 with a directive authored by George W. Bush. Protocols governing Controlled Unclassified Information were replaced and amended with Executive Order 13556 in 2010.

approved for communicating on unclassified government networks. In 2013, BlackBerry 10 devices were awarded FIPS 140-2 certification for low-level secure transmissions. FIPS or the Federal Information Processing Standard is issued by the National Institute of Standards and Technology (NIST) and publication 140-2 is a United States government computer security standard used to assess and approve cryptographic modules. This standard has not been updated since 2002 and efforts to revise or retool the standard were attempted and stalled out in 2013. The failed publication of FIPS 140-3 was mired in debates about which aspects of security to prioritize and how to shape future research and attitudes toward awarding certification.[143] Also in August of 2013, BlackBerry 10 phones, including the Z10 and Q10 alongside BlackBerry Enterprise Service 10, were given the "authority to operate" on U.S. Department of Defense networks, making it the first suite of cellular phones and services to receive this certification. As a result, the Defense Information System Agency (DISA) began developing its infrastructure and capabilities to support an influx of BlackBerry smartphones used by government personnel and contractors.

In 2013, NIST published the Security and Privacy Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53, Revision 4).[144] This almost 500 page guide fulfills NIST's statutory responsibilities as outlined by the Federal Information Security Management Act (FISMA) in developing minimum requirements for federal information systems which are not meant to superseded or contradict other federal requirements or statutes. Because NIST's function is meant to be necessarily broad, the advice given in this guide ranges from natural disasters to technical failure to human error to hostile attacks, instead

[143] See documents in Physical Security Testing Workshop. Retrieved July 19, 2016. http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-3/physec/physecdoc.html#

[144] National Institute for Standards and Technology. Joint Task Force Transformation Initiative. (2015). Security and Privacy Controls for Federal Information Systems and Organizations NIST Special Publication 800-53 Revision 4.

of a guide narrowly catered to a particular department defined by their purview. Of course, this guide is not meant to operate alone, instead requiring those in charge of or interacting with information systems to first establish the level or security of their information system by consulting FIPS Publication 199, the *Standards for Security Categorization of Federal Information and Information Systems*, and then the information system impact level from that security category as outlined in FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, and then and only then can the security requirements suggested by NIST SP 800-53 be implemented.

The Department of Defense and The State Department use one of three networks to circulate information, the Non-Classified Internet Protocol Router Network (NIPRNet), Secret Internet Protocol Router Network (SIPRNet) and the Joint Worldwide Intelligence Communications System (JWICS). These networks grew out of the Defense Data Network in the 1990s. As ARPANET transitioned from a government research project to an operational entity, the Defense Communication Agency ((DCA) which is now DISA) took over the essential infrastructure. The DDN functioned as a private internet providing connectivity across military bases and operational centers. Over time, DDN branched into four subnetworks which represented four separate military networks with differentiated security levels: Military Network (MILNET) for unclassified information; Defense Secure Network One (DSNET 1) for Secret information; Defense Secure Network Two (DSNET 2) for Top Secret information; and Defense Secure Network Three (DSNET 3) for Top Secret/Sensitive Compartmented Information. This division between networks defined by security level was maintained with the transition to the current network configurations.

SME-PED to DMCC-S

While the United States government has never been in the business of developing proprietary or publicly funded cell phone capabilities, it has certainly worked alongside and co-developed specific software and standards; and the impact of government needs and expectations cannot be underestimated in how it shapes and responds to markets. Mobile devices are an extremely vulnerable element of classified information infrastructure, and their rapidly increasing ubiquity outside of government contexts has presented significant challenges to ongoing security. The Secure Mobile Environment – Portable Electronic Device (SME_PED) program attempted to provide U.S. military personnel with a device that resembled the features and functionality of commercially available smartphone technology while simultaneously enabling interaction with SIPRNET at the secret level. As of 2011 the core elements of a SME-PED phone would involve four electronics boards at relative trust levels: a trusted crypto module, the semi-trusted black and red compute modules and an untrusted radio frequency (RF) module. The RF module would be easily removed and replaced allowing the device to operate on either the Global System for Mobiles (GSM) or as a Code Division Multiple Access (CDMA). In addition to cryptography, the crypto board crucially operates along the lines of a keyboard, video, and mouse (KVM) switch, enabling display sharing across multiple machines and allowing users to see what is happening on other machines. The devices also create a "trusted path," keeping the user informed of all security measures currently operating on any side of a networked interaction. SME-PED phones also support Common Access Cards (CAC), the standard form of identification for active duty uniformed service personnel, as well as Department of Defense civilian employees and a large number of contractors. This feature is an additional security measure, as CAC cards already act as crypto plugin providers for unclassified but sensitive email systems. The phones must also meet defense standards (MIL-SPEC) for environmental factors including heat and water, ensuring that these devices are more resilient than commercially available models. Instead of interacting with the security features within the Windows Mobile operating system, SME-PED devices are designed to rely on separate hardware in order to simplify security analysis. This also ensures that any attacks or external issues with the devices are contained to one compute module, representing an effective air gap between the levels of security within the phone. SME-PED phones require users to enter a personal identification number (PIN) in order to access the device. If the PIN is incorrect a certain number of times, the internal storage of the device will be zeroized, erasing stored data in addition to security protocols and parameters on the device. Although data is encrypted as it is stored and accessed, zeroization is authorized under a number of circumstances and remote zeroization is a feature of Research in Motion (RIM) Blackberry devices. Logistical and security challenges remained, as the phones remained extremely expensive, heavy and incompatible with convenient commercial products, and they entirely lacked the ability to crosswalk between civilian and military contexts. Security wise, the phones remain vulnerable when on “black” mode, as external agents can capture audio from the microphone and key presses from the keyboard, and CAC cards have allowed for the generation of digital signatures, should the software be compromised. These problems would be solved if the user only used the phone in its most secure “red” mode, but this is an unrealistic expectation given the reliance on the less secure mode for easy day-to-day communication.

Margaret Salter, a Technical Director in the Information Assurance Directorate stated in 2012 that the NSA was in the process of prioritizing commercial solutions. Of the development of the NSA’s Enterprise Mobility Architecture she said, “The plan was to buy commercial components, layer them together and get a secure solution. It uses solely commercial infrastructure to protect classified data."[145] Fishbowl, a mobile phone architecture providing secure voice over internet protocol (VOIP) capability, was unveiled the same year. It uses a modified Android operating system and both Secure Real-time Transport Protocol (SRTP) and Internet Protocol Security (IPSec) encryption protocols, which were developed through strong and sustained partnerships between corporate and government entities and funding streams. In October of 2012, the DoD announced that they were in search of industry partners to develop a secure communications system for just under 200,000 devices including iPhones, iPads and Android systems. Up to this point, Blackberry was the only commercial entity producing devices with approval to run secured email access to the Pentagon's unclassified networks.

In 2013, General Dynamics unveiled a software platform called GD Protected, which was designed to secure commercially available Android smartphone devices to the level at which they can handle classified information and communication. This represents a shift for General Dynamics in that GD Protected focuses on the operating system rather than just the hardware, creating a system in which a single processor core can run a dual operating system, either secure or unsecure. GD Protected is available for both the LG Optimus 3D Max and the Samsung Galaxy S IV, piggybacking onto the hardware security provided by the design of each device. Adding in two independent layers of encryption at both the voice over internet protocol (VOIP) and the virtual private network (VPN) level, GD Protected requires data to travel through servers at the NSA to be verified, logged and re-encrypted before going on to the carrier's network and its final destination. For the Samsung device, GD Protected comes as an addition to the KNOX platform co-developed by Samsung and General dynamics. KNOX has extensive security features geared towards protecting stored, sent and received data, and creating isolated areas

[145] Tarantola, Andrew. (2012) "NSA Agents Will Make All Their Calls with a Fishbowl." Gizmodo. Retrieved August 1, 2016. http://gizmodo.com/5889505/nsa-agents-will-make-all-their-calls-with-a-fishbowl

within the phone for secure communications. Each element of KNOX is designed as compliant with federal standards for security, a Federal Information Processing Standard (FIPS) approved VPN client. On May 3, 2013 the DoD announced that devices equipped with the Samsung KNOX platform were approved for use on DoD networks in addition to Blackberry 10 phones, the Playbook tablet and the Blackberry Enterprise Service 10. At that point, these devices were still only approved to access unclassified networks, and the only mobile devices approved for classified networks were the GD Sectera Edge and a test version of the Motorola Razr Maxx. As of 2014, Samsung Galaxy Note 4 and Galaxy S 5 became the first commercially available smartphones to be approved for having access to classified networks.

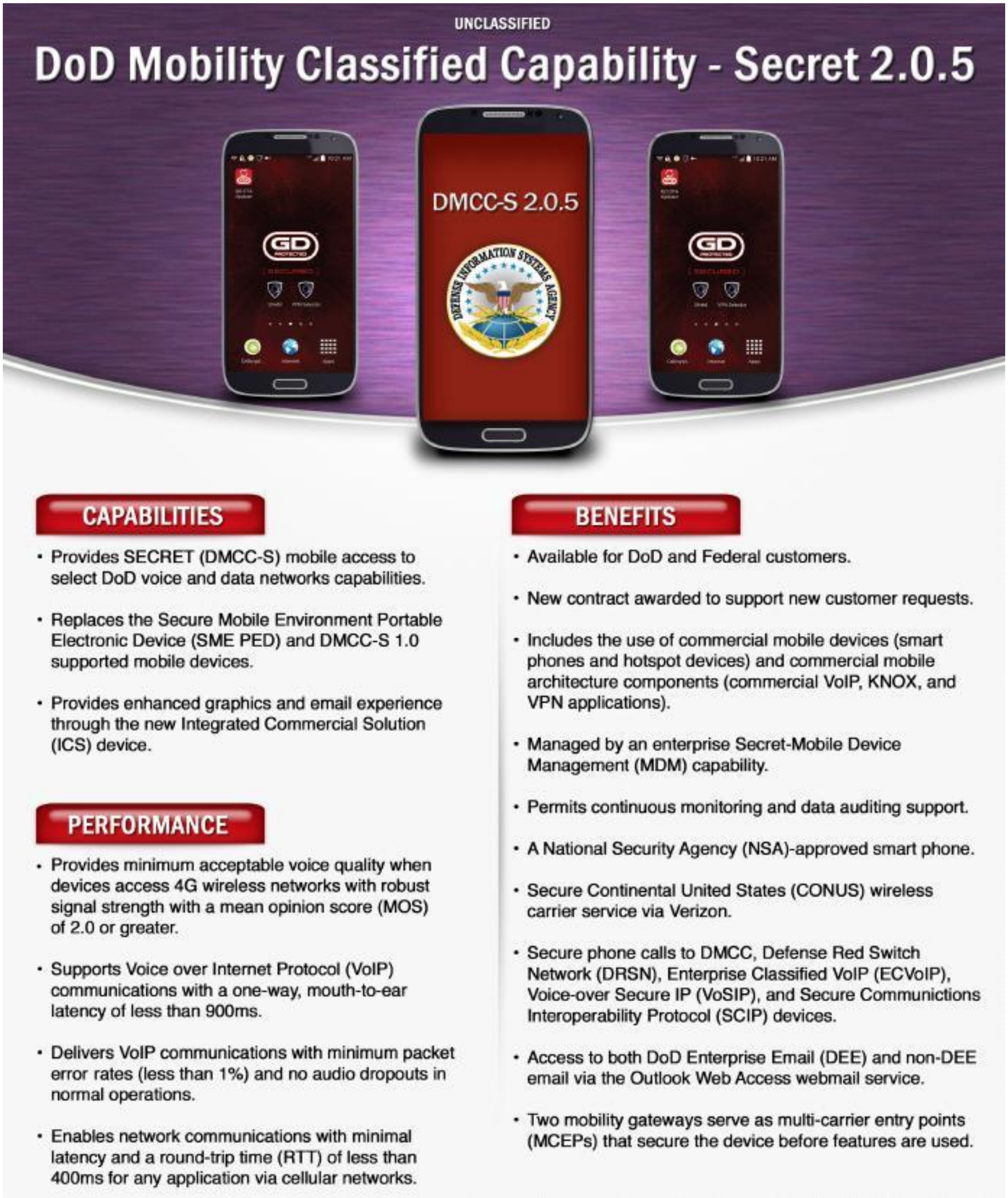
In 2015 GD Protected moved out of the pilot stage and what is now known as the Defense Mobile Classified Capability – Secret (DMCC-S) officially replaced SME-PED. This represents a complete move toward commercial smartphones with enhanced security features. DMCC-S phones, in addition to containing the security features outlined previously, are also distinctive because they have camera, GPS and Bluetooth entirely disabled. Signifying a move toward what the DoD called their Joint Information Environment plan, which would enable soldiers and government officials to access classified information "from any device, anytime, anywhere."[146] This goal requires economies of scale in order to provide devices to a reasonable number of people who need access to classified communications networks. In addition to the DOD the NSA has prioritized partnerships with commercial entities and corporations with the formation of the Commercial Solutions for Classified Program (CSfC). CSfC positions commercial products at the heart of its plan, prioritizing cost effectiveness and emphasizing

[146] McCaney, K. (2015). NSA Rolls Out New Classified Smartphone System. Defense Systems. Retrieved August 2, 2016. https://defensesystems.com/articles/2015/06/24/disa-classified-mobile-capability.aspx

"market-place competition."[147] Although General Dynamics has been at the forefront of developing tools for classified communication, Boeing has also thrown its hat into the ring with the development of Boeing Black, which signals a new test-phase for devices that can operate in

[147] National Security Agency. Commercial Solutions for Classified (CSfC) Brochure. Retrieved August 2, 2016. https://www.nsa.gov/resources/everyone/csfc/assets/files/handout-trifold.pdf

Top Secret environments. [148]


DMCC-S 2.0.5
DEFENSE INFORMATION SYSTEMS AGENCY
GD

UNCLASSIFIED

DoD Mobility Classified Capability - Secret 2.0.5

CAPABILITIES

- Provides SECRET (DMCC-S) mobile access to select DoD voice and data networks capabilities.
- Replaces the Secure Mobile Environment Portable Electronic Device (SME PED) and DMCC-S 1.0 supported mobile devices.
- Provides enhanced graphics and email experience through the new Integrated Commercial Solution (ICS) device.

PERFORMANCE

- Provides minimum acceptable voice quality when devices access 4G wireless networks with robust signal strength with a mean opinion score (MOS) of 2.0 or greater.
- Supports Voice over Internet Protocol (VoIP) communications with a one-way, mouth-to-ear latency of less than 900ms.
- Delivers VoIP communications with minimum packet error rates (less than 1%) and no audio dropouts in normal operations.
- Enables network communications with minimal latency and a round-trip time (RTT) of less than 400ms for any application via cellular networks.

BENEFITS

- Available for DoD and Federal customers.
- New contract awarded to support new customer requests.
- Includes the use of commercial mobile devices (smart phones and hotspot devices) and commercial mobile architecture components (commercial VoIP, KNOX, and VPN applications).
- Managed by an enterprise Secret-Mobile Device Management (MDM) capability.
- Permits continuous monitoring and data auditing support.
- A National Security Agency (NSA)-approved smart phone.
- Secure Continental United States (CONUS) wireless carrier service via Verizon.
- Secure phone calls to DMCC, Defense Red Switch Network (DRSN), Enterprise Classified VoIP (ECVoIP), Voice-over Secure IP (VoSIP), and Secure Communictions Interoperability Protocol (SCIP) devices.
- Access to both DoD Enterprise Email (DEE) and non-DEE email via the Outlook Web Access webmail service.
- Two mobility gateways serve as multi-carrier entry points (MCEPs) that secure the device before features are used.

Figure 3: DMCC-S Fact Sheet from Defense Information Systems Agency

“Smartphones” at the Top

Before President Obama took office in 2009, he made a seemingly impossible request at the time, to keep his smartphone. In many ways, his identity as a candidate was tied to his facility with technology, his ease with communication and his connection to a seemingly more tech-savvy generation. Judith Butler suggested that this was a part of a broader strategy of disidentification with the previous administration.[149] As president-elect he was quoted as saying, “I’m clinging to my BlackBerry. They’re going to pry it from my hands.”[150] The insistence on keeping his device led to the creation of an NSA lab in which dozens of people reportedly worked on making the BlackBerry secure. NSA Technical Director Richard George framed the issue in familiar light, casting functionality as vulnerability.[151] The more a phone can do, the more vulnerable it is. In addition, any phone with which this BlackBerry communicated needed to have the same protections in place. Obama kept a highly-secured version of his BlackBerry under specific conditions. Not only did everyone with access to the accounts tied to the phone have to attend a briefing from the White House counsel, but also the messages themselves were designed to prevent forwarding.[152] In many ways, high government officials are expected to work in a state of deprivation when it comes to basic technologies and tools for communication and interaction, and it is the case that although Obama was constantly photographed with his BlackBerry by White House photographer Pete Souza, those photos always showed him in

[148] Tucker, P. (2016). The NSA Chief Has a Phone for Top-Secret Messaging. Here’s How it Works. Defense One. Retrieved December 13, 2016. http://www.defenseone.com/technology/2016/11/nsa-chief-has-phone-top-secret-messaging-heres-how-it-works/132845/

[149] Marez, C. (2009). Obama’s BlackBerry, or This Is Not a Technology of Destruction. *journal of visual culture*, *8*(2), 219-223.

[150] Clifford, S. (2009). For BlackBerry, Obama’s Devotion is Priceless. New York Times. Retrieved October 20, 2016. http://www.nytimes.com/2009/01/09/business/media/09blackberry.html

[151] Fink E. (2014). I Made Obama’s BlackBerry. CNN. Retrieved October 12, 2016. http://money.cnn.com/2014/05/22/technology/security/nsa-obama-blackberry/

[152] Zeleny, J. (2009) For a High-Tech President, a Hard-Fought E-Victory. Retrieved October 12, 2016. http://www.nytimes.com/2009/01/23/us/politics/23berry.html

motion, in transit, in public space. In contrast, photos of him in the field or performing official business typically showed him using direct, wired lines of communication. The list of NSA approved devices in 2009 was a short one, and Obama's exception was truly singular. Then Secretary of State Hillary Clinton sought a similar exception to keep her smart phone and was denied,[153] and was offered use of the Sectera Edge instead (the L3 Communications Guardian was still in development). Technically, the Sectera Edge could not be labelled a smartphone and instead had more in common with the personal digital assistants (PDAs) that dominated the early 2000s. The Edge required a host of supporting products to be set up and synchronized with a desktop, and required separate specific accessories for both its secure and non-secure modes. For $4,750.00, the government could purchase the Executive Kit which included: Type 1 Sectéra® Edge™(GSM or CDMA) device plus: Executive Carry Case, Leather Holster Travel Charger, Red/Black USB Cables, Vehicle Charger, Earbud, Stylus 10-pack, microSD Card with User Manual, Spare Battery, Privacy Shield 4-pack, Antivirus Software, Apriva® Email Client and Perpetual Rights fee and Office Suite for Windows® CE. In addition, the government would also have to purchase a separate Apriva email server, annual licenses for each mail client, server support, AntiVirus maintenance, different phone modules for US and international use, and training. A heavily redacted email exchange from February 17, 2009 marked SECRET illustrates the ongoing back and forth over Clinton's use of her BlackBerry, as she requested permission to use it in the field inside of the SCIF. The response from the NSA further confused the point, "Sometimes the distinction between what can be done and what is, or is not, recommended to be done differently; this is one of those instances."[154]

[153] Gallagher, S. (2016) This is the phone NSA suggested Clinton use: A $4,750 Windows CE PDA: SME PED devices were only NSA-approved mobile phones for classified communications. Retrieved October 12, 2016.

[154]

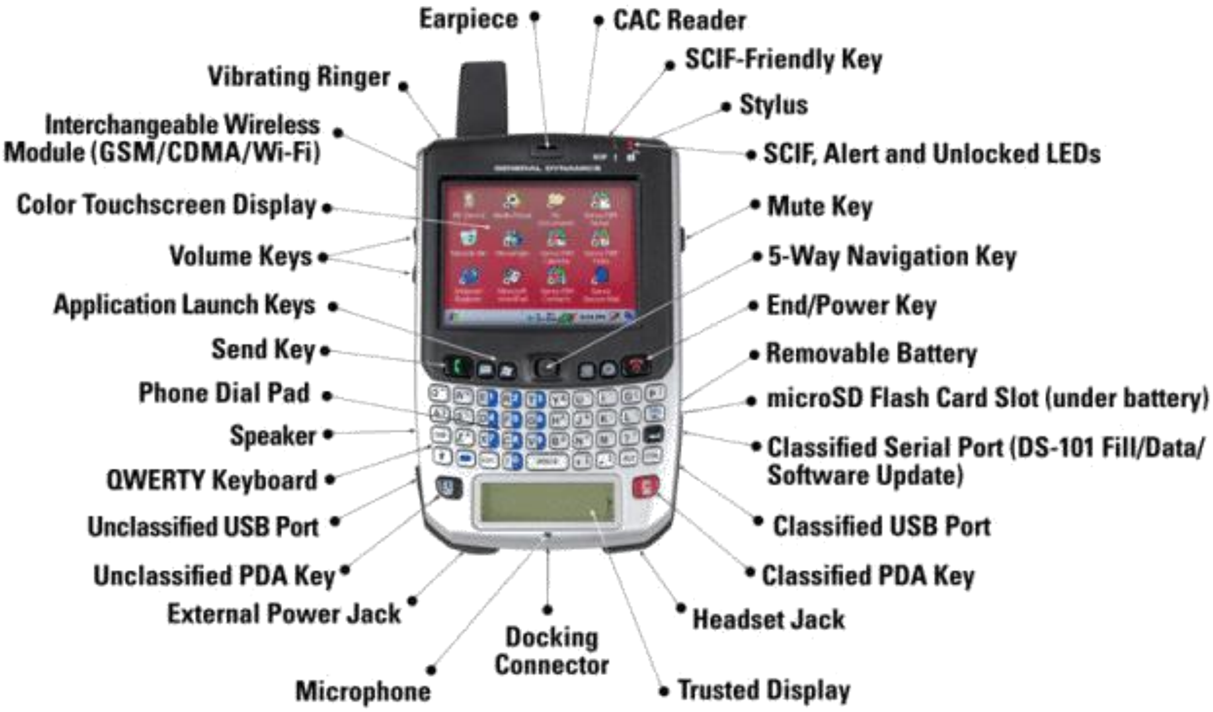


Figure 4: General Dynamics Sectera Edge - Discontinued

Classified Records

Apart from the security concerns and constraints that lead to use of devices with such extraordinarily limited communications capability, compared to commercially available smartphones, they present an especially difficult proposition for records management and archival work. These infrastructural arrangements mean that records are not merely the result of transactional work but also that they are produced within a blend of proprietary formats. As Amelia Acker explored in her dissertation work on the history of the SMS and its impact on archiving text messages, while the legal infrastructure is in place to demand recordkeeping of electronic communications, the technical infrastructure is not in place to follow through with those demands.[155]

[155] Acker, A. (2014). Born Networked Records: A History of the Short Message Service Format. P. 173.

These complications force us to reconsider what exactly we mean by record in this context? As we look towards crafting solutions that leverage expertise across security experts, archivists, records managers and legislators, we must determine what, if anything, we are trying to capture first and foremost. Definitions of ‘record’ necessarily proliferate throughout the multiple contexts in which records are of interest. In this particular case, the definition of record used by legislators is meant as declaration of commitment to knowledge sharing with the public and a directive for the work of archivists and records managers. This dual function makes the definition necessarily broad and diffuse. The definition of record from the Federal Records Act is:

> Records include all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of the data in them (44 U.S.C. 3301).

A few terms in this definition jump out as being especially useful in ascertaininghow the government understands its own relationship to records, record-keeping and archives, namely: evidence and informational value. The National Archives and Records Administration defines evidential value as “the value of records or papers as documentation of the operations and activities of the records-creating organization, institution, or individual,”[156] and there are almost 14,000 mentions of the word evidence in the Federal Code of Regulations that range in their level of specificity with relation to their institutional or juridical context. Although neither of these definitions provide us with an understanding of how something comes to be understood as evidence, within a legal context, authenticity is one of the primary requirements for determining

[156] Evidential Value [def. 1] National Archives and Records Administration. Glossary of Terms. Retrieved October 12, 2016. https://www.archives.gov/research/alic/reference/archives-resources/terminology.html

the admissibility of evidence. Before any record can be admitted into evidence, it must be authenticated by analyzing the context of record creation that is determined to be reliable, testimony or expert judgment (*Federal Rules of Evidence,* Rule 901). The state of authentication in terms of the legal context is in flux as the complexity of technological systems, the distributed nature of documentary forms and the relative technological expertise of involved parties leave traditional methods of assessment and determination wanting. Legal standards and expertise simply cannot keep up with technological change, and a system based on precedent is hard pressed to develop legal standards for new systems and their forms and formats. [157]

In his exploration of modernity's specific evidential paradigm, Carlo Ginzburg develops an argument founded on Jeremy Bentham's proclamation that evidence is fundamentally relational.[158] Ginzburg is explicit about the temporal relationship expressed by evidence; it remains a trace of what was once a contemporaneous action. He identifies this as venatic deduction, establishing part to whole, with an indexical quality relating past to present. By emphasizing the relationship between the form of evidence and action, Ginzburg gives us a clue to consider records as evidence, as their very form does not just point us to an activity but is also in some ways, a continuation of that activity.

While it cannot possibly stand entirely outside of the sphere of influence of modern evidential paradigms, archival studies has necessarily developed its own unique relationship to evidence and evidential value. Archival work has grown alongside and out of governmental and juridical contexts, but it also is concerned fundamentally with the management of and access to

[157] For further discussion of concepts of authenticity, see Chapter Four.

[158] Bentham, J. (1827). *Rationale of Judicial Evidence: Specially Applied to English Practice* (Vol. 5). Hunt and Clarke. P. 17
Ginzburg, C., & Davin, A. (1980, April). Morelli, Freud and Sherlock Holmes: clues and scientific method. In *History workshop* (pp. 5-36). Editorial Collective, History Workshop, Ruskin College.

and use of records. So rather than understanding evidence as relational through indexicality, what evidence is to whom and when it is has become a central subject of investigation and debate throughout the last century. In his *A Manual of Archival Administration*[159], Sir Hilary Jenkinson expressed a narrow and pointed definition of archival materials, defining them in the strictest terms of governmental business. Jenkinson equates the status of records as evidence with their production in the daily business and transactions of governmental work, their creation then somehow outside of bias or contingency. T.R. Schellenberg later distinguished and separated informational value and evidential value[160] but remained focused on governmental and administrative records. NARA defines informational value as "the value of records or papers for information they contain on persons, places, subjects, and things other than the operation of the organization that created them or the activities of the individual or family that created them."[161] Evidential value derives from evidence of the organization and functioning of a particular governmental agency or office, whereas informational value derives from evidence of who and what that agency dealt with. This understanding of records containing dual values, both evidential and informational, is clearly embedded in our legislative language, identifying records as containing evidence of the body producing records, as well as the people and issues involved in the production and circulation of that record.

Evidence becomes through "processes of social negotiation after the fact."[162] In order to facilitate these negotiations, however, preserving context and authenticity have been core tasks of archival work, maintaining records that are unchanged from their accession to their use. This

[159] Jenkinson, H. (1965). A manual of archive administration.

[160] Schellenberg, T. R., & Jones, H. G. (1956). *Modern archives: principles and techniques* (pp. 225-231). Chicago: University of Chicago Press.

[161] https://www.archives.gov/research/alic/reference/archives-resources/terminology.html

[162] Informational Value [def. 1] National Archives and Records Administration. Glossary of Terms. Retrieved October 12, 2016. https://www.archives.gov/research/alic/reference/archives-resources/terminology.html

context and authenticity does not have any bearing on whether the contents of the record are true or reliable. Within this infrastructural context, we are confronted by layers of challenges precipitated by media specificity. Previous attempts at codifying electronic recordkeeping have struggled with how to handle media specificity even as they tried to grapple with the increasing necessity of cross institutional partnerships.[163] It is clear from the description of the infrastructural landscape within this chapter, that even just considering the definition contained in the Federal Records Act requires a massive overhaul in practice to contend with the recognition and preservation of informational and evidential value as it would require retaining the record in its dynamic and overlapping infrastructural arrangement; including everything from proprietary corporate software to multiple security layers across communicating devices.

Although much more radical ideas directly challenging and destabilizing these traditional concepts of the record and evidence have been circulating within Archival Studies for decades, their reach into governmental arenas and/or implementation have yet to materialize. As records become increasingly inseparable from networked technologies and a multiplicity of platforms and infrastructural arrangements, it is worth considering what the techniques and concepts of records continuum thinking might contribute to the work of governmental records. The continuum approach eschews the linearity of the life-cycle model that moves records through from creation to disposition to preservation, conceptualizing each of these as a separate stage that clearly precedes and follows the other.[164] By contrast, the continuum model focuses on the movement and activity of records as well as their imbricated evidentialities. Instead of

[163] Cox, R. J., & Duff, W. (1997). Warrant and the definition of electronic records: questions arising from the Pittsburgh Project. *Archives and Museum Informatics*, *11*(3), 223-231.
Duranti, L., & MacNeil, H. (1996). The protection of the integrity of electronic records: an overview of the UBC-MAS research project. *Archivaria*, *42*.

[164] Atherton, J. (1985). From life cycle to continuum: some thoughts on the records management–archives relationship. *Archivaria*, *21*, 43-42.

understanding records in terms of stages, continuum theory places records within four dimensions: records creation, capture, organization of recordkeeping processes and pluralization.[165] The Records Continuum Model (RCM) has produced a multitude of frameworks situating records as dynamic entities within a range of ideas concerning the relative importance of material constraints. Frank Upward has asserted that records no longer should be considered physical entities but instead as logical entities.[166] Following this, the physical and material context of record creation, management and flow ceases to be tied to its authenticity. While RCM and noncustodial models of records and archival management proliferate, legal constraints continue to insist on the relationship between physical custody and authenticity. This leaves archivists and records managers in a double bind; challenged by shifting conceptual paradigms that understand records in a multiplicity of contexts and recognizing the limitations of juridical-evidentiary frameworks for collective memory, human rights work or social justice while still having to create and maintain systems that facilitate transparency and authenticity according to traditional understandings. Infrastructural thinking about records shifts the lens from the individual record to the system of its production and maintenance, facilitating a bridge between these shifting paradigms. Rather than thinking of records as fixed or in flux, we can understand them as systemic, allowing us to both capture and value not just their movement through space-time but also their capacity for a variety of meaning-making.

[165] McKemmish, S. (2001). Placing records continuum theory and practice. *Archival science*, *1*(4), 333-359.

[166] Upward, F. (1997). "Structuring the records continuum – part two: structuration theory and recordkeeping". *Archives and Manuscripts*. **25** (1): 10–35

Chapter Three: …but her emails or Spectacle and Rupture in Classified Information Infrastructure

Introduction

> The ranks of officials in this judiciary system mounted endlessly, so that not even the initiated could survey the hierarchy as a whole. And the proceedings of the Courts were generally kept secret from subordinate officials, consequently they could hardly ever quite follow in their further progress the cases on which they had worked; any particular case thus appeared in their circle of jurisdiction often without their knowing whence it came, and passed from it they knew not whither. Thus the knowledge derived from a study of the various single stages of the case, the final verdict and the reasons for that verdict lay beyond the reach of these officials. [167]

The crime of Joseph K. in Kafka's *The Trial* is a moving target, and his quest to understand exactly what it is he is on trial for represents the impossibility of the individual's confrontation of the wholly bureaucratic. He cannot see the system in its entirety and each layer pushes him into deeper confusion and frustration, a never-ending chain of referents. Citizens are simultaneously subject to the law and remote from it, shaped by constraints but unable to discern the boundaries, made all the more extreme by bureaucracy's most defining characteristic, tedium. The view of bureaucracy in *The Trial* is totalizing, opaque and never-ending. These features contribute to what Max Weber conceptualizes as the most powerful aspect of bureaucratic organization, inertia. A "settled orientation"[168] that provides a serene backdrop against which change and transition can occur is both a precursor and an effect of the organization and management of administrative artifacts. In considering classified information as bureaucratic infrastructure, this settled orientation becomes troubled.

In her essay "The Ethnography of Infrastructure," Susan Leigh Star defines the generalizable characteristics of infrastructure, one of which is that it is "visible upon

[167] Kafka, F. (1937). The Trial, trans. Willa Muir, Edwin Muir, and EM Butler.
[168] Star, S. L. (1999). The ethnography of infrastructure. *American behavioral scientist*, *43*(3), 377-391.

breakdown." Star and others have pointed to breakdown as a unique moment of visibility for infrastructure as a relational phenomenon, to see exactly the junctures at which standards, technology and the stuff of infrastructure fails to fulfill its function. Within the context of classified information, this breakdown is typically the rule rather than the exception, classified information infrastructure is almost spectacularly flawed, and the majority of experience that lay people have with classified information is through perpetual breakdown, or what I would like to refer to as rupture. I choose rupture in this instance because it has a certain suddenness to it, rather than the sense of a gradual wearing away. Classified information infrastructure does not breakdown from overuse or from gradual erosion or neglect, although its misuse and abuse might be routine, its breakdown is punctuated instead of singular. This rupture comes in myriad forms: leaking, hacking, misuse, overuse, design flaw, legal contradiction and theft, to name a few. Hacking has become so commonplace that in 2014 James Comey, then Director of the Federal Bureau of Investigation (FBI), characterized American corporations as belonging to one of two types, those who have been hacked by the Chinese and those who do not yet know they have been hacked by the Chinese.[169] More than once sensitive, redacted documents were quickly uncovered due to the misuse of an Adobe redaction tool, someone had to simply copy and paste text into a Word document to reveal the redacted information. Technologies approved for use with classified information are often outdated, poorly coordinated or inconvenient, failing to adequately deal with the complexity of networked records. The last decade has seen some high-profile leaks of classified information including those of Chelsea Manning and Edward Snowden, both of whom characterized their actions as essential checks against what they have

[169] Tadeo, M. (2014). FBI's James Comey Accuses China of Hacking into Every Major American Company. Independent. Retrieved October 12, 2016. http://www.independent.co.uk/news/business/news/fbis-james-comey-accuses-china-of-hacking-into-every-major-american-company-9777587.html

alternately described as an ever-growing and destructive secrecy state.[170] In the first few months of 2017, leaks from within the White House, the Intelligence Community and the State Department have been relatively consistent, exposing the somewhat routine use of leaks as both coordinated and uncoordinated forms of communication. Alternately, one element of rupture within the context of classified information infrastructure that is less publicly discussed is the contradiction contained within rules and regulations themselves. Hilary Clinton's use of a private email server throughout her tenure as Secretary of State serves as an ideal case study for the ways in which these possibilities for rupture coalesce, and how these ruptures transform into competing rhetorics, evolve into controversy and are framed as spectacle within classified information infrastructure.

Mapping a Controversy

Controversy mapping is a methodological and pedagogical tool stemming from concepts developed by Bruno Latour in *Reassembling the Social: An Introduction to Actor-Network Theory*.[171] While it relies on visualizing the competing constituencies and narratives across disciplines and professional circles, I adapt controversy mapping here without visualization in order to describe the complexity and interconnectedness of networks of information, technologies, policies and political entities. Much like infrastructural inversion, controversy mapping relies on switching figure and ground in order to enable focusing on particular layers as a part of the whole. Latour's four recommendations provide an entryway into processing the complexity of controversies. He begins by positing that one should attempt to avoid simplifying

[170] Delmas, C. (2015). The Ethics of Government Whistleblowing. *Social Theory and Practice*, 77-105.
Farrell, H., & Finnemore, M. (2013). The end of hypocrisy: American foreign policy in the age of leaks. *Foreign Affairs*, *92*(6), 22-26.
Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the US surveillance state*. Macmillan.

[171] Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford university press.

the individual propositions that enter into the discussion, thus capturing perplexity. Secondly, he maintains that in order to accurately and completely portray controversy, including the largest number of perspectives possible is ideal. Thirdly, when taking new propositions into account, you should compare and contrast pre-existing propositions in order to identify commonalities. Fourthly, once propositions are taken into consideration, they must be considered legitimate going forward. There are some obvious drawbacks and limitations to these four recommendations, least of which begins with his lack of definitional work on terms such as legitimate and proposition. However, what we can take from them is the importance of due diligence to the representation of a multiplicity of vantage points and although he falls short of identifying why, legitimacy of perspective is at the core of controversy. In analyzing the Clinton email server scandal, each of the constituencies is defined by their relationship to legitimacy, including the classified system at large, its justifications, the technologies in use, the investigatory body assessing the aftermath, and the media and multiple publics. Extending this Latourian framework with the aid of Yochai Benkler's concept of the "networked public sphere," allows us to think of the grounds for the development and circulation of a controversy as media ecology that encompasses social media, traditional media outlets, non-professional news outlets and, in this case, the possibility of external state intervention.[172]

Records Management in the State Department

"Slower than molasses running uphill in winter." – Roy Wood Jr.

[172] Benkler, Y. 2006. *The wealth of networks: How social production transforms markets and freedom*. New Haven, Conn.: Yale University Press.
Benkler, Y., Roberts, H., Faris, R., Solow-Niederman, A., & Etling, B. (2015). Social mobilization and the networked public sphere: Mapping the SOPA-PIPA debate. *Political Communication*, *32*(4), 594-624.Retrieved February 2, 2017. http://cyber.law.harvard.edu/node/8416,

An issue at the heart of the Clinton controversy that is highly misunderstood by those outside of archival and record-keeping professional communities is that of records management. One cannot begin to discuss the potential impediments and/or loopholes involved in managing classified information contained in emails without understanding the foundational challenges in email management at the federal level. In the eyes of the law and in the daily practices of the National Archives and Records Administration (NARA), what is a record, which records should be kept and how should those records come to NARA? The Archivist of the United States determines which federal records warrant permanent preservation, which records should be transferred to NARA and which should be made available for public access. This power, derived from The Federal Records Act in conjunction with 44 U.S.C. Chapters 21 and 29, extends to the retention and disposition of federal records. NARA estimates that less than five percent of records produced and managed by the federal government should be considered possessing permanent archival value and thus require custodial transfer to NARA from individual agencies. All federal records are required to be kept for a period of time, those not thought to have permanent value may be destroyed after they are no longer necessary for the immediate needs of the agency, and when their use for public or legal accountability has expired. Email has been a challenge for federal agencies and by extension for NARA as well. The legacy records management practices and protocols entrenched within daily agency work placed the responsibility of email records management on each individual end-user, including the decision to determine whether or not the email would be considered a record or non-record as well as whether it required retention based on the content of each individual email. Over time agencies adopted ad hoc “print-and-file” policies, leaving the user to print out all electronic records, not just email, for official filing. Bizarrely, this printed copy was then considered the official recordkeeping version, the “record copy.” Print-and-file persisted as the cost of implementing a new recordkeeping system prevented many agencies from doing so, leading to concerns over the results of ad hoc and mixed recordkeeping practices across agencies such as the potential loss of permanently valuable email. Printed emails also do not contain information crucial to determining the document’s authenticity including metadata. In addition, the sheer volume and speed at which email communication is produced within and across agencies made print-and-file untenable. Despite the passage of legislation by Congress in 2007 requiring email records to be managed electronically, instances of mismanagement have continued to plague the federal records management landscape. As so often is the case, legislation and mandates does not always come with funding attached, particularly when it comes to NARA. In 2014 alone, three separate incidents characterized the stakes of email records management. Lois Lerner, the former head of the tax-exempt status department of the Internal Revenue Service (IRS) became central to an investigation into the circumstances surrounding the application of added scrutiny regarding the tax-exempt status of Tea-party affiliated groups. Although roughly 67,000 emails with Lerner as the sender or the receiver were produced, two years-worth of email had purportedly disappeared. The details of how the IRS managed their email became the subject of both critique and skepticism. The IRS backed up data on its email server, which runs Microsoft Outlook, at the end of each day. These backups were then kept on digital tape for six months. Additionally, the IRS maintained a policy that kept employee email storage space on the email server at 500 megabytes. Since emails considered official records cannot be deleted, IRS employees saved official records locally and determined whether or not email rose to the standard of “appropriate for preservation as evidence of the government’s function or activities, or valuable because of the information they contain."[173] To make matters more complex, Lerner's computer crashed in 2011, right during the period of contention. Although she contacted technical support to assist her in recovering data from her hard drive, it was impossible and policies did not require individual machines be backed up.[174] In August of 2014, records management official Kathleen Cantwell at the Centers of Medicare and Medicaid Services (CMS), the agency in charge of the implementation of the Affordable Care Act, informed the National Archives of a breach in records management policy. A letter stated that some of Marilyn Tavenner's emails, a CMS administrator, had been deleted. Gina McCarthy, an administrator at the Environmental Protection Agency (EPA), was also prompted to inform Congress that the agency was incapable of accessing a number of emails belonging to a scientist working on a mining project assessment that had become the center of some controversy.

Throughout the last decade, NARA has consistently revised and published regulations and guides for electronic records and email management. In 2010 NARA put together the Email Management 2.0 working group wherein the Capstone Approach was researched and put forth as guidance across agencies. This, in conjunction with an Email Management webpage[175] and the Records Management Toolkit,[176] aimed at an audience of records managers and information officers within agencies rather than on individual users or federal employees. In tandem with President Barack Obama's signing of the Presidential Memorandum on Managing Government Records in 2011 and the issuance of Managing Government Records Directive (M-12-18) by the

[173] Bump, P. (2014). Here's how the IRS lost Emails from Key Witness Lois Lerner. The Washington Post. Retrieved February 2, 2017. https://www.washingtonpost.com/news/the-fix/wp/2014/06/16/heres-how-the-irs-lost-emails-from-key-witness-lois-lerner/?utm_term=.44f588435601

[174] Ibid.

[175] National Archives and Records Administration. Email Specific Guidance and Resources and Capstone Training and Resources. Retrieved February 2, 2017. https://www.archives.gov/records-mgmt/email-mgmt

[176] National Archives and Records Administration. Records Management Toolkit. Retrieved February 2, 2017. https://www.archives.gov/records-mgmt/toolkit

Office of Management and Budget and NARA, NARA published bulletin 2013-02, Guidance on a New approach to Managing Email Records. This bulletin advocated for the implementation of the Capstone Approach which attaches the determination of final disposition to the role of the sender/receiver rather than the content of the email, replacing email by email review and consideration by individuals, and categorizing entire email accounts as permanent or not. The bulletin, however, stands as a suggestion rather than a mandate, and further encourages the use of automated solutions to block capture based on specific email accounts and duplicates. It also suggests a radical shift in disposition authorities. In this bulletin, NARA acknowledges that many problems stem from individual users lacking awareness regarding specific disposition authorities. Instead of asking individual users to determine and mark emails according to content and disposition authority, the Capstone Approach allows agencies to propose a unique disposition schedule that considers email as its own record series rather than individual records within other series. NARA also developed a General Records Schedule (GRS) in an attempt to minimize the individualized records schedules proposed by individual agencies. Previously, these individual records schedules were proposed, open for public comment and then approved or not by NARA. The GRS provides disposition authority in three items: Item 010, Item 011 and Item 012. Item 010 outlines the disposition authority for the email of senior officials, including a definition of officials in ten categories: head of the agency; principal assistants to the head of the agency; deputies of all positions in categories 1 and 2; staff assistants to those in categories 1 and 2; principle management positions; directors of significant program offices; principal regional officials; roles or positions that routinely provide advice and oversight to the agency; those roles and positions filled by Presidential Appointment with Senate Confirmation; and any other positions that predominantly create permanent records to "mission critical functions or policy decisions or policy decisions and/or are of historical significance."[177] This item specifies itself as not media neutral and therefore applies only to electronic records. Additionally, it extends to any legacy email accounts and any email accounts in which agency business is done. Item 011 extends to all other officials not outlined in the previous item and sets a minimum retention of seven years for all email records. This would govern the majority of agency email traffic, signifying a fairly drastic increase in the minimum retention standard for most agencies. NARA's justification for this retention schedule suggests that seven years would be adequate in providing information for litigation as it is in line with general statute of limitations standards.[178]

FAM/FAH

In 2005 the State Department codified and published a sixteen-part manual, the Foreign Affairs Manual (FAM), that contains just under seven thousand references to classified information. This manual was developed in the midst of the George W. Bush administration, in which twenty-two million emails were "lost." The administration too used a private email server, in this case owned by the Republican National Committee. It was also non-compliant with laws governing government records and ignored a Congressional subpoena regarding the emails. The Presidential Records Act (PRA) was passed by Congress in 1978, mandating that all presidential and vice presidential created after January 20, 1981 be preserved and maintained. The PRA also mandated that presidential records are public materials. Although the first White House email system was installed and used by the Ronald Reagan administration, both the Reagan and George H.W. Bush administrations failed to maintain their email records. A 1989 federal law

[177] National Archives and Records Administration (2016). General Records Schedule 6.1: Email Managed Under a Capstone Approach. Retrieved February 2, 2017. https://www.archives.gov/files/records-mgmt/grs/grs06-1.pdf
[178] National Archives and Records Administration. White Paper on Capstone Approach and Capstone GRS. P. 12 https://www.archives.gov/files/records-mgmt/email-management/final-capstone-white-paper.pdf

suit designed to compel the White House to comply with the existing standards put forth by the PRA was filed by a number of groups, and inspired a court order preventing over 6,000 email backup tapes containing copies of White House emails from being erased. The George H.W. Bush administration additionally established a singular agreement with the National Archives and Records Administration (NARA) allowing George H.W. Bush to treat his White House emails as personal records. The lawsuit was settled with the Bill Clinton White House, and the email system implemented within the White House came complete with a pop-up notifying the user that deletion would be a violation of the PRA, when and if someone tried to delete an email. These measures did not however guarantee that guidelines were followed, as is evidenced by continued problems with email within the Clinton White House.[179] In 2003, a whistleblower came forward to the National Security Archive, informing them that the George W. Bush White House was not saving its emails. Alongside Citizens for Responsibility and Ethics in Washington, the National Security Archive refiled its previous lawsuit. The automated email system that had been in place during the Clinton White House had been discontinued and the "lost emails" began on January 1, 2003.

These lost emails were potentially at the core of cases involving the White House, including the purportedly political firing of several United States attorneys, and the case of the retaliatory outing of CIA agent Valerie Plame. In 2008, lawyers working for the administration claimed that a bad system upgrade had caused the loss of up to five million emails, including email backups from the lead up to the invasion of Iraq. Later they admitted that, contrary to original estimation, they had lost up to twenty-two million emails. In December of 2009, the Barack Obama White House found a similar number of emails dated between 2003 and 2005 that

[179] Woodbury, M. (1995). Clinton, Reno, and Freedom of Information: From Waldheim to Whitewater. *Social Justice*, *22*(2 (60)), 49--66. Retrieved from http://www.jstor.org/stable/29766878

had been mislabeled and, although the emails were handed over to the National Archives at the time and the lawsuit was settled, the emails would not be made available to the public as the majority of them were ineligible for declassification until 2021. The Senate Judiciary Committee's report on the firing of U.S. attorneys, in turn, seemed to imply that the email disappearances were a refutation of the assertions of the unintended consequences of system upgrades, problems in IT, or that Karl Rove's email deletion was simply a matter of "the type of routine deletions people make to keep their inboxes orderly."[180] The report stated "This subversion of the justice system has included lying, misleading, stonewalling and ignoring the Congress in our attempts to find out precisely what happened. The reasons given for these firings were contrived as part of a cover-up, and the stonewalling by the White House is part and parcel of that same effort." The wholesale disappearance of this number of emails is unlikely, but whether or not the National Archives has the resources to commit to restoring and making this kind of material available once it is declassified is another matter. As Thomas Blanton of the National Security Archives has stated, "Their entire budget is less than the cost of a single Marine One helicopter. It's an underfunded orphan."

So it is against this backdrop that the FAM and FAH (Foreign Affairs Handbook) were published. Like all manuals and guidelines, it derives authority from a collection of statutes, Executive Orders and previous iterations of similar instructional texts. In this case, section 5 FAM 752[181] which outlines the protocols and guidelines for managing email derives its authority from nine sources including: Privacy Act of 1974 as amended (5 U.S.C. 552 (a)); Freedom of

[180] Henry, E. & Goddard, L. (2007) White House: Millions of e-mails may be missing. CNN. Retrieved February 2, 2017. http://www.cnn.com/2007/POLITICS/04/13/white.house.email/index.html?_s=PM:POLITICS
(2007) Missing e-mail may relate to firing of U.S. attorneys. New York Times. Retrieved February 2, 2017. http://www.nytimes.com/2007/04/13/world/americas/13iht-justice.4.5281466.html
[181] Burleigh, N. (2016) George W. Bush White House 'Lost' 22 Million Emails. Newsweek. Retrieved February 2, 2017.
http://www.newsweek.com/2016/09/23/george-w-bush-white-house-lost-22-million-emails-497373.html

Information Act (FOIA) of 1966, as amended; privacy exemptions (5 U.S.C. 552(b)6 and (b)7(c)); Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et. Seq.); E-Government Act of 2002, Section 208 (44 U.S.C. 3602); Safeguarding against and Responding to the Breach of Personally Identifiable Information, M-07-16 (May 22, 2007); 35 CFR Parts 1220, 1222, 1228, and 1234 Electronic Mail Systems August 28, 1995; Executive Order 13526, Classified National Security Information; 1 FAM 271.5 and 5 FAM 113; and The Federal Records Act (44 U.S.C. 31). It is important to note that while other sections of the FAM have been routinely updated in the intervening years, this particular section has not. Authority derivation is at the heart of compliance expectations, as the assumption is that one who follows the instructions in this manual is compliant with each and every statute. The manual stresses limited personal use, the avoidance of features such as “reply all,” as well as the avoidance of anything that could slow down messaging or create backlog and the possibility of consistent monitoring of email use. The transmission of Sensitive But Unclassified (SBU) information is also outlined, which is sanctioned with a series of outlined reservations concerning the risks of transmitting personally identifiable information (PII) through unencrypted networks. Classification and sensitivity markings for email are briefly mentioned here, but are further explored in 5FAH-2 H-440, 5 FAM 460 and 5 FAH-3 H-700.

The onus of determining whether or not emails qualify for retention lies with both the originators and recipients of the email. When using SMART, this too is potentially automated, a user can simply click the “Convert to Archive” button in Microsoft Outlook to enable sending the email chain to the Archive where it is retained and available for SMART searches. The FAM asserts that email messages are records when and if they meet the definition of a record as stated in the Federal Records Act (44 U.S.C. 3301). In other words, emails are records when they are "made or received by an agency under Federal law or in connection with public business and are preserved or are appropriate for preservation as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government, or because of the informational value of the data in them."[182] The FAM further expands this into plainer language for users, outlining that the following must be marked for preservation: "records that document important meetings; records that facilitate agency officials' and their successors' action; records that make scrutiny by the Congress or other duly authorized agencies of the Government possible; and records that protect the financial, legal, and other rights of the Government and of persons directly affected by the Government's actions." Throughout the FAM, the simple missive that email should be treated just like paper records, attempting to situate new practices within familiar territory, especially for those with limited experience with digitally mediated recordkeeping, prevails. SMART retains two types of "record emails" including "directly addressed messages sent to one or more individuals; and for the record messages sent directly to the Archive." Curiously, since this section has not been updated since 1995, as it was adapted from previous statute, so the section on preservation of emails is glaringly inadequate both to instructing users and in its assessment of available technology and expertise. I reproduce this section in its entirety here, as I believe this reveals some of the most obvious internal contradictions within classified information infrastructure in addition to revealing both the impossibility of full compliance and the shifting priority from investing in human judgment to building an automated system. This also taps into an issue inherent to the genre of manuals, which are meant as working reference guides rather than texts to be memorized or read for pleasure. However, simply looking up guidance for preserving email records would yield just

[182] Federal Records Act. 44 U.S.C. 3301.

under 200 results, and the only one bestowed with the specific moniker of “how to” has not been updated since 1995, having little to do with the preservation standards and techniques which have since been partially automated through SMART.

> 5 FAM 443.3 How to Preserve E-Mail Records
>
> *(TL:IM-19; 10-30-1995)*
>
> For those E-mail messages and attachments that meet the statutory definition of records, it is essential to ensure that the record documentation include the E-mail message, any attachments, and essential transmission data (i.e. who sent the message, the addressees and any other recipients, and when it was sent). In addition, information about the receipt of messages should be retained if users consider it necessary for adequately documenting Department activities. If transmission and necessary receipt data is not printed by the particular E-mail system, the paper copies must be annotated as necessary to include such data. Until technology allowing archival capabilities for long-term electronic storage and retrieval of E-mail messages is available and installed, those messages warranting preservation as records (for periods longer than current E-mail systems routinely maintain them) must be printed out and filed with related records. Instructions for printing and handling of Federal records for most of the Department’s existing E-mail systems have been prepared and will be available through bureau Executive Offices[183]

This is followed by a promise that the Department is attempting to develop technology that would be capable of properly dealing with email and other forms of electronic communication. This also has remained without an update. Part of this section was indeed updated in 2015, containing guidance for the use of “Non-Official Email Accounts”

[183] 5 FAM 443.3

SMART and "Print-and-File"

The State Messaging and Archival Retrieval Toolkit (SMART) was introduced in 2009. It was designed to enable State Department employees to preserve emails and diplomatic cables through Microsoft Outlook. The system stored records centrally, facilitated access to material department wide and represented a coordinated attempt to "move away from what was a text-based, telegram-type messaging system."[184] Previous to SMART, employees were consigned to printing and filing in order to preserve records, and it should be noted that upon its introduction, the Office of the Secretary declined use of the system due to concern over controlling access to sensitive and classified materials.[185] Reports from the Office of the Inspector General have noted that since the implementation of SMART, use across agencies has varied quite widely.[186] However, in 2012 the Office of Management and Budget and NARA issued a joint memorandum mandating that agencies eliminate paper-based recordkeeping with respect to email, and transition to managing all email records in an electronic format by December 31, 2016.[187] In 2013, NARA then published a bulletin granting agencies the authority to use the Capstone Approach to managing email records. Among other things, this approach collects and manages based on the role of the recipient or sender of the email rather than focusing on the content of the email, allowing for easier compliance with federal statutes governing records management and preservation.

[184] Government CIO Magazine (2012). Interview with Susan H. Swart, CIO, Department of State. Accessed and Retrieved December 12, 2016. https://www.youtube.com/watch?v=WmxMRJzQgxU&feature=youtu.be

[185] Office of Inspector General U.S. Department of State Broadcasting Board of Governors (2016) Office of the Secretary: Evaluation of Email Records Management and Cybersecurity requirements. ESP-16-03. Retrieved January 6, 2017. https://oig.state.gov/system/files/esp-16-03.pdf

[186] OIG, Review of State Messaging and Archive Retrieval Toolset and Record Email (ISP-I-15-15, March 2015) and OIG, Inspection of the Bureau of Administration, Global Information Services, Office of Information Programs and Services (ISP-I-12-54, September 2012).

[187] OMB and NARA, Memorandum for The Heads of Executive Departments and Agencies and Independent Agencies: Managing Government Records Directive (OMB Memorandum M-12-18) (August 24, 2012)

In January of 2015, the Executive Secretary of State produced a memorandum to the offices of the Secretary, the Deputy Secretaries of State, the Under Secretary for Political Affairs and the Counselor of the Department that informed that starting in February of 2015, all email in their State Department accounts would be permanently retained stating, “You should not use your private email accounts (e.g., Gmail) for official business.”[188]

Hillary Clinton took office as Secretary of State in January of 2009 and that same month, an aide for former President Bill Clinton registered the clintonemail.com domain name and Hillary Clinton began to use hdr22@clintonemail.com. In this same year, the U.S. Code of Federal Regulations was updated to specifically refer to email accounts, stating that if personal email accounts were to be used for agency business, that it is the agency’s responsibility to ensure that the emails are preserved according to federal regulation and within the agency recordkeeping system. After Clinton stepped down as Secretary of State, NARA updated their guidelines regarding personal email accounts, stating that they should only be used in “emergency situations,” and repeating that if personal emails are used that they must be preserved in accordance with agency recordkeeping practices. In 2014, President Barack Obama signed the Federal Records Act which emphasized the responsibility of agency heads in the documentation and preservation of agency activities.

In the aftermath of the death of four Americans in the attack on a United States diplomatic outpost in Benghazi, Libya, investigations begin into how the incident was handled by the State Department, in general, and by then Secretary of State Hillary Clinton, specifically. In December of 2012, Darrel Issa, then chairman of the House Oversight Committee, asked Hillary Clinton about her possible use of a private email account in a letter to the State

[188] Memorandum To All Assistant Secretaries, Assistant Secretary Equivalents, And Principal Deputies: Email Retention (July 29, 2015).

Department and was met with a formal response that did not answer that specific question. After Clinton left office in 2013, the investigation into the incident in Benghazi found correspondence between Clinton’s private email account and government accounts of her staff and other agency employees. After the initial hearings on Benghazi, then House Speaker John Boehner created a select committee in May of 2014 to investigate the circumstances surrounding the attack as well as the government response. Negotiations regarding wholesale access to Clinton’s emails from the period in question begin with some urgency in July of 2014. Cheryl D. Mills, Clinton’s former chief of staff assured the select committee that they would gain access but that it would take time, within the month the State Department provided the committee on Benghazi 15,000 pages of documents including a small number of emails from Clinton’s private email account. In January of 2015, in response to a formal request by the State Department, Clinton produced 55,000 printed pages of more than 30,000 emails. It is not until February of 2015 that the State Department acknowledges that Hillary Clinton relied exclusively on her personal email account as Secretary of State. During this period, Clinton asked the State Department to release her emails to the public, and simultaneously acknowledged that during the course of her tenure she had deleted 32,000 personal emails from her personal account. It took close to a year to redact and publicly release the 30,000 emails originally handed over to the select committee and in this time, Hillary Clinton announced her candidacy for President of the United States, increasing media and official scrutiny of her email management practices. In July of 2015, investigators found classified information in emails from Clinton’s private server. The emails were not marked as classified when originally sent/received and therefore did not contain proper markings that would have alerted the sender to their status. The appearance of classified information however, prompted investigators to refer to the Justice Department and it did not take long for the Federal

Bureau of Investigation (FBI) to open an investigation. In January of 2016, the State Department announced that it would not release twenty-two emails that were classified as Top Secret. This classification was applied and elevated after the fact, for these too were not marked when they were sent/received.

The Office of the Inspector General released a report in May of 2016 reviewing the legacy of policies regarding email and records management. In this report, it is stated that in addition to Hillary Clinton, former Secretary of State Colin Powell used a laptop computer to send emails via his personal email account to his assistants, ambassadors and colleagues.[189] Additionally, Powell has told the State Department that he did not retain those emails in either electronic or "print-and-file" and that he remains ignorant about whether or not State Department systems captured any of his emails in agency servers. The report was careful to distinguish Powell's lack of compliance and Clinton's, as department policy had become much more nuanced and sophisticated regarding both electronic records management, in general, and email management, specifically. However, this report also describes widespread ignorance of and reluctance to use print and file methods within the State Department, noting that, "NARA stated that this lack of compliance exists across the government. Although the Department is aware of the failure to print and file, the FAM contains no explicit penalties for lack of compliance, and the Department has never proposed discipline against an employee for failure to comply."[190] Not to mention that even if print and file was a successful method of saving information, that is all it did, as no one was tasked with what would amount to an extremely labor intensive process of indexing thousands of printed emails. This is one of the issues meant to be ameliorated by the

[189] Office of Inspector General U.S. Department of State Broadcasting Board of Governors (2016) Office of the Secretary: Evaluation of Email Records Management and Cybersecurity requirements. ESP-16-03. Retrieved January 6, 2017. https://oig.state.gov/system/files/esp-16-03.pdf

[190] https://oig.state.gov/system/files/esp-16-03.pdf 17

introduction of SMART in 2009, but as with all other policies, “compliance varies greatly across bureaus, in part because of perceptions by Department employees that SMART is not intuitive, is difficult to use, and has some technical problems.”[191] The Capstone Approach was not implemented within the State Department until 2015, and this report states explicitly that it had plans to implement a commercial product to manage its email that will be capable of managing legacy email, enabling search, auto-tagging and security controls. The report goes on to describe in detail, the chaos that is State Department records management. Fairly consistently, claims that protocols and standards are being observed and maintained are followed by the exposure of practices that are spotty at best. For example, the Office of Information Resources Management (IRM) reported that it has maintained copies of email records through .pst files but had not created any form of inventory for the files. When further prompted, a considerable number of those .pst files were password protected and no one knew the password, or files were corrupted, incomplete or empty.[192] Another example, the FAM requires all employees to sign a statement of separation acknowledging and confirming that they have surrendered documentation related to their official business with the government upon their departure from the department. No Secretary since Madeline Albright has signed the DS-109 separation statement.[193] Although by October of 2016, the FBI investigation into Hillary Clinton had concluded, the FBI announced that it had discovered new emails they considered relevant to whether or not Clinton mishandled classified information. These emails were found on a seized device shared by Anthony Weiner

[191] OIG, Review of State Messaging and Archive Retrieval Toolset and Record Email (ISP-I-15-15, March 2015) and OIG, Inspection of the Bureau of Administration, Global Information Services, Office of Information Programs and Services

[192] Office of Inspector General U.S. Department of State Broadcasting Board of Governors (2016) Office of the Secretary: Evaluation of Email Records Management and Cybersecurity requirements. ESP-16-03. Retrieved January 6, 2017. https://oig.state.gov/system/files/esp-16-03.pdf p.
18 [193] Ibid p. 20

and Huma Abedin, an aide to Hillary Clinton. Ultimately, out of the emails turned over by Clinton, eight email chains included Top Secret information, thirty-six chains contained Secret information, 2,008 emails contained Confidential information. The vast majority of these classification designations were retroactive, so would not have been marked when sent/received initially.

A Generation of Controversy

On September 3, 2016 the FBI released both a summary of their interview with Hillary Clinton and a memorandum about the investigation. The investigation into whether or not any laws were broken with respect to the handling of classified information concluded that while Clinton's actions were "extremely careless," they did not warrant criminal charges, a result that was affirmed by Attorney General Loretta Lynch. However, the FBI investigation was not the only investigation into Clinton's use of a private email server and/or her handling of classified information. Judicial Watch, a conservative legal advocacy group, has brought a handful of lawsuits against the State Department under the Freedom of Information Act for records from Clinton's time there. In addition, although the Select Committee on Benghazi issued its final report, which found no evidence of wrongdoing on the part of Clinton, additional inquiries by the Senate Homeland Security Committee, the Senate Judiciary Committee and the Inspector General of the Intelligence Community have also been underway. There have been such a large number of requests for information regarding the Clinton email controversy that NARA has released and published forty-seven documents in response, addressing the intricacies of records management practices and policies with special attention to email records management. Not only has this information been coordinated and published, but there is an entire webpage on the NARA website devoted to disentangling State Department email policy, cataloging all media inquiries and appearances by NARA and State Department officials and tracking changes in policy over time.

Apart from the obvious chaotic nature of the records management environment within the State Department, there are several persistent issues that arise when considering the Clinton email controversy: the responsibility and requirements for marking classified information within the email environment; the responsibility and requirements for retention and deposit of email materials; the absence of a strategy for dealing with temporal disjunction in classification. These three issues also represent the ways in which classified information and archives and records management contexts are entirely inseparable, even as their policies are typically developed in isolation or contradiction to one another. When Sandy Berger walked out of the National Archives on two different occasions with classified documents hidden in his socks and pants,[194] it is a clearer determination of exactly who is at fault, what the intention might be, what the vulnerabilities are. In regards to Clinton's emails, the case exposes overlapping systematic failures in records management, classified information management and maintaining a consistent relationship to NARA. Diffuse problems within bureaucratic systems challenge notions of authority, culpability and responsibility that typically operate. The structures of legal culpability fail to consider the ways in which power, agency, and responsibility operate within bureaucratic contexts. The problem of "many hands,"[195] a central feature of bureaucratic organization that relies on many officials at different levels contributing to both the standards for behaviors as well as the behaviors themselves, makes it "difficult even in principle to identify who is morally

[194] Thompson, D. F. (1980). Moral responsibility of public officials: The problem of many hands. *American Political Science Review*, *74*(04), 905-916.
[195] Ibid.

responsible for political outcomes."[196] Typically, responsibility in government is considered in two ways, hierarchically and collectively. Within the hierarchical model, as outlined by Weber, responsibility for activities and their outcomes falls to the highest person within a formalized hierarchy. Here we also find a distinction between administrators and politicians, one who sets policies and one who executes those policies, relegating them to different regimes of responsibility respectively.[197] Furthermore, Weber effectively removes agency from the administrator, placing responsibility outside an individualized or collective understanding of morality. However, this does not resemble the contemporary configurations of bureaucratic labor and agency, and it could be argued that if this did at some point resemble a structure for interpreting moral responsibility, it should not have been. It is precisely this kind of diffusion of agency and responsibility that leads to routine abuses of power.[198] Apart from this, the distinction between politician and administrator collapses within complex bureaucracies, as officials routinely operate within "issue networks" that are rapidly and routinely shifting. In addition, officials are subjects within as well as elements of infrastructural networks that are at times inharmonious. Dennis Thompson describes the acceptance of hierarchical authority and blame as a kind of political ritual,[199] a display of control and responsibility without much political consequence. What Thompson does not consider is the highly gendered rhetorical economy of political discourse, in which the projection of strength and leadership might operate differently along gender lines. In contrast, collective responsibility acknowledges that culpability often resides in an exchange, namely that within an organization, it is exceedingly rare that any one

[196] Hall, R. H. (1963). The concept of bureaucracy: An empirical assessment. *American Journal of Sociology*, *69*(1), 32-40.
[197] Du Gay, P. (2000). *In praise of bureaucracy: Weber-organization-ethics*. Sage.
Weber, M. (1946). Bureaucracy. *From Max Weber: essays in sociology*, *196*, 232-235.
[198] Ibid.
[199] Thompson, D. F. (1987). *Political ethics and public office*. Harvard University Press.

person operates alone, especially in a case that results in political consequence. At its weakest, the collective responsibility model holds everyone accountable for everything or no one accountable at all, but routinely there are gradations of culpability according to implicit/inactive and explicit/active compliance. In this instance, we have the head of a Department working in a system that is riddled with policy holes and contradictions. If the series of reports by the Inspector General are to be believed, it was and is a relatively open secret that people were consistently in a state of noncompliance. Not only this, but that there is really no mechanism or will for enforcement with respect to records management and proper handling of information, until it reaches crisis. In an email to Hillary Clinton, a former Director of Policy Planning stated that "State's technology is so antiquated that NO ONE uses a State-issued laptop and even high officials routinely end up using their home email accounts to be able to get their work done quickly and effectively."[200]As we saw in the previous chapter discussing the difficulties in employee cell phone policy compliance, this is a common refrain with respect to using technology in the federal workplace. Compliance is often considered an impediment to efficient and effective work. The Inspector General's report went so far as to state that employees also avoided designating emails as records because they "do not want to make the email available in searches for fear that this availability would inhibit debate about pending decisions."

The question then remains, how exactly does Clinton's use of a private email server become controversy at an unprecedented scale, when all reports and investigations revealed widespread similar practices and an overall lack of expertise in managing email records across agencies? Although there are other high profile incidents involving classified information, rarely

[200] Office of Inspector General U.S. Department of State Broadcasting Board of Governors (2016) Office of the Secretary: Evaluation of Email Records Management and Cybersecurity requirements. ESP-16-03. Retrieved January 6, 2017. https://oig.state.gov/system/files/esp-16-03.pdf

has an incident garnered such attention without explicit intent on the part of the accused. The system itself, which is in many ways in a constant state of breakdown, is recast in the media and through public discourse as simple and knowable, casting Clinton then as spectacularly careless or nefarious. The legal framework governing the leaking, mishandling or theft of classified information is robust and diffuse. At its core is the Espionage Act of 1917, 18 U.S.C. § 793, which criminalizes such activities, but weds its successful prosecution to proof of intent of injuring the United States or aiding a foreign nation. Although the language of the Espionage Act does not specifically refer to classified information but to "national defense information," the very consideration of a record as classified belies its sensitivity and therefore its status could be used as evidence on its face of injury to the United States. A later amendment to the Espionage Act, 18 U.S.C. § 798, specified multiple forms of classified information, including the communication of intelligence activities, and importantly omits language concerning intent. Instead, the language foregrounds that the communication must be done "knowingly and willfully." A second law forming this larger legal framework is 18 U.S.C. §641, which is non-specific to classified information but instead refers to a general provision against theft of government property, including records. Additional laws take on more specific challenges, such as The Intelligence Identities Protection Act, which criminalizes the revelation of the identity of covert agents.

Customarily, investigations into the leaking of classified information are conducted by the Federal Bureau of Investigation under the supervision of The Department of Justice. Typically, the agency who produced and/or owned the classified information reports the leak or theft to the Department of Justice who determines whether or not an investigation is necessary and should be opened. Investigations are opened when and only when leaked information is confirmed.[201] However, at this point, there is no longer a typical order of events, as investigations are often subject to the rhetorical whims of partisanship and can be framed as retaliatory or without merit. The past few Administrations have seen fit to appoint special prosecutors when instances of leaking came to the fore, putting the investigation into the hands of law enforcement. It is a mistake to think about this or any controversy as a spontaneous or natural occurrence. In their book *Merchants of Doubt*,[202] Naomi Oreskes and Erik M. Conway trace the careers of a small number of scientists whose work contributed to several ongoing controversies, including climate change and the dangers of sustained tobacco use.[203] Rather than emerging out of established forms of debate and consensus building within scientific communities, these controversies are strategically funded and deployed by companies in whose interest they serve, and the doubt leveraged against scientific consensus is bolstered by the credentials and reputations of the scientists in question. Oreskes and Conway go on to contextualize the persistence and strength of these controversies as they become depicted by the media within a frame of false equivalence, and how the narrative of doubt becomes heroically situated as anti-establishment and anti-elite.[204] When considering Clinton's email server controversy, it is key to position its timing within the context of another controversy and associated conspiracy theories surrounding Clinton's tenure with the State Department: the attack on the United States consulate in Benghazi, Libya.

Those convinced that there was explicit wrong-doing were left with the desire for more information, the investigation did not yield the expected results and deferred confirmation of their belief not just in the events of the day, but those concerning Clinton's competence, at the

[201] Frontline Interview with David Szady. http://www.pbs.org/wgbh/pages/frontline/newswar/interviews/szady.html
[202] Oreskes, N., & Conway, E. M. (2010). Merchants of doubt.
[203] Ibid.
[204] Ibid.

very least, and her duplicitousness, at the very worst. After the release of the final report from the House Select Committee on Benghazi, *The Washington Post* reported the reactions of people attending a meeting of the Citizens' Commission on Benghazi, all of who expressed disappointment and skepticism. One woman is quoted as asking, "Has someone in the GOP leadership gotten their fingers involved in watering down some of this to benefit Secretary Clinton?"[205] The Citizens' Commission is still active, releasing their own research and reports, and now focused not just on uncovering the events leading up to the attack, but also in investigating the cover-up.[206] Right-wing conspiracy outlet InfoWars has published just under three thousand articles on Benghazi in the past five years, half of which explicitly claim that Hillary Clinton lied and/or hid information before, during and after the attack. Clinton's testimony in front of the House Select Committee became a referendum not only on her actions regarding Benghazi, but also played out in media as a test of her competence and authenticity; both double binds for Clinton as political roles and their defining attributes are cast as masculine, and analysis of women politicians is radically different in tone and content. An impossible challenge emerges for Clinton's rhetorical strategies with regard to the Benghazi hearings, one pitting femininity against competency within the political realm.[207] Further, femininity can be more specifically situated in this context as authenticity, insofar as any expression of emotional

[205] Milibank, D. (2016) Benghazi Conspiracy Theorists Turn on Trey Gowdy. Retrieved January 6, 2017. https://www.washingtonpost.com/opinions/benghazi-conspiracy-theorists-turn-on-trey-gowdy/2016/06/29/7c513ed4-3e44-11e6-80bc-d06711fd2125_story.html?utm_term=.f664eb8fccbf

[206] Citizens' Commission on Benghazi. Declaration of the Citizens' Commission on Benghazi. Retrieved. January 6, 2017. http://www.aim.org/benghazi/declaration-of-the-citizens-commission-on-benghazi/

[207] Jamieson, K. H. (1995). *Beyond the double bind: Women and leadership*. New York, NY: Oxford University Press.

identification or involvement was considered not only false but also highly calculated for political aim.[208]

The controversy over Clinton's use of a private email server emerges from not just the political theater of the Benghazi hearings, but from decades of analysis of Clinton's behaviors in both official and personal capacities. Quite literally too, the revelations concerning Clinton's use of a private server came from disclosures made during the investigation into Benghazi, as Williams & Connolly, Clinton's legal team turned over 55,000 pages of email to the State Department for review. If controversy and conspiracy theory thrive on the breakdown of trust in institutions and leaders, sustained media circulation of stories about Hillary Clinton sowed the seeds, which is not to say that Clinton's use of a private email server does not expose a range of deep seated issues regarding the complexities and pitfalls of the current records management framework within the federal government. An ad hoc strategy for communications technology represents a significant challenge to records management, signified by a lack of coordination, technological expertise and enforcement and oversight. The consequences of this are noteworthy within a framework that conflates appropriate records management practices with achieving transparency and accountability for those who hold public office. This relationship between records, transparency and accountability is at the core of the controversy's proliferation, and the ease with which political adversaries were able to leverage pre-existing stereotypes concerning Clinton to draw conclusions about intent. In many ways the depiction of the use of a private email server, and the subsequent fallout over email deletion that circulated in the media, relies on massive coordination and technical expertise. This runs counter to the results of the FBI investigation itself which revealed Clinton's own aversion to and lack of comfort with

[208] Harp, D., Loke, J., & Bachmann, I. (2016). Hillary Clinton's Benghazi Hearing Coverage: Political Competence, Authenticity, and the Persistence of the Double Bind. *Women's Studies in Communication*, *39*(2), 193-210.

technology, the general disorganization within her team, and the poor navigation of classification and regulatory systems that have decades to go before catching up with the basic technology use found within most business contexts.

The Investigation

On July 10, 2015, the FBI began their investigation into Clinton's use of a private email server. The investigation was initiated as a result of a referral received by the US Intelligence Community inspector General (ICIG), urging the FBI to look into "the potential unauthorized transmission and storage of classified information on the personal email server of former Secretary of State Hillary Clinton (Clinton)."[209] The FBI's investigation took on a more narrow focus, attempting to zero in on the possible transmission or storage of classified information on unclassified systems as well as whether or not that classified information was potentially accessible to unauthorized individuals. In late 2016, the FBI released its Form 302 interviews with Hillary Clinton and various aides along with their investigatory summary of her use of a private email server, outlining their results but also the chain of events leading up to 2016.

Justin Cooper, a former aide to President Bill Clinton purchased an Apple OS X server to host email services for the President's staff. That server was kept in the Clinton home in Chappaqua, New York and originally hosted both presidentclinton.com and wjcoffice.com, both used by the President's staff. Before Hillary Clinton was sworn in as Secretary of State in 2008, she used a personal BlackBerry with service from Cingular (at first) and AT&T (finally). In January of 2009 Clinton stopped using the email associated with her BlackBerry device and began to use a private domain, clintonemail.com, to host email on the Apple server in her Chappaqua home. At this time, the Apple server had become outdated and Bryan Pagliano was

[209] U.S. Department of Justice Federal Bureau of Investigation (2016) Clinton E-Mail Investigation: Mishandling of Classified – Unknown Subject or Country (SIM). P. 1

brought in as an information technology specialist to build a new server system and help with administration. In interviews, Pagliano has said that he assumed this server would be used by President Clinton's staff and Hillary Clinton claims to have been entirely unaware of the server transition. Pagliano ultimately requisitioned hardware for this second email server from Hillary Clinton's 2008 presidential campaign headquarters in Arlington, VA and purchased additional necessities from various commercial outlets; the server was eventually installed in the Clintons' basement in their Chappaqua residence. Pagliano then migrated email data from the Apple Server to the new server, however the FBI was unable to obtain the Apple server[210] to conduct a forensic investigation, so the extent to which the necessary data was transferred is unknown. Pagliano and Cooper served in various roles as IT assistance with respect to the server, conducting updates and installing additional security measures (including a Secure Sockets Layer (SSL) encryption certificate).[211] It is noted in the FBI report that Clinton said she had "no knowledge of the hardware, software, or security protocols used to construct and operate the servers."[212] An entire backup of the server was made on a weekly basis to a Seagate external hard drive and a differential backup was completed everyday from 2009-2011, when that hard drive was replaced with a Cisco Network Attached Storage (NAS) device.

In 2013 a combination of the need for increased technical support and Pagliano's own exit from staff necessitated finding a new vendor to manage the email server. Platte River Networks (PRN) was eventually awarded the contract and a Service Level Agreement was

[210] This Apple server was subsequently used as a personal computer for household staff. All remaining data was transferred to an iMac in 2014 and according to a review done by Clinton's legal team Williams & Connolly LLP, there was nothing on the iMac from Clinton's tenure as Secretary of State.

[211] SSL is a security protocol that is used to establish an encrypted connection between the server and any other machine, enabling the transfer of sensitive information in an encrypted format.

[212] U.S. Department of Justice Federal Bureau of Investigation (2016) Clinton E-Mail Investigation: Mishandling of Classified – Unknown Subject or Country (SIM). P.5

signed on July 13, 2013.[213] An employee of PRN powered down the Pagliano server in June of 2013 and sent it to a datacenter run by Equinix, Inc., where it remained until it was handed over to the FBI in 2015. At this point, no functioning hardware remained at the Clinton home in Chappaqua. In June of 2013, PRN remotely migrated email accounts from the Pagliano server to the PRN server and PRN took over hosting email services for the Clintons.[214] PRN had Datto, Inc. configure a backup device to take multiple snapshots of the server system on a daily basis that were then to be retained for a period of 60 days. While the snapshots were meant to be stored locally only, a the request of the Clintons, a technical oversight disclosed in 2015 revealed that Datto had also been backing up the server to Datto's secure cloud storage.[215] Interviews also revealed that although the Clintons requested that email be encrypted, so that no one but the senders/receivers could read the content, PRN did not configure email settings in this manner, citing that they needed to allow administrator access to provide service support.[216] In terms of security, PRN did set up two firewalls and used an Intrusion Detection System called CloudJacket.

Clinton's BlackBerry usage was also linked with each server throughout the period investigated. The FBI ultimately identified thirteen mobile devices that had been associated with her known phone numbers, any of which could have been used to send and receive emails using the clintonemail.com addresses. Of these thirteen identified devices, eight were used during her tenure as Secretary of State, but none of the devices were available at the time of the investigation.[217] Additionally, the FBI identified five iPad devices potentially used to send email.

[213] Ibid.

[214] Ibid.P. 6

[215] U.S. Department of Justice Federal Bureau of Investigation (2016) Clinton E-Mail Investigation: Mishandling of Classified – Unknown Subject or Country (SIM). P. 7

[216] Ibid.

[217] Ibid. 8

Ultimately, here they found e-mails from 2012 in a drafts folder that were determined not to contain any potential classified information. The location of Clinton's discarded mobile devices are unknown apart from two instances recalled by Justin Cooper in which he "destroyed Clinton's old mobile devices by breaking them in half or hitting them with a hammer."[218] No mention is made of resetting or wiping devices of data by anyone on Clinton's team or in the FBI report.

At the start of her term as Secretary of State, the State Executive Secretariat's Office of Information Resources Management (S/ES-IRM) offered Clinton a State email address. That offer was declined, favoring the continued use of the private email server previously established. Although at the time of Clinton's tenure, the FAM required the day-to-day operations of the State to be conducted via an "authorized information system," it is held by those involved that Clinton did not transition to an authorized system nor seek guidance on email as a system in question.[219] Stories regarding who and when people raised concerns or gave advice are mixed and inconclusive although Clinton has claimed that knowledge of her use of a private server must have been widespread. However, there was no official restriction during Clinton's tenure concerning using private accounts for official business, despite the fact that information regarding using personal accounts was circulated and generally warned against due to security risks. Security risks were also cited as the reason for opting out of the SMART system as it would have provided broader access to sensitive materials, leaving Clinton's office with the "print and file" method.

[218] Ibid. 9

[219] U.S. Department of Justice Federal Bureau of Investigation (2016) Clinton E-Mail Investigation: Mishandling of Classified – Unknown Subject or Country (SIM). P. 10

In terms of records management and preservation, there are indications that this was a concern for Clinton from the beginning of her tenure. One of the most curious episodes of this entire saga is Clinton's missive to former Secretary of State Colin Powell in early 2009 regarding his use of a BlackBerry during his tenure. Powell explicitly warns Clinton stating that "if it became 'public' that Clinton had a BlackBerry, and she used it to 'do business,' her e-mails could become 'official recor[s]and subject to the law' and "Be very careful. I got around it all by not saying much and not using systems that captured the data."[220] For her part, Clinton says she believed all necessary records would have been retained anyway, as she communicated with others' official State email accounts.

Interestingly, the Secretary of State's office is located within a Sensitive Compartmented Information Facility (SCIF). Known as "Mahogany Row," this area of the State Department maintains restrictions on the use and carrying of mobile devices. Clinton's office at State did not even have a computer and her personal devices were stored outside of the SCIF. In fact, Clinton also built a SCIF in her residence in Washington D.C. and in Chappaqua, and staff have stated that she never used a desktop computer and used her mobile devices alone to access email accounts.

Classified Information on the Server

Whether it was characterized as careless or intentional, the release of classified information was at the heart of the controversy and legally at that of the FBI's investigation. Hundreds of emails classified CONFIDENTIAL were sent or received by Clinton while she was traveling outside of the continental United States (OCONUS). The FBI also identified three email chains that included eight individual email exchanges to or from Clinton's personal email

[220] Ibid. 11

accounts which contained at least one paragraph marked (C). This marking could be an indication that the paragraph contained CONFIDENTAL information, but these messages contained no additional control markings. Through the FOIA review process, only one of these chains containing the marking (C) was determined to contain CONFIDENTIAL information, and it is undetermined whether or not this was a contemporary or retroactive classification. This little (C) became somewhat of a point of contention in testimony by FBI Director James Comey on why charges were not being brought up on Clinton. An exchange between Comey and Representative Matt Cartwright (D-PA) addressed widespread confusion regarding what, if anything, the (C) marking would have meant to Clinton. Comey clarifies that (C) was an inappropriate or mistaken marking and not even an expert could have been expected to recognize its meaning. [221]

Ultimately, there were 81 email chains containing 193 individual email exchanges that were classified from CONFIDENTIAL to TOP SECRET levels at the time the emails were drafted on UNCLASSIFIED systems and sent to or from Clinton's personal server. These 81 email chains also contained classified equities from five other agencies including the CIA, DoD, FBI, National Geospatial Intelligence Agency (NGA) and the NSA. Out of these, 8 chains were classified TOP SECRET, 37 were classified SECRET and 36 were classified CONFIDENTIAL at the time they were sent. In addition, 7 email chains had information related to a Special Access Program (SAP) and three email chains contained Sensitive Compartmented Information (SCI). 36 of these chains were Not-Releasable to Foreign Governments (NOFORN) and 2 were considered releasable only to Five Allied partners (FVEY). Sixteen of the email chains were

[221] Transcript of Live Coverage of FBI Director James Comey's Testimony on Clinton's E-Mails. Aired 11-11:30 AM July 7, 2016. Retrieved January 6, 2017. http://transcripts.cnn.com/TRANSCRIPTS/1607/07/ath.01.html

downgraded later by USIC agencies.[222] At least 32 classified email chains went through the personal email account of Clinton or the personal email accounts of close Clinton aides.

Interviews providing context for these numbers and the habits that lead to transmission of classified information reveal a daily acceptance of contradiction and workaround. One informant related that he knew information was classified but that speed and efficiency remained a priority. Stating, “you just can’t do business that way,”[223] he alludes to the complexities of the classification system. Another interviewed talked of the “operational tempo,” and noted that employees were constantly “talking around” classified information, not to mention that information considered classified was routinely already public knowledge.[224] Perhaps the most impactful result of the FBI investigation regards Clinton’s own knowledge of protocol, procedure and her own role in classified information infrastructure. While Clinton does acknowledge that she knew her position made her an Original Classification Authority (OCA), she did not recall ever receiving formal training or guidance on the matter and could not identify “how the classification of a document” is identified, instead relying on staff to guide her on specific policies.[225]

Perpetual Breakdown

This episode represents a visible rupture in the functioning of classified information infrastructure. Visible is the key here, as knowledge from within communities dealing on a daily basis with classified information would seem to suggest that while the behavior is routine and the problems common knowledge, the coverage and persistence of this story is what is remarkable.

[222] U.S. Department of Justice Federal Bureau of Investigation (2016) Clinton E-Mail Investigation: Mishandling of Classified – Unknown Subject or Country (SIM). P. 21

[223] Ibid. 24

[224] U.S. Department of Justice Federal Bureau of Investigation (2016) Clinton E-Mail Investigation: Mishandling of Classified – Unknown Subject or Country (SIM). P.
25 [225] Ibid. 26

Elizabeth Gotein, the co-director of the Brennan Center for Justice's national security program, has pointed out that "Classification is not an adjective; it's a verb."[226] This is a verb that operates at a distinct temporal register, one that is slower and more deliberate than the day-to-day "operational tempo" of the government, where reaction times and quick communication dominate information needs. This episode shows us the spectacular version of the mundane reality of inadequate training programs, redundant regulatory documents and procedures, out of date technology and the complexities of systems that cross vendors, proprietary technologies and professional boundaries. However, what this episode also puts on display is the rhetorical fusion of recordkeeping with transparency, accountability without nuance, and the media vacuum that can fill the void of secrecy with exaggeration, bias and conspiracy. Classified information infrastructure is indeed made visible in a particular way through rupture, but what it exposes is the perpetual breakdown endemic to classification work.

[226] Williams, L. (2015). The Issue Everyone is Missing in the Hillary Clinton Email Scandal. Retrieved January 6, 2017. https://thinkprogress.org/the-issue-everyone-is-missing-in-the-clinton-email-scandal-a8a1b824151f

Chapter 4: The Majestic Twelve: Classification, Evidence and Conspiracy

Introduction

Conspiracy theories have a unique place in American political discourse, their most virulent believers often cite a deep mistrust of the government as a core American value, forming identities and communities around a shared set of norms and evidence, and pitting their version of history or current events against the mainstream. David Brion Davis has, in looking at the fears and paranoias of early American political operatives, wondered if the circumstances and realities of the American Revolution forever aligned steely resistance to dark subversive forces with an essential part of a national identity.[227] The rhetorical invocation of contagion to invasion is familiar territory, and has arisen around disparate political movements and populations. From Jewish refugees described by President Franklin Roosevelt as a possible "Trojan horse," to rather familiar language from J. Edgar Hoover describing the "Trojan horse of Communist fifth column." Peter Knight identifies the 1960s, in general, and the assassination of President John F. Kennedy, in particular, as a cultural shift in which conspiracy theory thinking eked out into the American cultural mainstream. One might see this period of great political division and unprecedented surveillance of the American population as leading to an erosion of trust in government action and accountability. Also during this time, one of the most prominent and strongest set of interlocking conspiracy theories was beginning to crystallize; the known existence and government cover up of extraterrestrial life rose to the surface and has only gained traction with each passing year. The study of conspiracy theories and those that espouse them have ranged from political philosophical discussions, psychological diagnoses and other forms of

[227] Davis, D. B. (1971). *The fear of conspiracy: Images of un-American subversion from the revolution to the present* (Vol. 113). Cornell University Press.

pathologizing, but rarely have the ways in which conspiracy theorists form consensus around particular forms of evidence been considered as central to their functioning, reach or potential staying power. The relationship of any conspiracy theory community to evidence is complex, as the nature of conspiracy implies a lack of mainstream consensus and therefore a lack of accepted evidence. Conspiracy theories often rely on a calling forth of common sense, asking one to fill in the blanks in a list of tangentially related factors. While the possibility of the existence of extraterrestrials, intelligent or otherwise, remains a matter of debate and speculation for scientists and laypeople alike, the belief that the United States government knows of and covers up the existence of extraterrestrial life has grown into a vibrant and persistent conspiracy theory. For believers in this generation long coordinated cover up, proof comes in a variety of forms. While eyewitness testimony defines the majority of support for confirmed experiences with extraterrestrials, evidence of conspiracy requires different elements. Many believers invest substantive time, money, and effort into collecting, analyzing and authenticating evidence apart from eyewitness testimony. This chapter will consider a set of documents that have come to serve as definitive proof for some believers that the so-called Majestic Twelve (MJ-12) exists. They will be discussed in order to define and examine the role of the infrastructure of classified information in how these documents are perceived as evidence, both within communities that might be labeled conspiracy theorists as well as within the government agencies that supposedly authored the documents. The infrastructure of classification allows for these documents to circulate beyond and through levels of expertise and domains of knowledge, and to challenge practices of authentication and our assessment of evidentiary value. This chapter will begin by providing context for the MJ-12 as it functions in Ufology circles, as well as the discovery and subsequent investigation into the authenticity of unearthed documentation. I will then discuss the relationship between classified information and conspiracy theories at the infrastructural level. Then I will describe and analyze methodologies of authentication coming from ufology within the context of both diplomatics and critical bibliography as a means of deconstructing the evidential claims set forth by these documents, analyzing how their claims to authority arise through the aesthetic deployment of classification markings and institutional affiliation. This process runs counter to the ways in which these documents are presented and contextualized by the National Archives. Finally, I will discuss the documents of MJ-12 within the framework of "imagined records" set forth by Anne Gilliland and Michelle Caswell in order to get at the ways in which these records function across evidential boundaries, and persist not just in spite of but because of secrecy and absence.

The Majestic Twelve

In the winter of 1984, filmmaker and amateur ufologist Jamie Shandera found a manila envelope that had been anonymously and surreptitiously dropped through his mail slot. The envelope contained no information, no explanatory note or missive referring to its purpose apart from a New Mexico postmark. Contained inside was a single undeveloped role of 35mm film. The film, later developed by Shandera and his colleague and fellow ufologist Bill Moore, would prove to contain what would then be considered the bulk of existing evidence of a secret government organization. The Majestic Twelve is the code name of an alleged secret committee of scientists, military leaders, and government officials formed by a 1947 Executive Order authored by President Harry Truman, itself classified. The documentary evidence for the existence of The Majestic Twelve or MJ-12 included two documents, which would come to be known as the Eisenhower Briefing Document and the Truman-Forestall memo. Although this would not be the first mention of The Majestic Twelve entirely, it was the first to touch the inner circle of ufology, and these documents would become inextricable from key debates concerning government behavior with respect to the existence of extraterrestrials, the possession of alien technology and what is characterized by some ufologists (and some government officials) as a sustained campaign of disinformation on the part of government agencies. Moore and Shandera spent the next several years attempting to authenticate the documents through research in the National Archives, and the creation of a kind of "social life" of the documents[228] focused on connecting the people named in the documents to the times and places that could be verified. The next thirty years would see a splintering of the ufology community into camps defining themselves according to their understanding of these documents and three methodologies have emerged for their potential authentication or debunking. These include the use of forensics by Bob and Ryan Wood, the use of linguistic analysis by Michael Heiser and Carol Chaski and the historical/contextual approach championed by Stanton Friedman. With the exception of Carol Chaski, whose professional training and intellectual community stands outside of ufology for the most part, each of these people is heavily invested both personally and professionally in ufology debates. In addition, those outside of the ufology community have also taken up the challenge of authenticating or debunking this original set of documents, as well as the community of documents that have arisen around them. The Government Accountability Office (the investigative arm of Congress), the National Archives and the United States Air Force have all conducted independent investigations, determining these documents to be falsified or forged.

Within ufology circles, the standard story about how the Eisenhower briefing document and the Truman-Forestall memo came out into the open is by and large the same. It begins with

[228] Caswell, M. (2014). *Archiving the unspeakable: silence, memory, and the photographic record in Cambodia*. University of Wisconsin Pres.

Shandera's mysterious mail drop, and ends with authors and researchers Timothy Good,[229] Stanton Friedman and their colleagues making both the documents and their extensive efforts at authentication public; Friedman appearing most famously on ABC's Nightline to debate Phil Klass, an ardent denier of UFO cover ups and then Director of the Committee for Skeptical Inquiry (CSICOP). In this debate, in which Friedman refers to the documents as a "cosmic Watergate," Phil Klass infamously called out the mainstream media to investigate the documents, stressing that their typical vetting processes and standards for evidence would disqualify serious inquiry. So what, in the intervening three years, had given Friedman the sense that he really had broken through as significant a cover up as Watergate? Friedman and Bill Moore had spent considerable time and effort looking into the initial documents, beginning with the identification of those named as the members of the Majestic Twelve, corroborating their connections and movements, and assessing the likelihood of their participation. A little over a year after Shandera received the initial envelope containing the photographs, Bill Moore himself received an unsolicited, mysterious postcard containing a cryptic message imploring him to visit the National Archives of the United States and more specifically to visit Box 189. Moore and Shandera headed to the National Archives and found, folded between two folders, what would come to be known colloquially as the Cutler-Twining memo, written by Robert Cutler in July of 1964. Cutler, adviser of National Security Affairs for Eisenhower, was addressing Nathan Twining, a named (in the Eisenhower Briefing Document) member of the Majestic Twelve. For Friedman, Moore and Shandera, this was a game changer, not only did they see this document as authentication for their previously held materials, but its evidentiary value was bolstered by the

[229] Good had published the original two documents in his book *Above Top Secret* in 1987. He has since denounced the documents as elements in an elaborate disinformation campaign on behalf of the United States government to cover up its true covert activities.

fact that it alone was an original, not a duplication or photo as the previous documents had been. When asked about the recent interactions with Box 189, the staff at the National Archives told Friedman that it had been handled for the first time in September of 1984. Friedman points to this fact as significant because the last living named member of The Majestic Twelve, Jerome Huntzinger, died just two weeks before Box 189 was handled, suggesting that the release of these documents might have been timed to coincide with his death.

Studying Conspiracy Theory

It is difficult to deny that, in general, the term conspiracy theory carries with it a pejorative connotation. At its most basic, conspiracy theory merely means "a belief that some covert but highly influential organization is responsible for an unexplained event,"[230] and its application can be as broad as verifiable phenomena in United States history such as the Tuskegee experiments, which lasted four decades, to the patently absurd Pizzagate scandal that posited an underground childhood sex ring coordinated by Hilary Clinton operating out of a pizza parlor basement in Washington D.C. The latter's association with the same descriptive term as the former strains credulity, but the qualities that make or unmake a conspiracy theory are simply eventual proof that it is indeed more than a theory. This poses one of the most fundamental issues for those studying conspiracy theories: taking seriously extant theories and their evidential base as the expression of legitimate fears, concerns or anxieties while retaining a critical approach to their possible dangers and misuse.

In his 1945 book *The Open Society and Its Enemies*,[231] Karl Popper used the term "conspiracy theory" to describe and critique the ideologies he understood to be at the heart of

[230] Conspiracy Theory [def. 1] Oxford English Dictionary. Retrieved March 3, 2017. https://en.oxforddictionaries.com/definition/conspiracy_theory

[231] Popper, K. S. (2012). *The open society and its enemies*. Routledge.

historicism. He saw an undeniable link between the rise of totalitarianism and the absorption of conspiracy theories that at their heart were nationalist and racist, and while he stressed that the existence of actual conspiracies is also undeniable, he made the salient point that conspiracies typically fall apart before their promise is fulfilled. “Conspiracies occur, it must be admitted. But the striking fact which, in spite of their occurrence, disproved the conspiracy theory is that few of these conspiracies are ultimately successful. Conspirators rarely consummate their conspiracy.” Popper, for his part, eschews the dominant approach to studying conspiracy theory throughout the Western academy that tends to rely on a certain penchant for the pathological. The foundational 1966 essay, “The Paranoid Style in American Politics,” by American political historian Richard Hofstadter framed conspiracy theory thinking and paranoia in general as an attitude that undermined normative understandings of and attachments to what he framed as American democratic norms. The essay pits a healthy relationship to pluralism in both politics and culture against a singular, rigid and paranoiac belief system represented by conspiratorial thinking. Hofstadter walks a fine line in the essay as he simultaneously defines and diagnoses the paranoid style as non-normative, while also arguing for its historical place as a consistent, recurring and uniquely American style of political discourse that rears its head especially during moments of political and socio-economic flux.[232] Hofstadter outlines the six facets of the paranoid style, which are useful to summarize here not only because of the depth of their influence on the ways in which subsequent scholarship on conspiracy theories is framed, but for identifying how and why an attention (or inattention as it were) to documentation and evidentiary value is largely absent from conspiracy theory scholarship.

[232] Hofstadter, R. (2012). *The paranoid style in American politics*. Vintage. P. 39.

- Universal and historical in scope – The paranoid style centers conspiracy as the central driving force of history rather than something that is contingent or precipitated by specific configurations of people and events.[233]
- Apocalypse – The stakes are always urgent and world ending. “Time is forever just running out.”[234]
- Urgency – Rather than framing the conflicts at hand as issues that can be dealt with incrementally or through political compromise, conspiracies are framed in absolutes.[235]
- Omnipotence – The agents of conspiracy are all seeing, all knowing and all powerful. Since conspiracies are the driving force of history, their agents are bending history toward their will and their benefit.[236]
- Evidence – Reliance on a constant accumulation of facts that make up a coherent whole. Hofstadter is careful to point out here that the paranoid’s attitude towards evidence is totalizing “since it leaves no room for mistakes, failures or ambiguities.”[237]
- Interpretation – The paranoid always must at some point, in order to connect disparate facts or accumulate evidence where it does not immediately and obviously exist make a leap of the imagination in order to bridge the gap between the “undeniable to the unbelievable.”[238]

Hofstatder, in these last two points, touches upon issues that deserve more attention, as they are key to both the sustenance of ongoing conspiracy theories and the strength of their impact outward. The development of a culture of research and explanation, that requires the vantage

[233] Hofstadter, R. (2012). *The paranoid style in American politics*. Vintage. P. 29.
[234] Ibid. 30
[235] Ibid. 31
[236] Ibid. 32
[237] Ibid. 36
[238] Ibid. 37-38

point of someone who can make a leap of imagination, can simply see that the truth is a vital connective tissue bringing together disparate populations. Not only does this culture further solidify the identity of the researcher with the community, due to time and intellectual investment, but also legitimizes the results of the research through community consensus. What Hofstadter refers to as "pseudo-scholarship,"[239] has become an industry representing media outlets, in person conferences, and journals and publications that fully ape scholarly convention through a circular invocation of expertise, peer review and citation practices.

The bulk of scholarship concerning conspiracy theory within the American context takes this Hofstadter essay as its intellectual foundation, but range from the diagnostic to the historical. What I refer to as the diagnostic describes works that tend to classify conspiracy theory as non-normative, extreme and to be rooted out. In these works, Hofstadter's "paranoid style" is an illness that threatens to overtake American mainstream political rationalism. Philosopher Brian Keeley attempts to analyze the enduring popularity of conspiracy theories through their epistemological foundations, and what he identifies as fundamental epistemological flaws.[240] Specifically, he defines an even more specific subset of conspiracy theories that he names "Unwarranted Conspiracy Theories" or UCTs. Unwarranted in this case because of the ways in which conspiracy theorists themselves weigh, consider, evaluate and present evidence for their particular cases. According to Keeley, UCTs are defined by the following characteristics:

- An account that posits an alternative theory of events that opposes accepted views or understandings
- The reasons behind the conspiracy are self-serving to the conspirators and can also be considered to be evil

[239] Hofstadter, R. (2012). *The paranoid style in American politics*. Vintage. P. 39. 36-38
[240] Keeley, B. 1999. Of conspiracy theories. *The Journal of Philosophy* 96:109-26.

- These theories seek to tie together seemingly disparate and/or unrelated events, people and factors
- The real truth, to be uncovered, is made up of high-stakes, closely maintained secrets even though all of the players and events might be known to the public
- Their primary tool is "errant data"[241]

It is this "errant data" that Keeley sees as the central epistemological flaw of UCTs. The use of any data belies a trust in the source of the data itself and the means by which it was communicated. As the positionality of conspiracy theories typically relies on a breakdown of trust in mainstream institutions and authorities, the consideration of different forms of data becomes key. The more traditionally trusted an institution might be, the less trustworthy its data. Keeley points out that conspiracy theories bring the central role of trust in evidentiary evaluation to the surface. In addition, this trust also dictates whether or not one might allow evidence to challenge a perceived truth or value, or whether it is rejected. Keeley's concern is that the mutual development of the evidence/trust matrix implicated in conspiracy theories makes impossible a belief in legitimacy of scientific work or political discourse, and that the depths of that mistrust are boundless. Keeley understands this tendency as having a snowball effect, leading to an extreme skepticism. This skepticism, then, only breaks away in moments in which evidence confirms a deeply held belief or furthers a particular narrative. Exemplified by the all-encompassing maxim of The X-Files's Fox Mulder, "I Want to Believe," the epistemological foundations of conspiracy theories rely on a desire for the right evidence to be true and all clues to the contrary can be dismissed as part of the lie.

[241] Keeley, B. 1999. Of conspiracy theories. *The Journal of Philosophy* 96.p 117.

Rather than a dearth of evidence, conspiracy theories have a counter-intuitive relationship to evidence, in that they often are based on a much larger and more pored over evidential basis than mainstream, accepted beliefs, or what Steve Clarke has referred to as the "received view."[242] In the most extreme sense, all evidence is evidence of a conspiracy theory, as even evidence to the contrary is then evidence of the cover up. In his description of Gail Brewer-Giorgio's 1988 book that outlines the possible proof for Elvis Presley still being alive,[243] Clarke lays out the lengths of the argument to connect what appears on the surface to the actual meaning. For example, the appearance of Presley's poor health conditions prior to his death is exactly what one would expect from someone attempting to fake their own death, all evidence pointing to the plausibility of his death then becomes evidence that he went to great lengths to conceal his actual health. The enactment of conspiracy theory culture revolves around an almost fever like excitement regarding the accumulation and presentation of evidence, and typically an attempted adherence to the aesthetics and style of argumentation of widely accepted rhetorical standards.

An outgrowth of the Hofstadter school of conspiracy theory study, Daniel Pipes's *Conspiracy: How the Paranoid Style Flourishes and Where it Comes From*[244] takes a long historical view of paranoia and conspiracy theory thinking throughout the West. While Pipes analyzes the prevalence of fears geared towards ultra-powerful secret societies, the majority of his cases revolve around the persistence of scapegoating rooted in anti-Semitism. Like Hofstadter, Pipes frames conspiracy theory thinking and the paranoid style as a fundamental threat to democratic principles, going so far as to center "conspiracism" in an unqualified

[242] Clarke, S. 2002. Conspiracy theories and conspiracy theorizing. *Philosophy of the Social Sciences*, Vol. 32, No. 2.

[243] Brewer-Giorgio, G. 1988. Is Elvis alive? New York: Tudor.

[244] Pipes, D. 1997. Conspiracy: How the Paranoid Style Flourishes and Where It Comes From. New York: Free Press.

indictment of the fascist and communist regimes of the twentieth century. In her investigations into totalitarian regimes and the propaganda that aids in both their rise to and maintenance of power, Hannah Arendt also places conspiracy theories at the forefront of her diagnosis.[245] Similarly, Robert Robins and Jerrold Post's *Political Paranoia: The Psychopolitics of Hatred*[246] positions the paranoid style at the heart of twentieth century political turmoil, featuring short historical analyses of political upheaval or specific figures. These works identify conspiracy theories with a strong and charismatic leader, and although Pipes does spend a bit of time arguing for the threat of the web as a vehicle for conspiracy theories, their outline of the features of conspiracy theories are relatively inflexible for different forms of intellectual diffusion or political organization.

In *Hystories: Hysterical Epidemics and Modern Culture,* Elaine Showalter eschews the attention paid to charismatic leaders and manipulation, and attempts to frame conspiracies as groundswell epidemics. She explicitly makes the connection between psychological illness and belief in conspiracy theories, making a case for a one-to-one relationship between the two. Taking at times a pedantic tone, she addresses a series of contemporary "epidemics" including, perhaps most controversially, Gulf War Syndrome (GWS), "contemporary hysterical patients blame external sources – a virus, chemical warfare, satanic conspiracy, alien infiltration – for psychic problems."[247] Showalter oscillates between identifying these epidemics as individual or societal.

[245] Arendt, H. (1973). *The origins of totalitarianism* (Vol. 244). Houghton Mifflin Harcourt.

[246] Robins, R. S., & Post, J. M. (1997). *Political paranoia: The psychopolitics of hatred*. Yale University Press.

[247] Showalter, E. 1998. *Hystories: Hysterical Epidemics and Modern Culture*. London: Picador. 8.

For each of these scholars, the problematics arising from conspiracy theories are not merely rhetorical. In his analysis of the persistence of *The Protocols of the Elders of Zion*,[248] Chip Berlet posits that the strength of conspiracy theory claims can detach the details of their implementation from their often racist and hateful origins. Berlet, a veteran of tracking and documenting right-wing hate groups across the political landscape in the U.S., draws this parallel to the circulation of theories regarding Barack Obama's role in the planning and creating of a North American Union fusing the interests of Mexico, Canada and the United States. An outgrowth of the militia movements of the 1990s, and nurtured by contemporary "patriot" movements, the theory of the North American Union expresses a perfect fusion of the suspicion of the federal government with an erosion of national sovereignty rooted in nationalist and racist beliefs. Berlet in many ways is the canary in the coal mine of the current acceptance of radical conspiracy theories by the mainstream political right, as he documents the warnings of the North American Union from such divergent political figures as Patrick Buchanan, Ron Paul and Phylis Schlafly.[249] Berlet places conspiracy theories at the heart of American political discourse and identifies three persistent groups around which these theories coalesce: the Freemasons and/or the Illuminati; the Plutocrats and/or Bankers; and Jews. He maintains that every conspiracy theory that holds purchase on the American imagination will have one or more of these groups as their foundation. In the case of the North American Union, he tracks the ways in which different groups use particular scapegoats according to their prevailing political orientation. Berlet sees the persistence of conspiracy theories as a result of many overlapping factors, both historical and

[248] Berlet, C. (2005). Protocols to the Left, Protocols to the Right: Conspiracism in American Political Discourse at the Turn of the Second Millennium. In *conference: Reconsidering "The Protocols of the Elders of Zion* (Vol. 100, pp. 30-31).
[249] Berlet, C. (2009). Fears of Federalisme in the United States: The case of the 'North American Union'conspiracy theory. *Fédéralisme Régionalisme*.

contemporary, fusing religious traditions within the United States, political ideologies founded on individualism, economic libertarianism and populism with familiar scapegoats.

Although conspiracy theories all have their own particular historical moments and paranoiac touchstones, each has a set of characteristics that allow for their proliferation. The conspirators must be both easily identifiable and relatively obscure from public view – they must be seen and not seen simultaneously in order for power to be attributed to them. Jovan Byford stresses the power of the broad category in achieving this both identifiable and not identifiable quality. A category such as "international bankers" is both a real group of people and completely useless in terms of differentiation or identification.[250] This delicate balance between the visible and invisible also characterizes the methods by which conspiracies persist and succeed. Conspiracy theories require some form of mass manipulation, otherwise the conspiracy would be obvious to everyone. The conspiracy theorist then is cast as uniquely attuned and able to see through these forms of mass manipulation to uncover the truth. Ranging from control of the media, to purposefully introducing disease into particular populations, to planting microchips inside the bodies of the public, these methods of manipulation hinder otherwise healthy human agency. The truth and individual autonomy are just out of reach, and most importantly, not irretrievable. The conspiracy theories of the twentieth century are often concerned with the ownership and means of circulation of information. The rhetorical purchase of media manipulation has an extensive history, specifically in its historical ties to anti-Semitism, whose echoes are inescapable in contemporary invocations of conspiratorial media production. When Charles Lindbergh said that Jewish "ownership and influence in our motion pictures, our press,

[250] Byford, J. (2011) *Conspiracy Theories: a critical introduction*. Springer, 2011.

our radio and our Government"[251] was the greatest danger to America leading up to World War II, he not only advocated for a skepticism toward mainstream cultural production and news organizations but also identified Jews as an external force seeking to manipulate American hearts and minds. In this instance, a fear of centralized economic power makes an unhappy marriage with racist, nationalist and anti-Semitic ideas. In a different vein, the skepticism around science and medicine that results in disbelief of humanity's role in climate change or the effective use of vaccination, also paints a picture of a vast conspiracy attempting to silence brave dissenters through funding manipulation and false consensus building.

Contemporary opinion polls would lead one to believe that conspiracy theories have moved from something on the fringes of mainstream culture, to a typical way the American population processes national events signified by change or trauma. In a 2007 Zogby International poll, 42% of respondents reported that there was likely a cover-up involved in the investigation of the attacks on the World Trade Center on September 11, 2001.[252] Other polls have asked respondents to specify whether or not they thought the U.S. government was directly responsible, or if they had foreknowledge and chose to do nothing. The genre of 'speculative history'[253] that dominates the History Channel has ushered in a new style of narrative development, eschewing traditional rubrics of expertise and juxtaposing conspiracy-laden counter-narratives with historical scholarship. Ufologists are placed alongside archaeologists to speculate as to the possible hand of alien life in the construction of ancient civilizations, and the decades long saga surrounding the airing of *The Men Who Killed Kennedy* only served to drive ratings up. So too have conspiracy theories crept into the 24-hour television news cycle, as they

[251] Olmsted, K. S. (2009). *Real enemies: Conspiracy theories and American democracy, World War I to 9/11*. Oxford University Press.

[252]

[253] Byford, J. (2011) *Conspiracy Theories: a critical introduction*. Springer, 2011.

are repeated and legitimated by news anchors. Advocates of the "birther" conspiracy theory, postulating that Barack Obama is not a true citizen of the United States and thereby required a large scale cover up to doctor his birth certificate, saw their numbers grow and support strengthen as their questions circulated across news outlets in tandem with factual reporting. In the process, CNN's Lou Dobbs, as well as many Fox News anchors, legitimated not just the birther agenda but also its underlying racist foundations.

In each of these stances towards conspiracy theory development and the persistence of conspiracy theories, a most difficult reconciliation remains. Somewhere between the cognitive dissonance that dominates much of the evidentiary paradigm of conspiracy, and the reality of actual cover-ups and conspiracies, lies a space fertile with potential narrative. The question of what qualifies as a conspiracy theory has been breached by many, framed alternately as an issue of epistemology or simply as a matter of venue.[254] I argue that conspiracy theories and classified information infrastructure are co-constitutive in three significant ways: classified information infrastructure normalizes secrecy and places it at the center of the relationship between citizenry and the state, eroding trust; the temporal scale of classified information infrastructure creates an informational vacuum for determinate time periods, requiring citizens to fill in the blanks concerning government activities and historical development; and classified information infrastructure requires and generates new evidential paradigms as established evidential paradigms break down. As Jack Bratich argues, conspiracy theories are understood by their relationship to what Foucault calls a "regime of truth."[255]

> Each society has its regime of truth, its "general politics" of truth: that is, the types of discourse which it accepts and makes function as true; the mechanisms and instances

[254] Bratich, J. Z. (2008). *Conspiracy panics: Political rationality and popular culture*. suny Press.
[255] Ibid. p. 3

> which enable one to distinguish true and false statements, the means by which each is sanctioned; the techniques and procedures accorded value in the acquisition of truth; the status of those who are charged with saying what counts as true.[256]

This is key to understanding how classified information infrastructure and conspiracy theories co-constitute one another, as they legitimate not only the content, but the mechanisms by which truth and historical narrative are formed. Ginzburg's discussion of paradigm has been discussed previously but it is worth refiguring here. Specifically, the temporal orientation of venatic deduction uses current traces left behind as a guide to creating a relationship between part to whole, as well as present to past. These connections are at the root of the development of juridical standards of evidence within the American justice system. Evidence is considered evidence as such if it maintains a traceable connection to an event, its authenticity and admissibility relying on the preservation of this chain. Government records act as evidence not just of the organizational activity of singular agencies, but as a means for constructing contemporary and historical narratives about the activities of public officials. Classified information is a sanctioned break in the provision of evidence, leaving space for alternative narrative building and the development of new evidential paradigms that stem from new data or no data.

We Want to Believe

Explanations for the witnessing of unexplained phenomena are the stuff of mythology throughout human life. Unidentified flying objects are no different, that is until the relative increase in sightings coincided with shifts in military technology and political paranoia most exemplified by the hysteric response to the 1938 airing of the science fiction radio drama

[256] Foucault, M., Rabinow, P., & Martell, L. (2001). *Truth and power*. P. 131

adaptation of H.G. Wells *The War of the Worlds*. The “foo fighters” routinely seen throughout World War II by Allied pilots lay the foundation for contemporary ufology in the United States; confirmed by Kenneth Arnold’s sighting at Mt. Rainier, Washington in 1947. The “foo fighters” were understood by most to be experimental aircraft, but laid the groundwork for a powerful mixture of fear and mistrust. Furthermore, they helped shape the Arnold sighting which became the bedrock upon which the aesthetics of so-called alien craft and the narratives constructed around them would be built. Kenneth Arnold was himself a pilot, who on June 24, 1947, was searching for the wreckage of a Marine Corp C-46 transport airplane that had crashed. While in the air, he witnessed what he described as nine flashes of light in quick succession that with distance became clearer. Arnold described the objects in detail, even supplying a rough sketch as evidence to the Army Air Force.[257] The coining of the term “flying saucer” was an embellishment by the press, as Arnold had stated that the objects flew as if they were saucers skipping on water. Alternately, Arnold described their configuration as “flying on a single, horizontal plane, but they also weaved from side to side, occasionally flipping and banking – darting around….the tail of a Chinese kite.”[258] The visual gave a somewhat experienced pilot the impression that the crafts were not piloted and although he initially thought he was witnessing the testing of experimental aircraft, he would also state that the sighting gave him an “eerie feeling.”[259] The concept of flying saucers, birthed by what Arnold understood as a misquote and misunderstanding of his original description, diffused throughout American popular media and seeing flying saucers became somewhat of a household phenomenon. In a 1967 report on the

[257] Bartholomew, R. E. (1991). The quest for transcendence: An ethnography of UFOs in America. *Anthropology of Consciousness*, *2*(1---‐ 2), 1-12.

[258] Garber, M. (2014). The Man Who Introduced the World to Flying Saucers. The Atlantic. Retrieved October 12, 2016. https://www.theatlantic.com/technology/archive/2014/06/the-man-who-introduced-the-world-to-flying-saucers/372732/

[259] Ibid.

dramatic increase in sightings of unexplained aerial phenomena, Ted Bloecher, one of the first in the burgeoning field of ufology, documented 853 sightings[260] of flying saucers in 1947 in the United States and Canada alone following Arnold's description. It is difficult to overestimate the extent to which the imagery of Arnold's original sighting permeated popular culture. Comics, television shows and movies circulated the images of flying saucers, and the narratives around them were routinely paired with stories of invasion, takeover and the destruction of humankind by alien life.

Arnold's sighting, and with it the solidification of the flying saucer as a common cultural touchstone for a post-WWII generation, did not operate within a vacuum. 1947 remains an auspicious year in the annals of ufology, as a few weeks later saw the event that would become known as the "Roswell incident." The existence of alien life is in and of itself not a conspiracy. The conspiracy is the cover up of that existence by the United States government, but the histories of the potential existence and cover up are twin histories, their genesis mere weeks apart and their presence in the American cultural landscape inextricable. From an evidentiary standpoint, the sightings had provided people with eyewitness testimony, whereas Roswell offered a tantalizing promise of forensic evidence. After a preliminary press release, written by Lieutenant Walter Haut, initial interest in the Roswell crash died down as the military offered up the explanation of a downed weather balloon. The press conference was a parade of physical evidence, including the crumpled foil of the balloon itself; an offering to a scared and skeptical public that all of the elements were not only there, but were easily identifiable, familiar and fit into expected activities.

[260] Bloecher, T. (1967) Report on the UFO Wave of 1947. Self-Published. Retrieved January 7, 2017. http://web.archive.org/web/20080413203646/http://www.mimufon.org/historical_folders/nicap_pages/ReportOnWaveOf1947.pdf

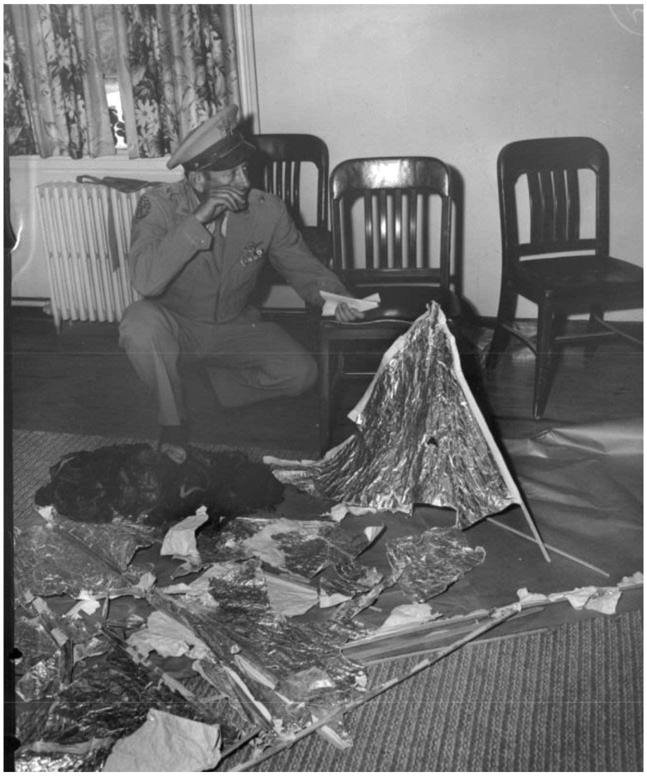


Figure 5: A.J. Bond Johnson photo of Gen. Ramey with the alleged Roswell debris. Credit - Fort Worth Star- Telegram Photograph Collection, Special Collections Division, The University of Texas at Arlington Libraries

In their book, *UFO Crash at Roswell: The Genesis of a Modern Myth*, Saler, Ziegler and Moore argued that the persistence of stories about Roswell resemble the methods of circulation of traditional folk tales, relying on trusted storytellers within a circumscribed community, shifting slightly with the generations but remaining faithful to its core elements. Economies and communities have materialized around the resurgence of interest in Roswell since the 1970s, including conventions, books, talk show appearances and various media spectacles. Each of these takes as its center a particular narrative and evidential framework from the initial crash and builds the case for a sustained government cover up of the truth. The release of classified information related to Roswell is a perennial topic for government officials. Famously, then candidate for the Democratic Party nomination for President of the United States Bill Richardson alluded to his own thwarted attempts as a Congressman to secure the release of Roswell documents by the Department of Defense and the Los Alamos Lab. He stated, “The government doesn’t tell the truth as much as it should on a lot of issues.”[261] Most recently, Presidential candidate Hillary Clinton publicly stated her intention to release Roswell documents when appearing in an interview with late-night talk show host Jimmy Kimmel, leading some in the ufology community to dub her the first “E.T. candidate.”[262] For many, the release of these documents would presumably serve to authenticate the knowledge already contained in the MJ-12 documents. While MJ-12 represents a much larger set of events than the singular Roswell, in many ways it is undeniably linked, as the original two MJ-12 documents refer to a crash and retrieval team, not just researchers or investigators but a team designed specifically to deal with Roswell-like incidents.

Although popular interest in the existence of extraterrestrials has remained at a steady pitch, the issue has remained marginal with respect to research communities. Scientific and establishment agendas have rarely seriously added extraterrestrial life to their agenda, creating a kind of “social stigmatization” associated with the interests.[263] The assumption of illegitimacy has positioned research into the phenomena as marginal, and over the last several decades, a parallel research community has emerged. Research institutions, conferences and other forms of information sharing, peer review and circulation have solidified, taking their cues from

[261] Slater, W. (October 27, 2007). "On Texas stop, Democratic Candidate Richardson Criticizes Government Secrecy". *The Dallas Morning News*.

[262] Chozick, A. (2016). Hillary Clinton Gives U.F.O. Buffs Hope She Will Open the X-Files. The New York Times. Retrieved January 7, 2017. https://www.nytimes.com/2016/05/11/us/politics/hillary-clinton-aliens.html?_r=0

[263] Schetsche, M., & Engelbrecht, M. (2008). Prekäre Wirklichkeiten am Himmel–eine wissenssoziologische Schlussbemerkung. *Von Menschen und Außerirdischen. Transterrestrische Begegnungen im Spiegel der Kulturwissenschaft*, 267-277.

established and reputable academic institutions. Within the United States, these parallel institutions often frame their activities as counter-balancing or directly antagonistic towards government secrecy. These boundaries between academic research and ufology were not entirely solid, a handful of researchers have expressed at least interest in the possibility,[264] but since the Condon Report was published in 1968, asserting that the work of a commission on UFOs out of the University of Colorado had yielded nothing of value or interest in two decades, serious academic research has been scant[265]; barring those scientists associated with the ongoing work at the Search for Extraterrestrial Intelligence (SETI).[266] These communities have also had to develop their own means of collecting, sharing and preserving information about sightings on a grand scale. The International UFO Museum and Research Center in Roswell, New Mexico implemented a unique cataloging system organizing their resources according to incident level, since many of their resources are made up of personal testimonies. The Mutual UFO Network (MUFON)[267] maintains a crowdsourced database of UFO sightings that anyone can contribute to and access through a simple form. Many people also keep personal collections; amateur ufologists such as Luis Schonherr developed a personal cataloging system in order to keep track of almost 3000 cases of UFO sightings he maintained on individual index cards.[268] In a broad sense, these research practices are seen as counter to scientific standards as they often rely on

[264] Sagan, C. (1994). The search for extraterrestrial life. *Scientific American*, *271*, 70-77.

[265] Gillmor, D. S., & Condon, E. U. (1970). *Scientific Study of Unidentified Flying Objects. Vision*. Interestingly, this report simultaneously reported the failure of this research to contribute to knowledges in the natural sciences but suggested that a study of the belief systems surrounding UFOs should be of great interest and could yield great knowledge for those in the social sciences.

[266] The SETI Institute is a non-profit research organization founded in 1984 and although their acronym suggests an exclusive focus on extraterrestrial intelligence, their mission frames their work a bit more broadly, "to explore, understand, and explain the origin and nature of life in the universe…" and tends to divide its work into research that would be considered more mainstream from research into the extraterrestrial both organizationally and financially.

[267] MUFON was founded in 1969 and is the largest and oldest civilian run research organization focused on UFOs. They train their own investigators and do not have any ties to formal scientific research communities in contrast to the SETI Institute.

[268] Eghigian, G. (2015). Making UFOs make sense: Ufology, science, and the history of their mutual mistrust. *Public Understanding of Science*.

eyewitness testimonies, and can be characterized as a system of belief in search of scientific support rather than the other way around. Much like the larger pattern of academic research into conspiracy theories, researchers focusing on communities of UFO believers have consistently pathologized their subjects.[269] This long-standing antagonism and positioning of oppositional knowledge institutions and research practices characterizes the way in which ufology communities consider evidence from the United States government. Reactions to reports from government entities range from skepticism to anger, as many see the government not just as a disinterested party but as active participants in campaigns of disinformation and sustained cover-up. Therefore, a leaked government document might be considered more likely to be authentic evidence than one released intentionally by the government itself. The discourse that has coalesced around the MJ-12 betrays the vitality of situating the document as evidence within pre-existing systems of belief and evaluation.

A Note on Authenticity

Within archival studies and practice, authenticity as both a state and a concept takes on slightly different or more complex meaning than the colloquial understanding of authenticity. Authenticity relies on the relationship between the record and the creator(s) of the record; an authentic record is a record that is created by the entities represented as the creator. However,

[269] Studies such as Leon Festinger et al's 1956 ethnography of a group of believers in a UFO religion characterized their subjects as exhibiting non-normative patterns of behavior brought on by irrational and extreme belief systems. For further reading see:
Denzler B (2001) *The Lure of the Edge: Scientific Passions, Religious Beliefs, and the Pursuit of UFOs.* Berkeley, California: University of California Press.
Little GL (1984) Educational level and primary beliefs about unidentified flying objects held by recognized ufologists. *Psychological Reports* 54: 907-910.
Melton JG (1995) The contactees: A survey. In. Lewis JR (ed.) *The Gods Have Landed: New Religions from Other Worlds.* Albany, NY: State University of New York Press, pp. 1-13.
Palmer SJ (2004) *Aliens Adored: Rael's UFO Religion.* New Brunswick, NJ; London: Rutgers University Press. Partridge C (2003) (ed.) *UFO Religions.* London and New York, NY: Routledge.
Zimmer TA (1984) Social psychological correlates of possible UFO sightings. *Journal of Social Psychology 123: 199-206.*

authenticity does not necessarily have anything to do with the truth or reliability of the record. For example, a document containing the signature of Harry S. Truman is considered authentic if the signature is verified, even if that document purposefully misrepresents reality, it is proof that the document came from where it claims to be from, not that its contents are true. To this end, methods of determining authenticity rely on contextual clues and processes of determining similarity dissimilarity to other records,

> Validating authenticity entails verifying claims that are associated with an object – in effect, verifying that an object is indeed what it claims to be, or what it is claimed to be (by external metadata). It is important to note that tests of authenticity deal only with specific claims (for example,' did X author this document?' and not with open-ended inquiry ('Who wrote it?'). Validating the authenticity of an object is more limited than is an open-ended inquiry into its nature and provenance.[270]

Hoax or Proof? Authenticating the MJ-12 Documents

An entire cottage industry has arisen around determining the authenticity of the MJ-12 documents. Their status has created camps within the ufology community, drained financial resources from several entities and resulted in one external investigation on the part of the United States Air Force. Over the past few decades, the number of MJ-12 documents has exploded, growing from the original three received by Shandera to hundreds, each representing degrees of connection to the original documents, however tenuous. Although the number of MJ-12 documents have proliferated greatly, for the purposes of this analysis, I will remain constrained to the original documents: the Eisenhower briefing document, the Truman-Forrestal memo. Three methodologies have emerged for their potential authentication or debunking, including: the use of forensics by Bob and Ryan Wood; the use of linguistic analysis by Michael Heiser and Carol Chaski; and the historical/contextual approach championed by Stanton Friedman. The

[270] Lynch, C. (2000). Authenticity and integrity in the digital environment: an exploratory analysis of the central role of trust.

Eisenhower briefing document lists the committee of twelve scientists, military officers and government officials tasked with both crash retrieval and the cover up of extraterrestrials after describing the recovery of a wreckage in 1947. It also includes the development of an alternate story to combat the public's knowledge of extraterrestrial life. The Truman-Forrestal memo is a memorandum signed by President Harry Truman directing then Secretary of Defense James Forrestal to move forward with the Majestic Twelve with "all due speed and caution."[271]

Bob and Ryan Wood have devoted a significant portion of their careers and reputations to authenticating and providing information about the MJ-12 documents. They maintain a website providing researchers with copies of the documents along with an authentication rating and analysis of their historical context. The Woods' understanding of authenticity is complex, pulling from an amalgamation of standards and practices, but always foregrounding forensic techniques. Their central concern remains placing these documents within reputable and replicable circles in order to facilitate wider, mainstream acceptance of their theories. In an "Introduction to Authenticity Ratings," they outline six separate questions for assessing the authenticity of documents including:

1. Where did the document come from?
2. What are the results of the forensic paper, ink, watermark, typewriter and handwriting tests?
3. Are there unique and obscure content markers that are accurate for this type of document?
4. Are there direct first hand witnesses?
5. How difficult is the document to hoax or fake?

[271] Truman-Forrestal Memo (1947). Source unknown.

6. Who would have faked the document and why?

In addition to these questions, the Woods also stress that each question and its attendant answer are not equal, there are relative weights given to particular aspects of the documents, “For example, there is a strong difference between forensic paper and ink testing, a weighting of 5.0, and more easily obtained document content, a weighting factor of 2.0. Courts widely recognize this concept, discounting eyewitness testimony in favor of DNA evidence.”[272] The Woods are consistently aligning their methods of authentication and their standards of evidence with juridical systems, claiming authority through similar adherence to basic concepts and some similar techniques of analysis. Ufology is especially concerned with asserting legitimacy, as their claims for so long relied on eyewitness testimony and the first-hand experiences of survivors and abductees demonstrate. The website makes repeated claims that their tools are adequate not only for confirming their own beliefs, but for converting the skeptic through the application of objective tools and analysis. Their final analyses considers eight weighted factors, including: eyewitnesses or first-hand witnesses that have seen, written, read or destroyed the document in question are given a weighting factor of 3.0; zingers are verifiable rare subtleties of particular documents, their example is “typographical anomalies associated with the printed process of the era,” and these are given a weighting factor of 5.0; content secures a weighting factor of 2.0 and refers to the words and meanings contained within the document; chronology considers the document within the context of organizational history and garners a weighting factor of 2.0; typography regards the techniques of production and reproduction and is given a weighting factor of 4.0; forensics considers testing inks, paper and watermarks against known and shared standard, this has a weighting factor of 5.0; linguistics utilizes expert analysis of syntax and style

[272] Wood, R. Introduction to Authenticity Ratings. Retrieved January 7, 2017. http://majesticdocuments.com/authentication_intro.php

and is given a weighting factor of 3.0; anachronisms considers formatting, dates or other detail that would be inappropriate for the time period in which the original document was produced, this is given a weighting factor of 5.0.

While the Woods have scrutinized the mountain of MJ-12 documents that have surfaced since 1984, in each of their analyses they include a curious redundant preamble. The logic follows that we know there have been UFO crashes due to the physical traces and remains of the crafts, in addition to eyewitness testimony. Therefore, we would assume that the United States government would have developed a plan to deal with the consequences and fall out from such knowledge. Presumably then, if such a government plan were formulated, we would then infer, bureaucracy being what it is, that there would be quite a substantive paper trail. In turn, we know that some documents *must* exist and, given the nature of classified documentation, we will only have incomplete information and means of authentication so we must start at a different point. "To take the position that without proof of genuineness they are fake is illogical because of the certainty that such documents exist if crashes have occurred. Similarly, to take the position that, without proof of fakery, they are genuine is also illogical because it is certainly true that some fake documents might exist. This logic says that, before a questioned document determination, *it is equally likely that they are genuine as that they are fake*."[273] (Author's emphasis.) It should be noted that the Woods favor considering the documents as a whole, and although they do provide individual document authenticity ratings, their emphasis remains on this as a class of documents. Skeptics both inside and outside of the ufology community have pointed to this as the Woods' and the MJ-12 documents' Achilles heel, as the house of cards relies on authentication across documents. In a two-part essay for the MUFON UFO Journal in 1999, former MUFON Board

[273] Wood, R. Mounting Evidence for Authenticity of MJ-12 Documents. Presented at the International MUFON Symposium July 2001, Irvine, CA. p.3.

Member Tom Deuley presented this as the crux of his skepticism. The bulk of the MJ-12 documents were given to the Woods by another source, Tim Cooper. Since the provenance of the MJ-12 documents is one of their most obvious issues, the Woods published a document on their website entitled “Ten Reasons Why Tim Cooper is NOT a Provenance Problem.”[274] Cooper acted as an independent researcher and claims that the majority of his documents were received through FOIA requests with a few in-person sources, including a CIA archivist. The Woods rebuttal document includes allusions to evidence of postmarks, the assessment of a forensic typewriter specialist named Dr. James Black and Cooper’s own lack of interest in attention and fame. Most curious is reason number 10, however, which deviates drastically from the former insistence on context, authentication and external verification.

> 10. Although of speculative value, high quality remote viewing (psychic) assets have targeted Tim Cooper and the documents and concluded the documents are predominately real and Cooper is not a forger. In fact, there seems to be multiple origins of documents feeding to Cooper.[275]

While police departments have been known to include psychics as investigatory resources[276] and on occasion some psychics have been allowed to testify in court,[277] psychic confirmation cannot be widely considered a standard forensic technique of authentication. While in some ways, this blending of epistemological frameworks and commitments is characteristic of ufology circles, it

[274] Wood, R. Ten Reasons Why Tim Cooper is NOT a Provenance Problem. Self-Published. Retrieved January 7, 2017.

[275] Ibid.

[276] Martinez, L. (2004). Looking into the crystal ball: can using a psychic help or hinder a case. *Law Enforcement Technol*, *31*(7), 52-54.
Butler, P.(2003) "DNA test proves body was Braun's" Centralian Advocate, p. 3.
Jones, G. (2006)“Forensic Psychics Get It Right Sometimes" The Daily Telegraph (Australia). P.23.

[277] Dearen, J. Judge Allows Polk to Question Psychic. East Bay Times. Retrieved January 7, 2017. http://www.eastbaytimes.com/2006/06/07/judge-allows-polk-to-question-psychic/

is distinct here as the Woods pride themselves on their commitment to generalizable, agreed upon techniques of authentication. Vitally, Cooper's addition to the group of MJ-12 documents provided the Woods with a second version of the Eisenhower Briefing Document and the Truman-Forrestal memo, versions that were not photos, allowing them to analyze the paper and typographical techniques, which they determined to be authentic. Currently, they assess these documents with the highest possible rating on their authenticity scale. Their quest to provide evidence in support of the documents' authenticity also includes direct responses to issues raised by critics.

Although the Woods have taken on the mantle of providing a comprehensive guide to the MJ-12 documents, Stanton Friedman is most closely associated with long standing efforts to authenticate the documents. Friedman is a retired nuclear physicist who has found a robust second career in ufology. He has written five books and dozens of articles, including a book devoted to the MJ-12 documents and what they reveal. He contends that "…the documents, when carefully and objectively examined, lead to the conclusion that there was indeed an Operation Majestic-12."[278] There are many people, skeptics and believers alike, who have taken issue with the investment in the MJ-12 documents. Throughout their research efforts, Moore, Shandera and Friedman have conceded the possibility that the documents are fraudulent,[279] but insisting that whether or not they are fraudulent, they would have had to have been produced from within the government.[280] None have been more vocal than Philip Klass, who has insinuated himself into the authentication debate at every turn. He and Friedman have a

[278] Friedman, S. T. (2005). *Top Secret/Majic: Operation Majestic-12 and the United States Government's UFO Cover-Up*. Perseus Books Group. P 210.

[279] Moore, W. L., & Shandera, J. H. (1990). *The MJ-12 Documents: An Analytical Report*. Fair Witness Project.

[280] Friedman, S. T. (2005). *Top Secret/Majic: Operation Majestic-12 and the United States Government's UFO Cover-Up*. Perseus Books Group. P 210. P. 138

particular tone of dismissiveness for each other, both in their publications and in the handful of interviews they have done together. In his book on the documents, Friedman says of Klass, "…in denigrating UFOs in general and the MJ-12 briefing document in particular, [Philip] Klass is basically whistling in the dark. The small amount of time he has spent in archives shows that he is essentially an armchair theorist, as are most debunkers…his minimal research, flawed logic, and propagandistic writing call into question of his claims…"[281] Friedman consistently references his time spent in multiple government archives and his deep knowledge of archival research. His methods for authentication predominantly rely on this strength, he builds a case for authenticity through confirming details and context within and outside of the documents. For the Eisenhower Briefing Document, Friedman has claimed that there is no "mistaken information" in the document, solidifying its claims to authenticity.[282]

The centrality of mechanisms for knowledge sharing and information evaluation within the ufology community makes publications in circulation venues for disagreement and consensus building. Citizens Against UFO Secrecy was an activist organization founded in 1977 focused specifically on putting pressure on the United States government to make information about UFOS publicly available. The organization filed FOIA requests and published a newsletter entitled *Just Cause* three times a year. *Just Cause* featured analysis of the MJ-12 documents and the cultures growing around them between 1985-1990.

In early 1989, *Just Cause* published information regarding a developing project between former National Enquirer reporter Bob Pratt, William Moore and Richard Doty, the goal of which was to release MJ-12 related information within fictional contexts. This triad represented

[281] Friedman, S. T. (2005). *Top Secret/Majic: Operation Majestic-12 and the United States Government's UFO Cover-Up*. Perseus Books Group. P 125-126.
[282] Friedman, S.T. (1987) CSICOP/Majestic P. 5

the complexity of relationships, motivations and vantage points circulating within these communities. While Moore was investigating Doty as a possible source of intentional government disinformation concerning UFOs, Pratt was investigating both of his partners on the project under a similar light. The proceedings from the 2007 International MUFON Symposium, a venue for consistent and lively debate concerning the MJ-12 documents, among many other things, reveal the devolution of Moore's reputation within the ufology community as revelations of his participation in disinformation campaigns were alleged. In the proceedings, Brad Sparks and Barry Greenwood trace the movement of information back and forth between Moore and Doty. They use Friedman and Moore's own claims about their identification of key names and dates prior to any release of MJ-12 documents as evidence of their aid, either implicitly or explicitly, in document forgery.[283] Sparks and Greenwood also repeat the call for Shandera, Moore and Friedman to release the postcards and other communication with anonymous sources as contextual information, bolstering the evidence of document authenticity. Sparks and Greenwood see all of Friedman's work of lining up figures and dates as collapsing under the weight of its own circularity. As Friedman has stated, "somebody had to do a lot of homework that no one else has done," identifying himself and Moore as the primary researchers on Roswell and the crash recovery/cover-up.[284] From the point of view of Sparks and Greenwood, the preeminent researchers on a phenomenon meticulously compiled details which they then shared with government insiders who, in turn, produced documents confirming the information they were given; Moore and Friedman may have inadvertently created the very disinformation they consumed.

[283]

[284] Interview with Stanton Friedman. Daily Gleaner 8/28, 1987 p. 16

Friedman's authentication work represents the most complete of the historical/contextual framework, as his extensive archival work and first-hand interviews attempt to verify details within the records with supporting documentation or witness testimony. Friedman was extensively supported by the larger ufology community, receiving a $16,000.00 grant[285] from the Fund for UFO Research to conduct his studies. One of his biggest revelations was the extent to which Donald Menzel, an alleged member of the MJ-12, was himself involved in secret government work. Friedman's research asserted that Menzel had done work for the CIA, NSA and more than thirty corporations, and was fluent in several languages and cryptography. Menzel's status had been as a public skeptic, so Friedman's allegations cast Menzel as leading somewhat of a double life.

Friedman's final report and subsequent book were awaited with great anticipation, and commented upon extensively in several newsletters and community publications. *Just Cause* repeatedly covered Friedman's investigations and other MJ-12 related updates, their general tone increasing with credulity as events unfolded in late 1987, calling the saga a "fiasco" and systematically taking apart the main arguments made by proponents of the documents' authenticity.[286] Three years later they were steeped in their critique, asserting that it is an important story "for the devastating effect it has had on legitimate government document research on UFOs," and stating, "[t]here is no question that because of the MJ-12 story, the credibility of that with which CAUS deals has been seriously damaged."[287] While *Just Cause* remained skeptical throughout their coverage of the MJ-12 story, the tone of later publications contrasts greatly with the hopeful, investigatory spirit of initial coverage.[288] Once the tide turned,

[285] Stacy, D. "MUFON Las Vegas Symposium" MUFON UFO Journal August 1989
[286] Just Cause Ed. Barry Greenwood September 1987 Number 13
[287] Ibid 1990 Number 25
[288] Ibic 1985 Number 6

the intimate nature of the ufology community itself became a source of evidence against the authenticity of the documents. In a 1990 issue of *Just Cause*, Robert G. Todd uses details of his own correspondence with Moore to outline similarities between the Eisenhower Briefing Document and his personal letters. Todd shows Moore's return address, which he alleges is made with a stamp kit, and compares this with the headers included in the Eisenhower Briefing Document, drawing similar typographic details including the raised letter "I."[289]

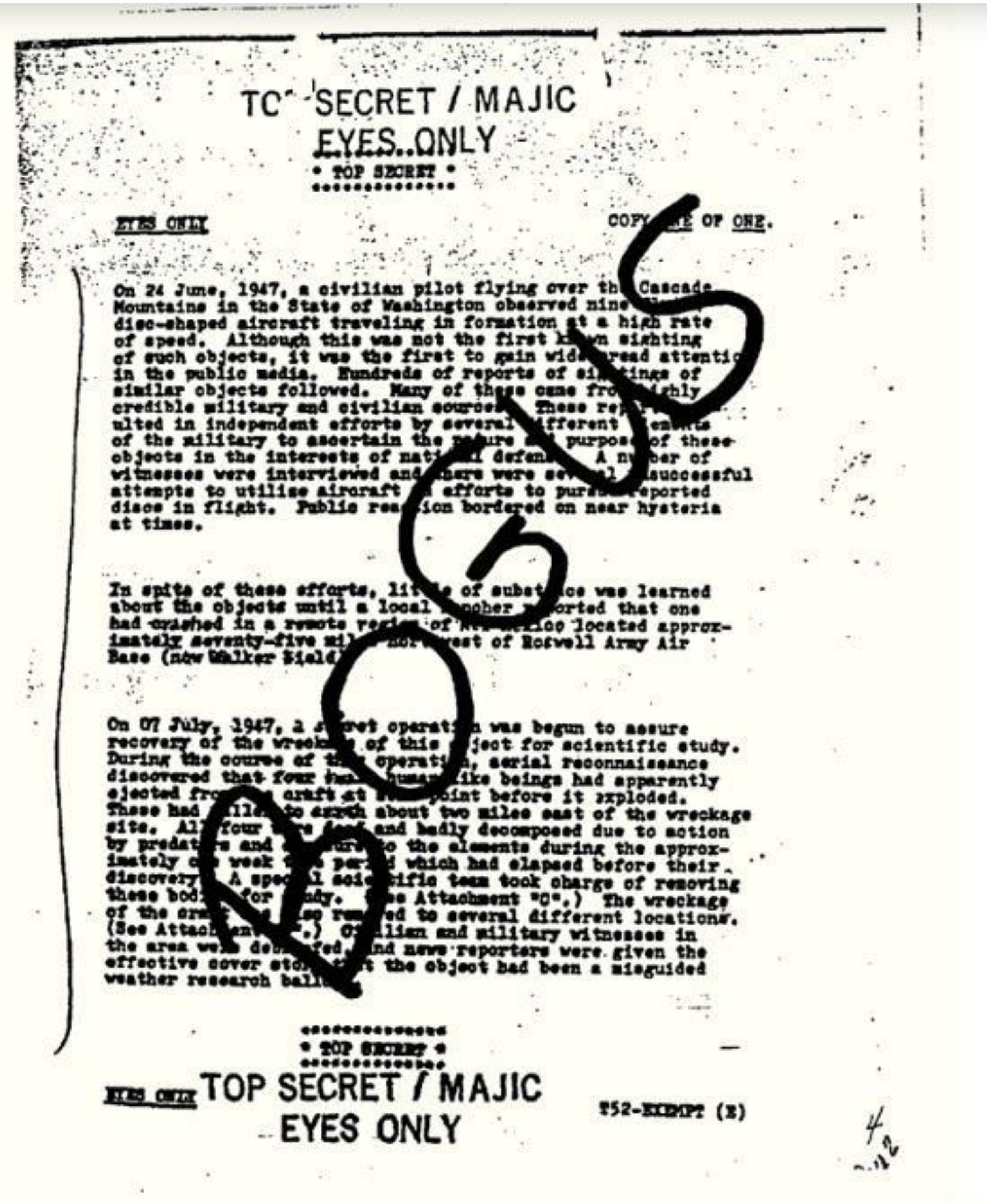
Another method peppered throughout both Woods and Friedman's work is linguistic analysis. However, Michael Heiser and Carol Chaski were the two researchers with the skills and background who focused primarily on linguistic authentication. Although their methodologies excluded many of the documents as they only examined those with clear author attribution and were of substantive length. In his report on their analysis, Heiser explains Chaski's methods, including biometric analysis, qualitative analysis of idiosyncracies and quantitative computational stylometric analysis of the language in the documents. The only possible method to employ with respect to the MJ-12 documents is the third, "focusing on readily computable and countable language features, e.g. word length, phrase length, sentence length, vocabulary frequency, distribution of words of different lengths…function word frequency and punctuation.[290] For their analysis, Heiser and Chaski ran computational stylistic comparisons between verifiable authored documents and known MJ-12 documents, looking for statistically significant overlap. Of the documents tested, only the Cutler-Twining memo was determined to be likely authentic. Many in the ufology community dismiss this analysis as part of a political

[289] Ibid 1990 Number 23

[290] Heiser, M. (2007) The Majestic Documents: A Forensic Linguistic Report. p 9

agenda on the part of Heiser whose work has included research countering theories about alien civilizations.

The FBI has investigated MJ-12 documents sent to its offices in 1988 and although the details of their report were not published, MJ-12 documents were published on the FBI website; the only difference between these documents and the ones published by Wood and his cohort is that the FBI's version has BOGUS jubilantly written across the pages.[291]



TOP SECRET / MAJIC
EYES ONLY

• TOP SECRET •

EYES ONLY

COPY ONE OF ONE.

On 24 June, 1947, a civilian pilot flying over the Cascade Mountains in the State of Washington observed nine [illegible] disc-shaped aircraft traveling in formation at a high rate of speed. Although this was not the first known sighting of such objects, it was the first to gain widespread attention in the public media. Hundreds of reports of sightings of similar objects followed. Many of these came from highly credible military and civilian sources. These reports resulted in independent efforts by several different elements of the military to ascertain the nature and purpose of these objects in the interests of national defense. A number of witnesses were interviewed and there were several unsuccessful attempts to utilize aircraft in efforts to pursue reported discs in flight. Public reaction bordered on near hysteria at times.

In spite of these efforts, little of substance was learned about the objects until a local rancher reported that one had crashed in a remote region of New Mexico located approximately seventy-five miles northwest of Roswell Army Air Base (now Walker Field).

On 07 July, 1947, a secret operation was begun to assure recovery of the wreckage of this object for scientific study. During the course of this operation, aerial reconnaissance discovered that four [illegible] human-like beings had apparently ejected from the craft at some point before it exploded. These had fallen to earth about two miles east of the wreckage site. All four were dead and badly decomposed due to action by predators and exposure to the elements during the approximately one week time period which had elapsed before their discovery. A special scientific team took charge of removing these bodies for study. (See Attachment "C".) The wreckage of the craft was also removed to several different locations. (See Attachment [illegible].) Civilian and military witnesses in the area were debriefed, and news reporters were given the effective cover story that the object had been a misguided weather research balloon.

BOGUS

• TOP SECRET •

EYES ONLY TOP SECRET / MAJIC
EYES ONLY

T52-EXEMPT (E)

4

Figure 6: Page 5 of the Majestic 12 documents in "The Vault" Credit: The FBI

NARA maintains a short disclaimer on their website alongside their documents and reports concerning the Air Force and Project BLUE BOOK. The statement refers to “numerous inquiries concerning documents identified as ‘MJ12,’” describes several searches for these documents and details references made to them at NARA, including within the records of the U.S Air Force, Joint Chiefs of Staff, Truman and Eisenhower Libraries, and the National Security Council. Their searches yielded but one result for a “Memorandum for General Twining, from Robert Cutler, Special Assistant to the President, Subject: ‘NCS/MJ-12 Special Studies Project” dated July 14, 1954, and the memo does not define or identify MJ-12.[292]

Diplomatics

Diplomatics, which was reconceptualized as contemporary archival displomatics in the 1990s by archival scholar Luciana Duranti. Duranti’s invocation of diplomatics techniques responded to the need for working with electronic records. Medieval documents needed to be considered and authenticated individually, and the methodologies used arose out of this particular need. Duranti posited that these methodologies were relevant in the face of changing formats and technological contexts, and could assist in providing a framework for determining the authenticity of digital records. This is not to say that each document must contain all of these elements, or that somehow something does not qualify as a document if it does not contain one element. The central driving force behind diplomatic analysis remains enabling the determination of authenticity through the identification of relationships between form and function. Form, or what diplomatics considers the set of conventions and rules that govern representation, can be broken out from the specific persons, institutions or operations about which a document might be. According to diplomatics, form is comprised of extrinsic and intrinsic elements. The extrinsic

[292] National Archives and Records Administration. Project Blue Book – Unidentified Flying Objects. Retrieved October 4, 2016. https://www.archives.gov/research/military/air-force/ufos.html

elements are the material of the document, its medium, seals, annotations, original markings, the "technique used to prepare it for receiving the message."[293] Language is key here, beyond meaning conventions, order and formatting are what distinguish particular disciplinary or administrative norms. This has some relationship to the concept of genre, which dictates what is determined by the relationship between the function of the document and its formal qualities. In other words, you might communicate the same basic information in an inter-office memo and a year-end report, but their formal qualities would signal the audience and intent in particular ways. Since diplomatics arose as a set of methodologies to determine and analyze the authenticity of medieval documents, the seal was a vital extrinsic documentary element. While this might not be immediately relevant, its contemporary corollaries such as the stamp, folder or markings remain central in determining the "authority and solemnity of a document, its provenance and function, and its authenticity."[294] In addition, the annotations contained within the document are considered extrinsic. Annotations can include those added by an archives or records manager in order to identify the document as part of a group of document, or to enable its findability and subsequent retrieval; those considered as part of the transaction that claims the document as part of its process, or after the completion of an event documented. The forms of annotations are varied but include signatures, notes, inter-agency or office instructions, marks and signs and other evidence of movement throughout contexts during both the handling of the document and through its subsequent management. A document's intrinsic elements are comprised of its protocol, text and eschatol, and are all derived from a sense of an ideal text; which is also a concept in bibliographic and textual studies.[295] The protocol, or the signaling of

[293] Duranti, L. (1998). *Diplomatics: new uses for an old science*. Scarecrow Press.

[294] Ibid.

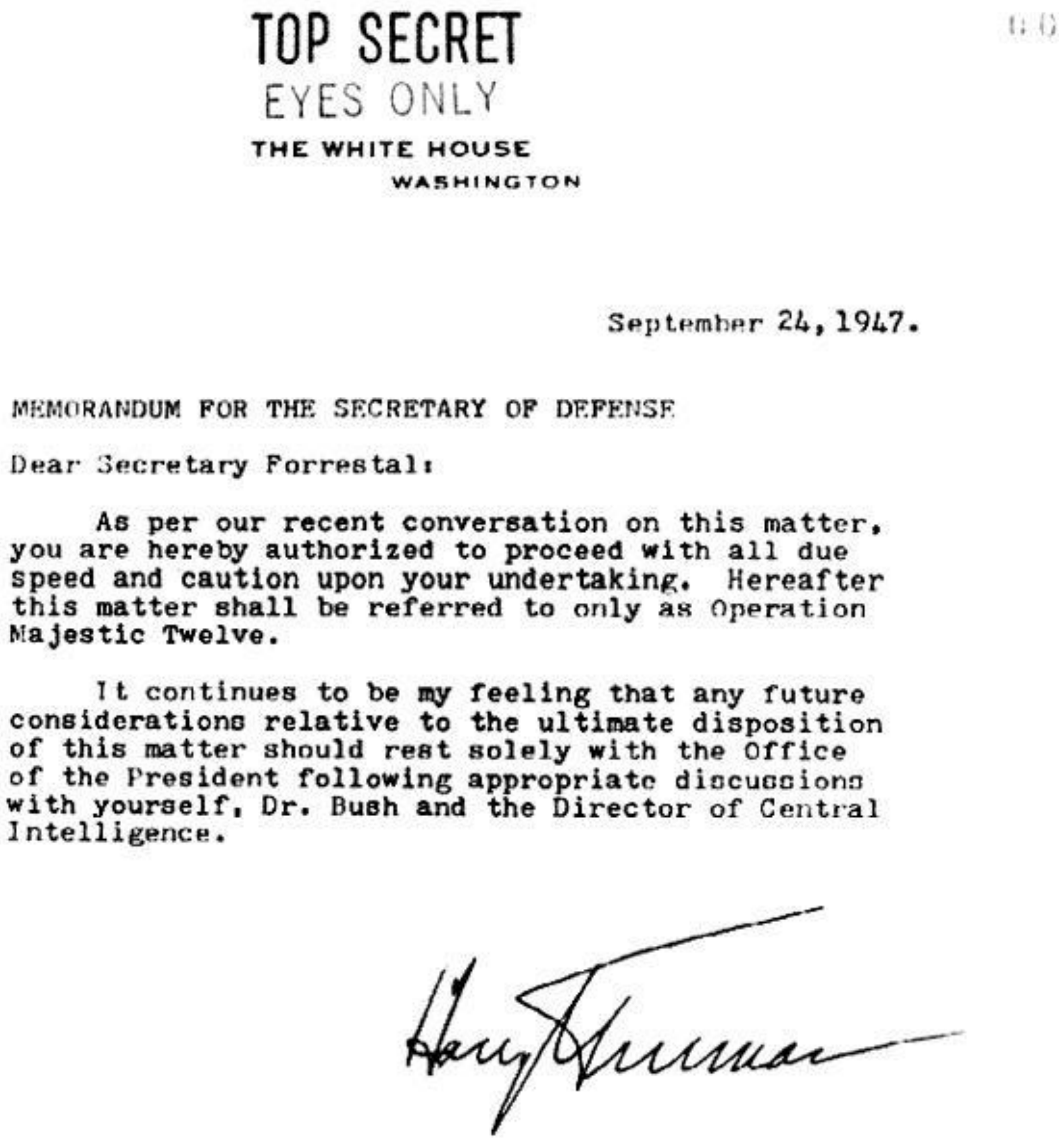
[295] Duranti, L. (1998). *Diplomatics: new uses for an old science*. Scarecrow Press.

the administrative context of the document's production and circulation, includes the people and agencies or institutions involved. This contains the letterhead, the date issued, the superscription (if present, this will signal the author of the document), inscription (which indicates the intended audience or receiver), salutation and subject.[296] The text of the document typically makes up the bulk of the document, and it constitutes the desires of the author or authorizing agency, might provide description or evidence of a singular act, or describes the memory or impact of an act. While this might be the most salient part of the document for the majority of scholars, simply understood as the content, with respect to diplomatics it is to be similarly considered as the document's other qualities. The final intrinsic element of a text is the eschatol, or the attestation of the context of the documents final authorization, which might include another date specific to the witnessing or signing of a document; in addition to complimentary clauses or any accompanying notes about the circumstances of signing. For the purposes of analyzing the MJ-12 documents, diplomatics is a particularly salient methodology with its focus on individual documents outside of documentary context, as well as their aesthetic and formal qualities. In its resurgence with respect to electronic records, an attention to the tools of production are also of interest.

For their part, the ufologists working to authenticate the MJ-12 documents circle these techniques, claiming their authority but rarely implementing the most thorough practice. Take for

[296] While there are more granular definitions and explanation of protocol that relate to the specific qualities of medieval documents that have religious contexts of production and circulation.

example, the examination of the signature of Harry S. Truman in the Truman-Forrestal memo.



TOP SECRET

EYES ONLY

THE WHITE HOUSE
WASHINGTON

September 24, 1947.

MEMORANDUM FOR THE SECRETARY OF DEFENSE

Dear Secretary Forrestal:

As per our recent conversation on this matter, you are hereby authorized to proceed with all due speed and caution upon your undertaking. Hereafter this matter shall be referred to only as Operation Majestic Twelve.

It continues to be my feeling that any future considerations relative to the ultimate disposition of this matter should rest solely with the Office of the President following appropriate discussions with yourself, Dr. Bush and the Director of Central Intelligence.

Harry Truman

Figure 7: The Truman-Forrestal Memo Credit: Ryan Woods

Diplomatics draws a clear line from the status and form of a particular signature to the document’s claims to authenticity; authentication “is the legal recognition that a signature is affixed by and belongs to the person whose name it expresses, that a document is what it purports to be, or that a copy conforms to an original.[297] Since the signature of Harry S. Truman is present on a multitude of documents that can be authenticated quite easily, it is one of the many things that has fixated ufologists on either side of the authentication debate. Stanton Friedman and the Woods have drawn parallels to another known memo from Truman to Vannevar Bush written in 1947. Philip Klass and other skeptics have attempted to prefigure assumptions around the signature's resemblance to other Truman documents by focusing on the mediation of the MJ-12 documents. Klass has specifically pointed to the possibility of Xerox technology being used by forgers to create an identical signature.[298] By calling attention to the potential forgery enabled by xerography, Klass may have accidentally put these documents into dialog with some of the most famous leaked classified documents in American history, the Pentagon Papers. Daniel Ellsberg's process of photocopying and releasing what later became known as the Pentagon Papers involved editorial work through Xerox, as he sometimes omitted classified markings or other contextual information, understanding the documents' evidentiary value as something entirely outside of bibliographic fidelity or aesthetic consistency.[299]

The MJ-12 Documents as Imagined Records

In two articles, archival scholars Anne Gilliland and Michelle Caswell position the concept of imagined records as a resistant framework challenging juridical standards of evidence that have understood records narrowly, discounting affective registers, eyewitness testimony and collective counter-narratives.[300] This work seeks to expand the function of the record both inside

[297] Duranti, L. (1998). *Diplomatics: New Uses for an Old Science.* Scarecrow Press.

[298] Klass, P. (1990). New evidence of MJ-12 Hoax. Skeptical Inquirer.

[299] Gitelman, L. (2014). *Paper knowledge: Toward a media history of documents*. Duke University Press.
Chicago

[300] Caswell, M., & Gilliland, A. (2015). False promise and new hope: dead perpetrators, imagined documents and emergent archival evidence. *The International Journal of Human Rights, 19*(5), 615-627.

and outside of official contexts. Narratives proliferate around the MJ-12 documents in spite of the dubious results of decades long investigations into their authenticity, suggesting that their persistence fulfills functions external to traditional juridical evidentiary structures. The documents express a collective desire to prove not just the existence of extraterrestrials, but also the existence of a long-standing government cover-up. The confirmation of these desires could only be expressed by leaked government documents. Classified information infrastructure facilitates the imaginary by relying on a persistent informational absence.

Caswell and Gilliland offer up a critique of the quest for a singular truth. In the fact of its spectacular inadequacy within the context of post-conflict societies or human rights related tribunals, a singular truth is not only impossible but may not be desirable. While the stakes in this case are radically different, the evidential economies and parallel scientific institutions maintained and nurtured by ufologists express a similar desire to operate outside of the bounds of the accepted. The MJ-12 documents are a unique example of this, as they still commit to the primacy of the tangible, which is roundly taken apart in Gilliland and Caswell's critique. The records and the vibrant debates around their authenticity also provide an opportunity for a subversion of official truth-making and the state's version of events. For any community defined by an adversarial relationship to the state, especially one characterized by paranoia and lack of trust, the control over the mechanisms of authorizing evidence are paramount.

Conclusion

Gilliland, A. J., & Caswell, M. (2016). Records and their imaginaries: imagining the impossible, making possible the imagined. *Archival Science*, *16*(1), 53-75.

This dissertation is partly an experiment in thinking infrastructurally about classified information. In attempting to pin down the constituent parts of classified information infrastructure, we have new insight into the ways in which records are produced, managed and preserved (or not) within a complex array of technological, organizational and social arrangements. Rather than use this conclusion to revisit some of the previous arguments made, what follows will consider some of the larger conceptual and practical shifts required by thinking infrastructurally, and how these developments can affect change within Archival Studies, Information Studies and Infrastructure Studies.

Each chapter in this dissertation focused on a piece of the infrastructure puzzle, but what can bringing them together do? At the level of policy and training, an ideal type of classified information infrastructure is articulated. This ideal type assumes the legitimacy of official secrecy and represents information as a carrier of potential risk building classified information into the fabric of narratives of national security. Classified information infrastructure is co-constituted by ever deepening investments and reliance on private contracts. As public investment in technological infrastructure has waned, the technologies of classification have become significant competitive markets. Work that had been conceived of as inherently governmental is up for bid, under the dominant rubric of efficiency and cost-effectiveness. This rearrangement of investment prioritizes short term commitments over enduring ones. The national security industrial complex blurs distinctions between political and economic commitments, figuring public information as an untapped profit center and eliding significant questions about long term use and integrity.

Classified information infrastructure is irrevocably embedded within private economic networks. Infrastructure is built upon an installed base, its persistence and strength the flipside of its intractability. This base includes individual devices developed with information security protocols, proprietary software, forms and formats and network architecture, just to name a few, and makes the profitability of contractors synonymous with continued security.

Rupture within classified information infrastructure is often spectacular, as the need for secrecy must always be performed in order to be justified. The close examination of the case of Hillary Clinton's private email server reveals several things including the mundanity of breakdown, the routine ignorance of protocols and guidance, the lack of technical expertise throughout the government. What was characterized as an exception and a drastic one as that is revealed to be business as usual. These punctuated spectacles justify the vitality and necessity of secrecy at the federal level. In this instance then, rupture is a structural feature of this infrastructure, rather than something that merely reveals its otherwise smooth functioning.

Paradoxically, classified information infrastructure operates in the public sphere not just through the performance of spectacular failure but also through its imaginative properties. The known existence of secret information allows for collective imaginings about the activities of the government, producing knowledge cultures and communities from the absence of information. We see this with the robust community that has formed around the Majestic-12 documents, a community with complex and unique evidentiary practices.

Problems that proliferate within classified information infrastructure are created through the interaction of protocols, technological systems and cultural norms and expectations. Competing temporalities of these constituencies create a temporal disjunction of records in which their status is troubled by anachronisms exemplified by the persistence of "print and file" practices. This leads to an artificially hampered record, keeping systems bounded by the inability of law and technology to participate in an even exchange. As records move through a system, the system itself becomes as much a document of organizational practice as the content or form of an individual record.

We must move beyond the assumptions built into both the life-cycle model of records and archives management and the records continuum model, as they still conceptualize some kind of fixed entity that moves within a system. In thinking infrastructurally about classified information, it becomes imperative to shift the figure and ground to consider the system itself as the record. This does not eliminate the need for assessing value, implementing retention schedules, conducting appraisal and other such activities, but does require archival thinking to be part and parcel of every day communication practices. As we have seen, NARA does not have the financial or logistical support to substantively address their existing workload much less act in oversight or regulatory capacities. However, as records become ever more embedded in complex arrangements of proprietary hardware and software, and overlapping systems of recordkeeping and networked communication, it is vital for NARA to reconceptualize its relationship to the daily work of government agencies; integrating their principles and practices from the point of creation instead of acting only after the transfer of records occurs between agencies. Classified records themselves also need reconceptualization, as they are new records with each iteration.

This temporal disjuncture has also led to an increase in transferring human expertise in marking and handling records to automated systems. This is both a response to complexity and cost, but fundamentally shifts responsibility as well as practice. While standards and protocols for marking and handling classified information are public knowledge, published routinely by government agencies in accessible forms, the details of proprietary software and hardware are not available to citizens, rendering this layer of transparency inert. Thinking infrastructurally about classified records enables us to shift the narrative away from rupture as exceptional and recognize a system in a state of perpetual breakdown that requires a radical rethinking. Particularly if we continue to see government records as key to a sustained healthy relationship between citizens and the state, as a critical tool in crafting historical narrative, and the formation of diverse knowledge communities. Further work needs to be done toward developing a model of system as record that adequately addresses these prevailing issues. Additionally, this work focused on the United States federal context specifically. Future work could consider the ways in which cultures of secrecy and the historical development of secrecy infrastructure develop alongside political cultures. Much of the conspiracy theory literature labors to point to a uniquely American political sensibility that produces the conditions for ongoing narratives, but this does not mean conspiracy theories do not exist elsewhere. Crucially, classified information infrastructure is no longer nationally isolated. Global economics, technologies and supply chains dominate contracts and cooperation between governments in terms of information sharing dictates that practices and standards must be legible and open enough to allow for communication. The installed base of infrastructure creates a condition of precarity in which shifting economic or political winds could present significant challenges public information.

Appendix A

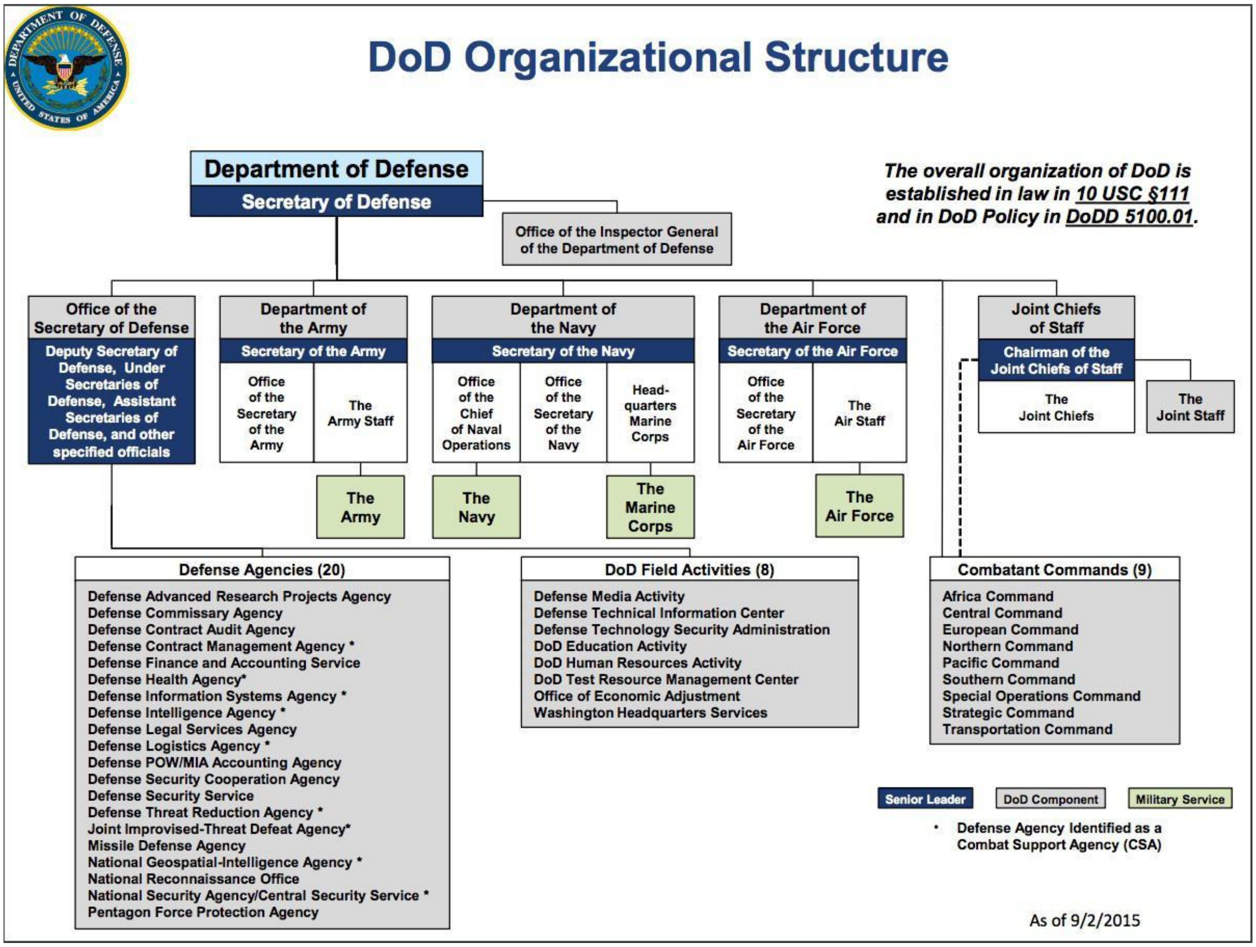
Abbreviations and Acronyms

AEA	Atomic Energy Act
ARPANET	Advanced Research Projects Agency Network
C	Confidential
CAC	Common Access Cards
CAGE Code	Commercial and Government Entity Code
CAPCO	Controlled Access Program Coordination Office
CCI	Controlled Cryptographic Items
CMDA	Code Division Multiple Access
CDO	Controlling DoD Office
CMWG	Classification Management Working Group
CNWDI	Critical Nuclear Weapon Design Information
COMINT	Communications Intelligence
COMSEC	Communications Security Information
CTS	COSMIC Top Secret
CUI	Controlled Unclassified Information
DCA	Defense Communication Agency
DCID	Director of Central Intelligence Directive
DCS	Defense Courier Service
DDN	Defense Data Network
DFARS	Defense Federal Acquisition Regulation Supplement
DIDO	Designated Intelligence Disclosure Official
DISA	Defense Information Systems Agency
DMCC-S	Defense Mobile Classified Communication - Secret
DNI	Director of National Intelligence
DoDD	DoD Directive
DoDI	DoD Instruction
DOE	Department of Energy
DoS	Department of State
DSNET 1	Defense Secure Network One
DSNET 2	Defense Secure Network Two
DSNET 3	Defense Secure Network Three
DTIC	Defense Technical Information Center
DUSD (I&S)	Deputy Under Secretary of Defense, Intelligence and Security
DTM	Directive-Type Memorandum
EMSEC	Emissions Security
E.O.	Executive Order
EPA	Environmental Protection Agency
EXDIS	Executive Distribution
FAR	Federal Acquisition Regulation
FBI	Federal Bureau of Investigation
FCL	Facility Security Clearance
FDO	Foreign Disclosure Officer

FGI	Foreign Government Information
FISA	Foreign Intelligence Surveillance Act
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FRD	Formerly Restricted Data
FSE	File Series Exemption
FSO	Facility Security Officer
FVEY	Five Allied Partners
GEOINT	Geospatial Intelligence
GRS	General Records Schedule
GSM	Global System for Mobiles
HCS	HUMINT Control System
HUMINT	Human Intelligence
HVSACO	Handle via Special Access Channels Only
IAW	In Accordance With
IC	Intelligence Community
ICD	Intelligence Community Directive
ICPM	Intelligence Community Policy Memorandum
ICRC	Interagency Classification Review Committee
IT	Information Technology
IMCON	Controlled Imagery
IPSec	Internet Protocol Security
IRS	Internal Revenue Service
ISCAP	Interagency Security Classification Appeals Panel
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
JPL	Jet Propulsion Laboratory
JWICS	Joint Worldwide Intelligence Communications System
KVM	Keyboard, Video, Mouse
LIMDIS	Limited Distribution
MASINT	Measurement and Signals Intelligence
MILNET	Military Network
MJ-12	Majestic Twelve
NARA	National Archives and Records Administration
NASA	National Aeronautics and Space Administration
NDP	National Disclosure Policy
NF	NOFORN
NOFORN	Not Releasable to Foreign Nationals
NGA	National Geospatial-Intelligence Agency
NIPRNET	Non-Secure Internet Protocol Router Net
NISP	National Industrial Security Program Policy
NISPPAC	National Industrial Security Program Policy Advisory Committee
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NNPI	Naval Nuclear Propulsion Information

NODIS	No Distribution
NSI	National Security Information
OADR	Originating Agency’s Determination Required
OCA	Original Classification authority
OCONUS	Outside of the Continental United States
ODNI	Office of the Director of National Intelligence
ORCON	Originator Controlled
OUSD(I)	Office of the Under Secretary of Defense for Intelligence
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PRA	Presidential Records Act
PROPIN	Proprietary Information
RCM	Records Continuum Model
RD	Restricted Data
RELIDO	Releasable by Information Disclosure Official
REL TO	Authorized for Release to
RF	Radio Frequency
RIM	Research In Motion
S	Secret
SAMI	Sources and Methods Information
SAP	Special Access Program
SBU	Sensitive but Unclassified
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facilities
SF	Standard Form
SI	Special Intelligence
SIGINT	Signals Intelligence
SIPRNET	Secret Internet Protocol Router Network
SLTPS-PAC	State, Local, Tribal, and Private Sector Policy Advisory Committee
SMART	State Messaging and Archival Retrieval Toolkit
SME-PED	Secure Mobile Environment – Portable Electronic Device
SMS	Short Message Service
SNM	Special Nuclear Material
SRTP	Secure Real-Time Transport Protocol
SSC	Special Security Center
STINFO	Science and Technology Information Policy
TS	Top Secret
U	Unclassified
UCNI	Unclassified Controlled Nuclear Information
U.S.C.	United States Code
USCENTCOM	United States Central Command
URL	Uniform Resource Locator
USD(I)	Under Secretary of Defense for Intelligence
U.S. IAEA AP	U.S. International Atomic Energy Agency Additional Protocol
VOIP	Voice Over Internet Protocol

Appendix B
DoD Organizational Structure



DoD Organizational Structure

The overall organization of DoD is established in law in 10 USC §111 and in DoD Policy in DoDD 5100.01.

Department of Defense
Secretary of Defense

Office of the Inspector General of the Department of Defense

Office of the Secretary of Defense
Deputy Secretary of Defense, Under Secretaries of Defense, Assistant Secretaries of Defense, and other specified officials

Department of the Army
Secretary of the Army
Office of the Secretary of the Army
The Army Staff
The Army

Department of the Navy
Secretary of the Navy
Office of the Chief of Naval Operations
Office of the Secretary of the Navy
Head-quarters Marine Corps
The Navy
The Marine Corps

Department of the Air Force
Secretary of the Air Force
Office of the Secretary of the Air Force
The Air Staff
The Air Force

Joint Chiefs of Staff
Chairman of the Joint Chiefs of Staff
The Joint Chiefs
The Joint Staff

Defense Agencies (20)

- Defense Advanced Research Projects Agency
- Defense Commissary Agency
- Defense Contract Audit Agency
- Defense Contract Management Agency *
- Defense Finance and Accounting Service
- Defense Health Agency*
- Defense Information Systems Agency *
- Defense Intelligence Agency *
- Defense Legal Services Agency
- Defense Logistics Agency *
- Defense POW/MIA Accounting Agency
- Defense Security Cooperation Agency
- Defense Security Service
- Defense Threat Reduction Agency *
- Joint Improvised-Threat Defeat Agency*
- Missile Defense Agency
- National Geospatial-Intelligence Agency *
- National Reconnaissance Office
- National Security Agency/Central Security Service *
- Pentagon Force Protection Agency

DoD Field Activities (8)

- Defense Media Activity
- Defense Technical Information Center
- Defense Technology Security Administration
- DoD Education Activity
- DoD Human Resources Activity
- DoD Test Resource Management Center
- Office of Economic Adjustment
- Washington Headquarters Services

Combatant Commands (9)

- Africa Command
- Central Command
- European Command
- Northern Command
- Pacific Command
- Southern Command
- Special Operations Command
- Strategic Command
- Transportation Command

Senior Leader | DoD Component | Military Service

* Defense Agency Identified as a Combat Support Agency (CSA)

As of 9/2/2015

References

The 9/11 commission report: Final report of the national commission on terrorist attacks upon the United States. Government Printing Office, 2011.

Abrams, P. Notes on the Difficulty of Studying the State. Paper delivered at the 1977 British Sociological Association. University of Durham.

Acker, A. (2014). Born Networked Records: A History of the Short Message Service Format.

Alberts, D. S., & Hayes, R. E. (2006). *Understanding command and control*. ASSISTANT SECRETARY OF DEFENSE (C3I/COMMAND CONTROL RESEARCH PROGRAM) WASHINGTON DC.

Atherton, J. (1985). From life cycle to continuum: some thoughts on the records management–archives relationship. *Archivaria*, *21*, 43-42.

Barthes, R. (1994). 11 The Death of the Author. *Media Texts, Authors and Readers: A Reader*.

Bartholomew, R. E. (1991). The quest for transcendence: An ethnography of UFOs in America. *Anthropology of Consciousness*, *2*(1-2), 1-12.

Beniger, J. (2009). *The control revolution: Technological and economic origins of the information society*. Harvard university press.

Benkler, Y., Roberts, H., Faris, R., Solow‐Niederman, A., & Etling, B. (2015). Social mobilization and the networked public sphere: Mapping the SOPA-PIPA debate. *Political Communication*, *32*(4), 594-624.

Benkler, Y. 2006. *The wealth of networks: How social production transforms markets and freedom*. New Haven, Conn.: Yale University Press.

Bentham, J. (1827). *Rationale of Judicial Evidence: Specially Applied to English Practice* (Vol. 5). Hunt and Clarke.

Berlet, C. (2009). Fears of Federalisme in the United States: The case of the 'North American Union'conspiracy theory. *Fédéralisme Régionalisme*.

Berlet, C. (2005). Protocols to the Left, Protocols to the Right: Conspiracism in American Political Discourse at the Turn of the Second Millennium. In *conference: Reconsidering "The Protocols of the Elders of Zion* (Vol. 100, pp. 30-31).

Birchall, C. (2011). Introduction to 'Secrecy and Transparency' The Politics of Opacity and Openness. *Theory, Culture & Society*, *28*(7-8), 7-25.

Bloecher, T. (1967) Report on the UFO Wave of 1947. Self-Published. Retrieved January 7, 2017.

Bowker, G. C., & Star, S. L. (1996). How things (actor-net) work: Classification, magic and the ubiquity of standards. *Philosophia*, *25*(3-4), 195-220.

Bowker, G. C., & Star, S. L. (2000). *Sorting things out: Classification and its consequences*. MIT press.

Bratich, J. Z. (2008). *Conspiracy panics: Political rationality and popular culture*. suny Press.

Bratich, J. (2006). Public secrecy and immanent security: a strategic analysis. *Cultural Studies*, *20*(4-5), 493-511.

Brewer-Giorgio, G. 1988. Is Elvis alive? New York: Tudor.

Briet, S., Day, R. E., Martinet, L., & Anghelescu, H. G. (2006). *What is documentation?: English translation of the classic French text*. Scarecrow Press.

Brooks, N. (2006). The Protection of Classified Information: The Legal Framework. *National Security Issues*, 139.

Bump, P. (2014). Here's how the IRS lost Emails from Key Witness Lois Lerner. The Washington Post. Retrieved February 2, 2017.

Burleigh, N. (2016) George W. Bush White House 'Lost' 22 Million Emails. Newsweek. Retrieved February 2, 2017.

Bush, G. W. (2001). *The President's Management Agenda, Fiscal Year 2002*. EXECUTIVE OFFICE OF THE PRESIDENT WASHINGTON DC.

Bush, V. Pieces of the Action (New York: William Morrow, 1970).

Butler, P.(2003) "DNA test proves body was Braun's" Centralian Advocate.

Butler, S. M. (1985). *Privatizing Federal Spending. A Strategy to Eliminate the Deficit*.

Byford, J. (2011) *Conspiracy Theories: a critical introduction*. Springer.

Cash, R. (1963). Presidential power: Use and enforcement of executive orders. *Notre Dame Lawyer* 39(1), 44-55.

Caswell, M. (2014). *Archiving the unspeakable: silence, memory, and the photographic record in Cambodia*. University of Wisconsin Press.

Caswell, M., & Gilliland, A. (2015). False promise and new hope: dead perpetrators, imagined documents and emergent archival evidence. *The International Journal of Human*

Rights, *19*(5), 615-627.

Chicago and Southern Airlines v. Waterman Steamship Cor., 333 U.S. 103, 111 (1948).

Chozick, A. (2016). Hillary Clinton Gives U.F.O. Buffs Hope She Will Open the X-Files. The New York Times. Retrieved January 7, 2017

Citizens' Commission on Benghazi. Declaration of the Citizens' Commission on Benghazi. Retrieved. January 6, 2017.

Clanahan, K. D. (2013). Wielding a Very Long, People-Intensive Spear: Inherently Governmental Functions and the Role of Contractors in US Department of Defense Unmanned Aircraft Systems Missions. *AFL Rev.*, *70*.

Clarke, S. 2002. Conspiracy theories and conspiracy theorizing. *Philosophy of the Social Sciences*, Vol. 32, No. 2.

Clifford, S. (2009). For BlackBerry, Obama's Devotion is Priceless. New York Times. Retrieved October 20, 2016.

The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. White Paper, May 22, 1998.

Cohen, D. The History of privatization: How an Ideological and Political Attack on Government became a Corporate Grab for Gold. Talking Points Memo. Retrieved August 8, 2016.

Costas, J., & Grey, C. (2014). The temporality of power and the power of temporality: Imaginary future selves in professional service firms. *Organization Studies*, *35*(6), 909-937.

Cox, R. J., & Duff, W. (1997). Warrant and the definition of electronic records: questions arising from the Pittsburgh Project. *Archives and Museum Informatics*, *11*(3), 223-231.

Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection. October 1997.

Davis, D. B. (1971). *The fear of conspiracy: Images of un-American subversion from the revolution to the present* (Vol. 113). Cornell University Press.

Dearen, J. Judge Allows Polk to Question Psychic. East Bay Times. Retrieved January 7, 2017.

DEF. DEP'T COMM. ON CLASSIFIED INFO., REPORT TO THE SECRETARY OF DEFENSE BY THE COMMITTEE ON CLASSIFIED INFORMATION 6 (1956)

Deleuze, G., & Guattari, F. (1987). A thousand plateaus.

Deleuze, G. (1992). Postscript on the Societies of Control. *October*, *59*.

Delmas, C. (2015). The Ethics of Government Whistleblowing. *Social Theory and Practice*, 77-105.

Denzler B (2001) *The Lure of the Edge: Scientific Passions, Religious Beliefs, and the Pursuit of UFOs*. Berkeley, California: University of California Press.

Department of Defense. (2012) *DoD Information Security Program: Overview, Classification and Declassification*. 5200.01, Volume 1.

Department of Defense. (2012) *DoD Information Security Program: Marking of Classified Information.* 5200.01, Volume 2.

Department of Defense. (2012) *DoD Information Security Program: Protection of Classified Information.* 5200.01, Volume 3.

Department of Defense. (2012) *DoD Information Security Program: Controlled Unclassified Information (CUI).* 5200.01, Volume 4.

Director of Central Intelligence Directive (DCID) 6/9, *Physical Security Standards for Sensitive Compartmented Information Facilities* (SCIFs)

DoD Dictionary and Terminology Repository.

DuGay, P. (2000) In Praise of Bureaucracy: Weber – Organization – Ethics. London: Sage.

Duranti, L. (1998). *Diplomatics: new uses for an old science*. Scarecrow Press.

Duranti, L., & MacNeil, H. (1996). The protection of the integrity of electronic records: an overview of the UBC-MAS research project. *Archivaria*, *42*.

Edwards, D. F. (2010). OCIs in Construction Contracting: Bumps in the Road Ahead. *Procurement Law.*, *46*, 4.

Edwards, P.N. "Infrastructure and Modernity: Force, Time, and Social Organization in the History of Sociotechnical Systems," Modernity and Technology, T.J. Misa, P. Brey, and A. Feenberg, eds., MIT Press, 2004, pp. 185–225.

Eghigian, G. (2015). Making UFOs make sense: Ufology, science, and the history of their mutual mistrust. *Public Understanding of Science*.

Eilon, L. and Lyon J. (2010). White Paper: Evolution of Department of Defense Directive 5100.01 "Functions of the Department of Defense and Its Major Components"

Exec. Order 13526. 75 C.F.R. 707 (2009).

Exec. Order 13636 78 C.F.R. 11737 (2013).

Fairclough, N.(2003). Analysing Discourse: Textual Analysis for Social Research. London: Routledge.

Fairclough, N. and Holes, C. (1995). Critical Discourse Analysis: The Critical Study of Language. Longman.

Fairclough, N. (2001). Language and Power. Longman.

Farrell, H., & Finnemore, M. (2013). The end of hypocrisy: American foreign policy in the age of leaks. *Foreign Affairs*, *92*(6), 22-26.

Federal Records Act. 44 U.S.C. 3301.

Fink E. (2014). I Made Obama's BlackBerry. CNN. Retrieved October 12, 2016.

Fisher, L. (1995). Presidential war power. University Press of Kansas.

Foucault, M. (1979). *What is an Author?*.

Foucault, M., Rabinow, P., & Martell, L. (2001). *Truth and power*.

Friedman, S.T. (1987) CSICOP/Majestic.

Friedman, S. T. (2005). *Top Secret/Majic: Operation Majestic-12 and the United States Government's UFO Cover-Up*. Perseus Books Group.

Gaddis, J. L. (2002). A grand strategy of transformation. *Foreign Policy*, 50-57.

Galison, P. (2010). Secrecy in three acts. *social research*, 941-974.

Gallagher, S. (2016) This is the phone NSA suggested Clinton use: A $4,750 Windows CE PDA: SME PED devices were only NSA-approved mobile phones for classified communications. Retrieved October 12, 2016.

Garber, M. (2014). The Man Who Introduced the World to Flying Saucers. The Atlantic. Retrieved October 12, 2016.

Gasco-Hernandez, M. Ed. (2014) Open Government: Opportunities and Challenges for Public Governance. New York: Springer.

Gilliland, A. J., & Caswell, M. (2016). Records and their imaginaries: imagining the impossible, making possible the imagined. *Archival Science*, *16*(1), 53-75.

Gillmor, D. S., & Condon, E. U. (1970). *Scientific Study of Unidentified Flying Objects. Vision*.

Ginzburg, C., & Davin, A. (1980, April). Morelli, Freud and Sherlock Holmes: clues and scientific method. In *History workshop* (pp. 5-36). Editorial Collective, History Workshop, Ruskin College.

Gitelman, L. (2006) Always Already New: Media, History and the Data of Culture. Cambridge: MIT Press.

Gitelman, L. (2014). *Paper knowledge: Toward a media history of documents*. Duke University Press.

Good, T. (1988). *Above Top Secret: The Worldwide UFO Cover-up*. William Morrow & Company.

Government CIO Magazine (2012). Interview with Susan H. Swart, CIO, Department of State.

Graeber, D. (2015) The Utopia of Rules: On Technology, Stupidity, and the Secret Joys of Bureaucracy. New York: Melville House.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the US surveillance state*. Macmillan.

Gurstein, M. (2011) Open Data: Empowering the Empowered or Effective Data Use for Everyone? First Monday.

Guttman, D. (2003). Contracting United States government work: Organizational and constitutional models. *Public Organization Review*, *3*(3), 281-299.

Hall, R. H. (1963). The concept of bureaucracy: An empirical assessment. *American Journal of Sociology*, *69*(1), 32-40.

Halloran, L. (2005). *Briefing Memorandum for the Hearing "Emerging Threats: Overclassification and Pseudo-Classification,"* Memorandum for the Members of the Subcommittee on National Security, Emerging Threats, and International Relations.

Harp, D., Loke, J., & Bachmann, I. (2016). Hillary Clinton's Benghazi Hearing Coverage: Political Competence, Authenticity, and the Persistence of the Double Bind. *Women's Studies in Communication*, *39*(2), 193-210.

Harvey, D. (2007). Neoliberalism as creative destruction. *The annals of the American academy of political and social science*, *610*(1), 21-44.

Heiser, M. (2007) The Majestic Documents: A Forensic Linguistic Report.

Henry, E. & Goddard, L. (2007) White House: Millions of e-mails may be missing. CNN. Retrieved February 2, 2017.

Hofstadter, R. (2012). *The paranoid style in American politics*. Vintage.

Hogan, Michael J. (2000). A Cross of Iron: Harry S. Truman and the Origins of the National Security State, 1945-1954. Cambridge University Press.

Hoy, D. C. (1981). Power, repression, progress: Foucault, Lukes, and the Frankfurt school. *Triquarterly*, *52*, 43.

Hull, M. (2012) Documents and Bureaucracy. The Annual Review of Anthropology. Vol 41, 251-67.

Intelligence Community Policy Memorandum (ICPM) 2005-700-1.

Jamieson, K. H. (1995). *Beyond the double bind: Women and leadership*. New York, NY: Oxford University Press.

Jenkinson, H. (1965). A manual of archive administration.

Jones, G. (2006)"Forensic Psychics Get It Right Sometimes" The Daily Telegraph (Australia).

Just Cause Ed. Barry Greenwood September 1985 Number 6

Just Cause Ed. Barry Greenwood September 1987 Number 13

Just Cause Ed. Barry Greenwood September 1990 Number 23

Just Cause Ed. Barry Greenwood September 1990 Number 25

Kafka, B. (2012) The Demon of Writing: Powers and Failures of Paperwork. Cambridge: MIT Press.

Kafka, F. (1937). The Trial, trans. Willa Muir, Edwin Muir, and EM Butler.

Keeley, B. 1999. Of conspiracy theories. *The Journal of Philosophy* 96:109-26.

Kittler, F. (1999) Gramophone, Film, Typewriter. Stanford: Stanford University Press.

Klass, P. (1990). New evidence of MJ-12 Hoax. Skeptical Inquirer.

Knezo, G. J. (2006, November). Sensitive but Unclassified Information and Other Controls: Policy and Options for Scientific and Technical Information. LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE.

Latour, B. (2010). *The making of law: an ethnography of the Conseil d'État*. Polity.

Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford university press.

Little GL (1984) Educational level and primary beliefs about unidentified flying objects held by recognized ufologists. *Psychological Reports* 54: 907-910.

Luckey, J. R., Grasso, V. B., & Manuel, K. M. (2009, June). Inherently governmental functions and Department of Defense operations: background, issues, and options for Congress. LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE.

Lynch, C. (2000). Authenticity and integrity in the digital environment: an exploratory analysis of the central role of trust.

Mahoney, J. (2000) Path Dependency in Historical Sociology, Theory and Society, 29, 507-548.

Marez, C. (2009). Obama's BlackBerry, or This Is Not a Technology of Destruction. *journal of visual culture*, *8*(2), 219-223.

Martinez, L. (2004). Looking into the crystal ball: can using a psychic help or hinder a case. *Law Enforcement Technol*, *31*(7), 52-54

Marx, K. and Engels, F. (1965) The German Ideology. London: Lawrence and Wishart

Mayer, K. (2001). With the stroke of a pen: Executive orders and presidential power. Princeton University Press.

McCaney, K. (2015). NSA Rolls Out New Classified Smartphone System. Defense Systems.

McDougall, W. A. (1985). Heavens and the earth: a political history of the space age.

McKemmish, S. (2001). Placing records continuum theory and practice. *Archival science*, *1*(4), 333-359.

Melton JG (1995) The contactees: A survey. In. Lewis JR (ed.) *The Gods Have Landed: New Religions from Other Worlds.* Albany, NY: State University of New York Press, pp. 1-13.

Milibank, D. (2016) Benghazi Conspiracy Theorists Turn on Trey Gowdy. The Washington Post.

Misa, T.J. , "How Machines Make History, and How Historians (and Others) Help Them to Do So," Science, Technology, & Human Values, vol. 13, nos. 3–4, 1988.

Moore, W. L., & Shandera, J. H. (1990). *The MJ-12 Documents: An Analytical Report*. Fair Witness Project.

National Archives and Records Administration (2016). General Records Schedule 6.1: Email

Managed Under a Capstone Approach. Retrieved February 2, 2017

National Archives and Records Administration. Email Specific Guidance and Resources and Capstone Training and Resources. Retrieved February 2, 2017.

National Archives and Records Administration. Glossary of Terms.

National Archives and Records Administration. Project Blue Book – Unidentified Flying Objects. Retrieved October 4, 2016.

National Archives and Records Administration. Records Management Toolkit. Retrieved February 2, 2017.

National Archives and Records Administration. White Paper on Capstone Approach and Capstone GRS.

National Institute for Standards and Technology. Physical Security Testing Workshop.

National Institute for Standards and Technology. Joint Task Force Transformation Initiative. (2015). Security and Privacy Controls for Federal Information Systems and Organizations NIST Special Publication 800-53 Revision 4.

National Security Act of 1947, 50 U.S.C. 3002

National Security Agency. Commercial Solutions for Classified (CSfC) Brochure.

National Security Agency. (2005) *Redacting with Confidence: How to Safely Publish Sanitized Reports Converted from Word to PDF.* Report #1333-015R-2005. Ft. Meade, MD: National Security Agency

New York Times Co. v. United States, 403 U.S. 713, 728 (1971).

Obama, Barack (2010) National Security Strategy. Office of the President of the United States, White House.

Office of Inspector General U.S. Department of State Broadcasting Board of Governors (2016) Office of the Secretary: Evaluation of Email Records Management and Cybersecurity requirements. ESP-16-03.

Office of Inspector General, Review of State Messaging and Archive Retrieval Toolset and Record Email (ISP-I-15-15, March 2015) and OIG, Inspection of the Bureau of Administration, Global Information Services, Office of Information Programs and Services (ISP-I-12-54, September 2012).

Office of Management and Budget and NARA, Memorandum for The Heads of Executive Departments and Agencies and Independent Agencies: Managing Government Records

Directive (OMB Memorandum M-12-18) (August 24, 2012)

Olmsted, K. S. (2009). *Real enemies: Conspiracy theories and American democracy, World War I to 9/11*. Oxford University Press.

Orlikowski, W. J., & Yates, J. (1994). Genre repertoire: The structuring of communicative practices in organizations. *Administrative science quarterly*, 541-574.

Osborne, D., & Gaebler, T. (1992). Reinventing government: How the entrepreneurial spirit is transforming government. *Reading Mass. Adison Wesley Public Comp*.

Oreskes, N., & Conway, E. M. (2010). Merchants of doubt.

Oxford English Dictionary.

Palmer SJ (2004) *Aliens Adored: Rael's UFO Religion.* New Brunswick, NJ; London: Rutgers University Press.

Partridge C (2003) (ed.) *UFO Religions.* London and New York, NY: Routledge.

Peck, M. J., & Scherer, F. M. (1962). THE WEAPONS ACQUISITION PROCESS; AN ECONOMIC ANALYSIS.

Peled, A. (2011) When Transparency and Collaboration Collide: The USA Open Data Program. JASIST. Vol. 61, 2085.

Peters, B.G. (2006) Path Dependency and Public Sector Reform, Paper presented at conference on Path Dependency Theory, Roskilde University, Denmark.

Peters, B.G. (2009) The Politics of Bureaucracy: An Introduction to Comparative Public Administration. 6th Ed. New York: Routledge.

Pipes, D. 1997. Conspiracy: How the Paranoid Style Flourishes and Where It Comes From. New York: Free Press.

Pirie, M. (1985). Dismantling the State. *Dallas: National Center for Policy Analysis*, 20-21.

Popper, K. S. (2012). *The open society and its enemies*. Routledge.

Presidential Policy Directive. Critical Infrastructure Security and Resilience. PPD-21. February 12, 2013.

Privacy Impact Assessment for EINSTEIN -3 – Accelerated. U.S. Department of Homeland Security. April 19, 2013.

Report of the commission on Protecting and Reducing Government Secrecy, S. Doc. No. 105-2

(1997).

Randall, J.G. (1951). Constitutional problems under Lincoln. University of Illinois Press.

RAULWING, P. (2009). The Kikkuli Text. Hittite Training Instructions for Chariot Horses in the Second Half of the 2nd Millennium BC and Their Interdisciplinary Context.

Reid, J. (2003). Deleuze's War Machine: Nomadism Against the State. *Millennium*, *32*(1), 57-85.

Roberts, A. S. (1994). *The rhetorical problems of the management expert* (Doctoral dissertation, Harvard University Cambridge, Massachusetts).

Robins, R. S., & Post, J. M. (1997). *Political paranoia: The psychopolitics of hatred*. Yale University Press.

Rumsfeld, *D. (2005) War of the Worlds*, Wall St. Journal, July 18.

Sagan, C. (1994). The search for extraterrestrial life. *Scientific American*, *271*, 70-77.

Sarangi, S. and Slembrouck, S. (2014) Language, Bureaucracy, and Social Control. New York: Routledge.

Scassa, T. (2014). Privacy and open government. *Future Internet*, *6*(2), 397-413.

Schellenberg, T. R., & Jones, H. G. (1956). *Modern archives: principles and techniques* (pp. 225-231). Chicago: University of Chicago Press.

Schetsche, M., & Engelbrecht, M. (2008). Prekäre Wirklichkeiten am Himmel–eine wissenssoziologische Schlussbemerkung. *Von Menschen und Außerirdischen. Transterrestrische Begegnungen im Spiegel der Kulturwissenschaft*, 267-277.

Schwartz, M. (2009) Department of Defense Contractors in Iraq and Afghanistan: Background and Analysis. 7-5700-R40764.

Secure Systems & Technology. TEMPEST Standards.

Shachtman, N. (2010). Pentagon to Troops: Taliban Can Read Wikileaks, You Can't. Wired Magazine.

Showalter, E. 1998. *Hystories: Hysterical Epidemics and Modern Culture*. London: Picador.

Slater, W. (October 27, 2007). "On Texas stop, Democratic Candidate Richardson Criticizes Government Secrecy". *The Dallas Morning News*.

Stacy, D. "MUFON Las Vegas Symposium" MUFON UFO Journal August 1989.

Star, S. L. (1999). The ethnography of infrastructure. *American behavioral scientist*, *43*(3), 377-391.

Sterne, J. (2012). *MP3: The meaning of a format*. Duke University Press.

Tadeo, M. (2014). FBI's James Comey Accuses China of Hacking into Every Major American Company. Independent. Retrieved October 12, 2016.

Tarantola, Andrew. (2012) "NSA Agents Will Make All Their Calls with a Fishbowl." Gizmodo.

Taylor, M. D. (1973). The legitimate claims of national security. *Foreign Aff.*, *52*.

Thompson, D. F. (1999). Democratic secrecy. *Political Science Quarterly*, *114*(2), 181-193.

Thompson, D. F. (1980). Moral responsibility of public officials: The problem of many hands. *American Political Science Review*, *74*(04), 905-916.

Thompson, D. F. (1987). *Political ethics and public office*. Harvard University Press.

Tiefer, C. (2013). Restrain 'Risky Business': Treat High-Risk Private Security Contractors as Inherently Governmental.

Tucker, P. (2016). The NSA Chief Has a Phone for Top-Secret Messaging. Here's How it Works. Defense One.

Truman-Forrestal Memo (1947). Source unknown.

Tzu, S. (1963). The Art of War. Translated by Samuel B. Griffith. *New York: Oxford University.*

United States Department of State and the Broadcasting Board of Governors Office of inspector General. (2007) Report of Inspection: Review of Department Headquarters' Implementation of Cellular Telephone Security Policies. SIA-I-07-01.

Under Secretary of Defense (2009). *Memorandum on Clarification of Current DoD Policy on Controlled Unclassified Information (CUI).*

United States v. Nixon, 418 U.S. 683 (1974).

United States Department of Justice. Federal Bureau of Investigation (2016) Clinton E-Mail Investigation: Mishandling of Classified – Unknown Subject or Country (SIM).

United States Department of State. Memorandum To All Assistant Secretaries, Assistant Secretary Equivalents, And Principal Deputies: Email Retention (July 29, 2015).

United States Department of State and the Broadcasting Board of Governors Office of Inspector General. (2013) *Evaluation of Department of State Implementation of Executive Order*

13526, Classified National Security Information. AUD-SI-13-22.

United States Department of State Office of Inspector General. (1999). *Security and Intelligence Oversight Audit: Protecting Classified Documents at State Department Headquarters.* SIO/A-99-46.

Upward, F. (1997). "Structuring the records continuum – part two: structuration theory and recordkeeping". *Archives and Manuscripts*. **25** (1): 10–35.

USA Patriot Act of 2001, 42 U.S.C. § 5195

Vienna Convention on Diplomatic Relations (VCDR)

Vismann, C. (2008) Files: Law and Media Technology. Trans. Geoffrey Winthrop-Young. Stanford: Stanford University Press.

Weber, M.(1958). Bureaucracy. In H.H. Gerth (translated). From Max Weber: Essays in Sociology. New York: A Galaxy Book.

Wilson, P. (1968). *Two kinds of power: An essay on bibliographical control*. Univ. of California Press.

Williams, L. (2015). The Issue Everyone is Missing in the Hillary Clinton Email Scandal. ThinkProgress.

Willoughby, W.F. 1918. The Institute for Government Research. *The American Political Science Association.* 12 (1).

Winthrop-Young, G. (2013). Cultural techniques: Preliminary remarks. *Theory, Culture & Society*, 30, 3-19.

Withey, K. C. (2012). Does information really want to be free? Indigenous knowledge systems and the question of openness.

Wodak, R. (1995). Critical Linguistics and Critical Discourse Analysis. Verschueren et. al. 1995.

Wodak R. 1996. Disorders of Discourse. London: Longman.

Wodak R, ed. 1989. Language, Power and Ideology. Studies in Political Discourse. Amsterdam: Benjamins.

Wolter, U. (1995). Institutional frames. *Recent Trends in Data Type Specification*, 469-482.

Wood, R. Introduction to Authenticity Ratings. Retrieved January 7, 2017.

Wood, R. Mounting Evidence for Authenticity of MJ-12 Documents. Presented at the International MUFON Symposium July 2001, Irvine, CA.

Wood, R. Ten Reasons Why Tim Cooper is NOT a Provenance Problem. Self-Published. Retrieved January 7, 2017.

Yates, J., & Orlikowski, W. J. (1992). Genres of organizational communication: A structurational approach to studying communication and media. *Academy of management review*, *17*(2), 299-326.

Zeleny, J. (2009) For a High-Tech President, a Hard-Fought E-Victory. Retrieved October 12, 2016.

Zimmer TA (1984) Social psychological correlates of possible UFO sightings. *Journal of Social Psychology 123: 199-206.*

Yin, R. K. (2013). *Case study research: Design and methods*. Sage publications.