The Securitization of Secrecy: The role of leaks in determining the function of secrecy in International Relations

By
Sean Conner

A thesis submitted in fulfillment of the requirements of Master of Research POIR899

Master of Research
In
Faculty of Arts
Department of Politics and International Relations

Macquarie University

October 2015

Table of contents

SUMMARY

The recent events of low-level government employees, disclosing secret information to both traditional and non-traditional media publishers has been responded to by the Obama administration with an increase in the number of prosecutions being executed. Such events have led to questions concerning the role of secrecy in International Relations.

Using the Copenhagen School's conceptual framework of securitization, and Gibbs' theoretical approaches of the use of secrecy in general in International Relations, this thesis discusses to what extent unauthorized disclosures reveal information about the role secrecy plays in the International Sphere.

The securitizing moves of government agencies in seeking to prevent whistleblowers and leakers from disclosing confidential information, and the reverse attempts of privacy advocates and tech companies attempting to securitize the issue of online privacy, demonstrate how this issue has moved into cyberspace. Individuals and organizations on both sides of the debate have implemented extraordinary measures in their efforts to securitize the issue.

Securitization theory provides the means and Gibbs' theoretical approaches provide the motives as to why secrecy is of such importance between governments and competing agencies. After discussing the issue, this thesis concludes that unauthorized disclosures tend to support the notion that secrecy is a valuable tool, not to prevent external enemies from understanding a state's capabilities, but rather to prevent internal agencies from disrupting the executive branch's objectives. As such, secrecy can be viewed as a tool to concentrate power in the elite, away from the general population, contrary to the ideals of democracy.

INTRODUCTION

"A secret remains a secret until you make someone promise not to reveal it."
(Fausto Cerignani in Morris 2013, 17)

For governmental executives and their empowered agencies, secrecy is a crucial tool of governance. Nowhere is this more evident than when 'national security' is involved. Balancing a free press that informs in the public interest, with control over the flow of secrets in order to protect the state, has never been more difficult than in the hyper-connected world of today. The topicality of this balancing act for contemporary politics has been illustrated by the so-called 'war on leakers' conducted under President Barack Obama in the United States. This administration has prosecuted low-level government employees and contractors who disclose information to established traditional media, or non-traditional media such as Wikileaks, without authorization. The number of leaks disseminated during this administration is greater than ever before, as is the number of leakers challenged in the courts for their actions. The issue has been framed as an existential threat to national security and justified the implementation of extraordinary measures.

The increase in leaks is partly due to the rise of non-traditional publishers that distribute online. These publishers contravene the restraint that had been adhered to since the publishing of the infamous Pentagon Papers during the Vietnam War. They use sophisticated modes of encrypting data and anonymizing their sources. This has impelled greater expertise and range in government techniques to identify leakers. Some of these methods have existed outside of extant laws and regular procedures and have themselves been the subject of damaging leaks for the US government.

This thesis examines what leaks can demonstrate about governmental use of secrecy; how successful various governments have been in securitizing leaks; and conversely, how successful privacy advocates and leakers have been in securitizing privacy and transparency in ways that may be contrary to government interests. The thesis then turns to the impact of cases in which leakers have been pursued or prosecuted and analyses what these processes can reveal about why governments need secrecy.

The thesis is divided into three sections. The first deals with the conceptual and theoretical frameworks used to examine leaks and the way in which they can

illustrate a government's use of secrecy. The first of these frameworks is the Copenhagen School (CS) concept of securitization, which will be discussed in the light of recent developments. These include the addition of a new sector of Cyberspace that is relevant to the analysis of leaks in the present, and discussion of the extent to which images can be considered a speech act. The second conceptual framework is that of the three theories of David Gibbs which seek to explain the use of secrecy by governments. These theories are: the external threat theory, the internal threat theory, and the theory of bureaucratization.

The second section examines attempts to securitize leaking by governments and alternatively, attempts to securitize privacy and transparency by leakers and privacy advocates. The language of political leaders, and the extent to which various visual images and leaks can also function as speech acts, is discussed. The section analyses the success or otherwise of securitization measures by drawing on poll data to ascertain the acceptance of the public. The data is derived from a selection of countries both affected by leaks and where there has been an attempt to implement extraordinary measures.

The third section examines what the quantifiable consequences of these leaks can tell us about the role of secrecy in governments. It shows which leaks can be classified as a threat because of disclosure to external enemies; which leaks cause little damage but are embarrassments that complicate the acquisition and maintenance of public approval; and which leaks support the notion that secrecy is often a by-product of the bureaucratic nature of government agencies. The assessments of some professionals in the field, such as academics and intelligence officers, assist in establishing the impact of leaks. Other data and examples are applied to further support these assessments.

CHAPTER ONE: THE NATURE OF SECRECY

SIMMEL AND GIBBS ON SECRECY

According to German sociologist Georg Simmel (1906), secrecy is the fundamental foundation on which all relationships are based. In *The Sociology of Secrecy and Secret Societies,* he explores the nature of secrecy in social interactions. He argued that the reciprocal nature of information exchange forms the underlying framework for all relationships. Such information exchange exists somewhere on a scale between complete knowledge, which Simmel claimed as impossible because it would require knowing all true feelings and emotions of another, and a complete lack of knowledge. When interactions are carried out with one participant having no knowledge, confidence replaces knowledge. Any information that can be hidden from others or that can be discovered, can deliver advantages in conducting the relationship.

In comparing pre-modern times to his own, Simmel acutely states that individuals had more true knowledge of one another previously because of the proximity of communities and greater homogeneity of labour. Nowadays, despite further intensification in the division of labour, and the even more distant geographical dispersion of communities, the knowledge individuals can have of one another has increased exponentially as a result of the hyper-connectivity of information networks.

Secrecy can assist to anticipate, deceive and suppress the capabilities of enemies (Colaresi 2015, 45-46). Even liberal proponents of openness and transparency admit that there are occasions when states must resort to secrecy for effective governance. In Kant's *Perpetual Peace, A second supplement and secret article* he stated that when a statesman takes advice from a philosopher he may resort to secrecy in order to avoid embarrassment (Kant 1917, 138-1309). Jeremy Bentham philosophized extensively about transparency and government openness, however, even he detailed exceptions including when the result would, "favour the projects of the enemy" (Bentham 1843, 315). The US constitution, oft-cited as a bastion of free speech, makes allowances for the use of secrecy. In a study of the need to maintain secrecy as a matter of national security versus the public's right to know, Schoenfeld (2011, 64) cites Article One of the Constitution, "Each house [of Government] shall

keep a journal of its proceedings, and from time to time publish the same, excepting such parts as may in their judgment require secrecy".

Three theories proposed by Gibbs (1995) will be explored in this thesis. Gibbs aimed to better understand the obstacles that hinder academics and other parties as they seek access to official documents for scholarly work or in the public interest. These theories are applied to various unauthorized disclosures to ascertain what they can reveal about the nature of secrecy. The nature and content of leaks as a whole and their quantifiable impact on diplomacy, military strategy and the popular support of governments and their agencies is tested.

The first theory, labeled the 'External Threat Approach', argues that secrecy in international relations is necessary to protect sensitive information from foreign enemies. The type of information classified is limited in scope and range and little effort is exerted to continue withholding information from domestic actors once the information is known externally. According to this theory, "Deception of the public is an unfortunate yet inevitable side-effect of this process" (Gibbs 1995, 214). The recent Snowden revelations are not the first time that US cryptology secrets were leaked to the rest of the world. Herbert O. Yardley, a US cryptographer working before the Second World War, revealed that a program named Black Chamber was able to decrypt the codes of radio traffic, with an estimated 45000 cryptograms from over 20 countries, including US' allies, being solved between 1917 and 1929. The revelations sparked a wave of anti-Americanism, particularly in Japan, where the sense of national humiliation was high, and resulted in Japan upgrading its security. Consequently, the US was no longer able to read their communications in a timely fashion (Schoenfeld 2010, 118-120). Schoenfeld is damning of Yardley, attributing partial blame to him for the Japanese upgrading their communication systems and ultimately the surprise attack on Pearl Harbor. This historical example of an unauthorized disclosure is an instance in which the External Threat approach seems to be supported.

The second theory, labeled the 'Bureaucratic Politics Approach', argues against the commonly accepted idea that foreign policy is a consequence of an overall strategy designed to achieve stated objectives. Instead, it argues that secrecy is merely an adherence to standard operating procedure whether it be a consequence of inter-agency competition or simply because it is the way agencies have always operated.

Gibbs highlights that interagency competition can sometimes lead to greater classification of documents so as to gain some advantage. That could explain why documents of very little academic interest are the objects of over classification (Gibbs 1995, 215). Ironically, in the wake of 9/11, the very principle of increasing intelligence sharing among agencies led to the leaking of documents such as those obtained by Wikileaks. In a statement to the Senate Committee on Homeland Security and Governmental Affairs, the increased amount of intelligence sharing is praised ten years after the attacks.

> The attacks on 9/11 showed all of us that the Cold War "need to know" system for managing classified and sensitive information drove a culture of information security that resulted in countless stovepipes and secretive pockets of the nation's most valuable information. It may have worked in the Cold War, but it was not adequate to keep America safe in a world of asymmetric threats. Many realized that protecting America in this new threat environment would require the government to operate in an entirely new way (Budinger & Smith 2011, 1).

Leakers such as Bradley Manning have been able to access vast quantities of information not directly related to their specialist fields. Such a system, as has been demonstrated, is prone to abuse and leakers.

Gibbs' final theory is labelled 'The Internal Threats Approach' and it is presented in two variants. The first argues that secrecy in government circles is a device intended to deceive the public and "ensure elite control of public policy," while the second claims that secrecy is used to promote the self interests of policy makers (Gibbs 1995, 215). In the first variant, classifying information as secret is the easiest way to suppress information and therefore diminish public awareness. Despite the best intentions of administrations in democratic states while campaigning for office, once such individuals are placed in positions of authority, they are influenced by the perceived advantages that a culture of secrecy presents. "Inevitably cabinet officers, senior agency personnel, and political appointees become persuaded by the proven efficacy of tactical bureaucracy … Each new administration develops an interest, agency by agency, in using bureaucratic techniques to expand the boundaries of secrecy (Armstrong in Theoharis 1998, 160).

The second variant contends that the release of classified information is only beneficial to policy makers when it, "reflects favourably upon themselves, [and] their

bureaux," (Gibbs 1995, 217). This is supported by examples that indicate a general desire to deny or suppress accountability. Take, for instance, the example of the US Department of Defense (DOD) denying accountability for Gulf War syndrome. Both the Department and the Pentagon, hindered attempts to declassify field reports and identify intelligence reporting systems. Even when this was done, it was only in part and, "came to be perceived by veterans, the press and even congress as part of an elaborate cover-up" (Armstrong in Theoharis 1998, 164).

SECURITIZING A THREAT

The CS developed the concept of securitization to provide a framework for widening the field of security studies beyond the military-political threats that dominated the field during the Cold War era. The core members of the CS, Buzan, Wæver and de Wilde, created a new conceptual space between security studies' traditionalists and postmodern/post-structural approaches that incorporated the economic, environmental and societal sectors. The CS argue against the notion that security threats relate solely to war and material force (Buzan Buzan, Wæver & de Wilde 1998, 4). The CS's concept of securitization should be seen not as an attempt to diminish traditional interpretations of security concerned with threats to the political and military sectors. Their aim was to "present a framework that will incorporate the traditionalist position … keeping the security agenda open to many different types of threats" and thereby respond to criticisms that "wideners risk intellectual incoherence" (Buzan et al 1998, 4).

Buzan had earlier categorised these different threats in sectoral terms. The military sector is concerned with the defensive-offensive capabilities of states and their perceptions of other states' intentions. The political sector focuses on maintaining the stability and legitimacy of governance systems and the ideologies that guide them. The economic sector is concerned with access to the resources necessary to sustain a sufficient level of welfare and sovereign control. The environmental sector concerns the maintenance and survival of bio-systems at a level that enables humans to function. The societal sector concerns the sustainability of culture and identity, such as language and customs (Buzan 2007, 19-20). The CS readily admits there is great overlap between sectors and this categorization of

security analysis is not intended to segregate. Rather, it is an attempt to facilitate and broaden the investigation of what constitutes a security threat:

> Sectors serve to disaggregate a whole for purposes of analysis by selecting some of its distinctive patterns of interaction. But items identified by sectors lack the quality of independent existence. Relations of coercion do not exist apart from relations of exchange, authority, identity, or environment. Sectors might identify distinctive patterns, but they remain inseparable parts of complex wholes. The purpose of selecting them is simply to reduce the complexity to facilitate analysis (Buzan et al 1998, 8).

The CS model demonstrates how an issue can begin as non-political; become politicized and managed within the existing political framework; then become unmanageable in that form and require other discursive action. This process is labeled securitization. However, before understanding this process, it is necessary to understand the CS definition of security. They argue "Security is about survival. It is when an issue is presented as posing an existential threat to a designated referent object" (Buzan et al 1998, 21).

The acceptance of an issue as posing an existential threat justifies the use of measures outside those normally applied. It allows a securitizing actor to adopt extraordinary means in a state of exceptionalism that exceed the hitherto norms of the political sphere. The process begins with a securitizing move and, "A discourse that takes the form of presenting something as an existential threat to a referent object" (Buzan et al 1998, 25). This discourse is otherwise referred to as a speech act, although a speech act, according to CS, cannot in itself be considered a successful act of securitization. This requires acceptance of the issue as an existential threat by an intended audience. CS impress that securitization cannot be imposed but rather, "the existential threat has to be argued and gain enough resonance for a platform to be made from which it is possible to legitimize emergency measures" (Buzan et al 1998, 25). Such resonance can be acceptance by the inner circles of political leadership, the voting public at large, or the leaders of commerce who interact with government and abide by legislation.

The CS concept of securitization is useful for the analysis of issues that cannot be neatly defined within a traditional interpretation of security in a democratic system. This thesis applies the concept to the topical phenomenon of leaks and

unauthorized disclosures in the democratic world and the prosecution of those responsible. It explores the extent to which: i) secrecy can act as a mechanism for concentrating power within the political elite while illustrating ii) how mass publics have attempted to acquire power through control over their electronic privacy and by compelling greater government transparency.

RELEVATORY 'SPEECH ACTS' AND EXPANDING THE CONCEPT

The CS framework aimed to generate some consensus about a widening of the field of security studies. One major area where there has been widespread research and criticism is the nature of the speech act or discourse required at the commencement of the securitization cycle. According to CS, if an issue is not verbalized in a discourse, the intended audience is unable to process and accept the threat, giving the speech actor authority to implement extraordinary measures that may be outside existing law or accepted procedure. Thereby the speech actor acquires a privileged power position. However, it also limits both the issues that can be securitized and the actor who can do the securitizing. As Bigo (Buzan et al. 1998, 31) argues, "Security is very much a structured field in which some actors are placed in positions of power by virtue of being generally accepted voices of security, by having the power to define security".

There are some issues that cannot be securitized due to the absence of suitable speech actors. For instance, Hansen has argued that gender is absent within the CS framework. She refers to Pakistani honour killings and violence against women in some societies. She contends that "The focus on the verbal act of speech causes difficulties in coming to terms with what can be called 'security as silence': a situation where the potential subject of security has no, or limited possibility of speaking its security problem" (Hansen 2000, 294). This may be due to a disadvantageous position held by women within such societies or, additionally and paradoxically, a speech act by the victim may bring about the existential threat to survival in itself. For example, in the case of rape in societies such as Pakistan, a woman faces victimization and honour killing if she reports the crime committed against them (Hansen 2000, 294). Despite gender not necessarily being a constant consideration in the securitization of secrecy or privacy, the common thread of security as silence is relevant as not all 'speech actors' are in a position to freely

create discourse. The incarcerated Bradley Manning and the Free Press when issued a gag order are two examples.

According to CS, only a speech act can securitize unauthorized disclosures. This severely limits the number of speech actors since some people have privileged roles that give them access to a wider audience than is normal. A politician usually has ready access to the media to create a discourse whereas a human rights advocate may not. Williams (2015, 116) notes that securitization "expands the gap between rulers and ruled in a democratic sense by concentrating discussion and action in the hands of the state executives".

Politicians and personalities who speak either for or against leaks can have a persuasive effect on an audience, but what of the leakers themselves? Manning, currently serving 35 years for leaking classified material, has been effectively silenced. Julian Assange is hindered by imprisonment in the Ecuadorian Embassy in London. Their leaks and the televisual images associated with them substitute for revelatory speech acts yet are not acknowledged within the CS framework. According to Williams, the speech act:

> is not just a metaphor; it delineates a structure of communicative action, and a framework for the explanation of social practices. The act itself is conceived of in linguistic terms, the institution refers to the position from which it is spoken, and the appropriate tool for its recognition as a securitizing act is an analysis of the rhetorical and discursive structure … of the act and its consequences. Yet … this focus stands in contrast to a communicative environment ever more structured by televisual media and by the importance of images" (Williams 2003, 525).

While CS refer to the "utterance itself that is the act," (Buzan et al 1998, 26), they have left scope for other forms of communication as the trigger. "What is essential", they argue, "is the designation of an existential threat requiring emergency action or special measures and the acceptance of that designation by a significant audience" (Buzan et al 1998, 27). It is plausible that not only a speech act can cause this; the role that (other) images can play in developing security communities should not be dismissed. Möller has written of the powerful impact images of 9/11 have had on the collective memories of individuals: "They transform violent memories into peaceful encounters". However, he states that "the power of images to form security policy should not be exaggerated" (Möller 2007, 192). Discussing the power of images in

relation to the securitization of nuclear power, with reference to the doomsday clock, Vuori (2010, 274) concludes "It is difficult to fathom how images without anchorage could bring about securitization that would not have been institutionalized previously." Vuori's 'anchorage' corresponds to what Williams labels 'image rhetorics', or the discourse that accompanies an image. He writes:

> Security policies today are constructed not only with the question of their linguistic legitimation in mind; they now are increasingly decided upon in relation to acceptable image-rhetorics. Questions of the acceptability and sustainability of security policies cannot be divorced from considerations of the impact of these policies within a logic of images (Williams 2003, 527).

While they may not constitute a trigger to substitute the discourse surrounding a speech act, images can support the rhetoric of a speech act in enabling securitization. Hansen (2011) has outlined the beginnings of a general theory of visual securitization. She cites three factors in favour of the securitizing power of the visual image: immediacy, circulability and ambiguity. She argues that the immediacy of the image allows for an audience to have an emotive response than can be in excess of the text or the discourse. Furthermore, the circulability of the image, focusing on the rapid speed and widespread space that leaks in image form can be distributed, gives importance to the power of the image as a speech act. Finally, ambiguity results in the audience not having the full context behind an image, lacking clear articulation of what is being identified allowing interpretation from the audience (Hansen 2011, 56-58). This critique is relevant as it points to speech acts being committed not solely through discourse, but also through the use of images and the act of leaking itself.

SECTORS OF SECURITIZATION

Threats and referent objects do not exist independently of one another and CS did not imply so by dividing the sectors of securitization. Rather, it was an attempt at a more easily digestible analysis of a referent object of securitization. For governing authorities, national security is a convenient mantra that can be invoked whenever it is deemed that the veil of secrecy should be maintained.

Unauthorized disclosures, therefore, are present in all sectors of the securitization framework. Some are clearer than others. For instance, Manning's disclosures of the Afghan and Iraq war log, revealed more statistics, facts and evidence of how those wars had been conducted than ever before. It was a pivotal claim of prosecutors in his court martial that the release of such information had directly aided the enemy, and this was one of 22 charges that the presiding military judge refused to dismiss in his case (Cowan 2013). It was also claimed that Snowden's leaks aided terrorists in providing the necessary information on how intelligence services were listening to their communications, and consequently the tools of how to evade such detection. Politicians in the United States asserted that Snowden's unauthorized disclosures of NSA surveillance tactics led to at least three terrorist organisations changing how they communicated (Joscelyn 2013). US secretary of State, Hilary Clinton, has implied that Snowden aided unfriendly foreign states, such as Russia, by claiming asylum there and either willingly or unwillingly gave it access to a vast treasure trove of material, thereby providing that state with unprecedented knowledge of how the US conducts surveillance (Roller 2014). These reports clearly place unauthorized disclosures within the military sector.

At the same time, unauthorized disclosures are situated within the political sector. The release of US diplomatic cables, dubbed 'Cablegate', impacted upon US diplomatic and political relationships. Brazilian President Dilma Rouseff cancelled a visit to the US after cables suggesting she and her top aides had been spied upon regarding Brazil's largest firm, the oil company Petrobas, were released (Schmitt and Schmitt 2013). There is evidence to suggest that Cablegate contributed to the revolution in Tunisia, effectively tipping the balance, and sparking political unrest across the Middle East (Brevini et al. 2013, 230). The downfall of the Tunisian Government, and the regime in Egypt thereafter, shows the cumulative effect that unauthorized disclosures released on the internet can have on political sovereignty and global affairs.

The economic sector is not immune and this can affect a government's ability to provide resources to the population. An example is the recent publishing of a secret draft of the Australian Government's core text of the Trade in Services Agreement (TiSA) negotiations, which involves Australia, North America, the European Union and parts of developed Asia. The text reveals that the Australian Government, in its

efforts to encourage foreign investment into the Australian economy, is creating legislation that will make it very difficult if not impossible for future Australian Governments to regulate areas of the economy where it currently has controls, such as in the human services sector involving child care and aged care (Dorling 2015). The leaking of confidential material shows how secrecy has become securitized at lower levels and is a matter that resonates across some of the established sectors. It also supports arguments for the creation of a sixth sector of cyberspace.

CYBERSPACE - A NEW SECTOR FOR ANALYSIS

The CS approach needs extension to accommodate advances since the formulation of their framework. Buzan and his colleagues have written of sectors whose main analytical function is to allow the various forms of interaction to be distinguished. It is not unusual to discover units and sub-units existing across different sectors (Buzan et al. 1998, 27). In considering hackers and cybersecurity, the CS argued that even if the Pentagon designates cybercriminals as a "serious threat to national security," the impact would not be felt outside the field of computer studies (Buzan et al. 1998, 25). Nearly twenty years later, the threats related to cyberspace have advanced enough to justify inclusion of a cyberspace sector into the securitization analytical framework.

Hansen and Nissenbaum (2009) have attempted to theorize this very sector, addressing the threats that characterize cyberspace, the features which differentiate it from other sectors, the number of specific cyber securitizations which can be analyzed, and the benefits and advantages that are to be gained in considering cybersecurity as a sector distinct from the others. They argue that "cyber security should be theorized as a sector where multiple discourses may be found, yet we think that understanding this multi-discursivity as arising from competing articulations of constellations of referent objects, rather than separate referent objects, better captures the securitizing and political dynamic of the field" (Hansen and Nissenbaum 2009, 1163). In other words, instead of there being distinct referent objects, such as the state, these referent objects exist as groups of networked or linked referent objects of security. If we were to consider privacy as a referent object of security, we would need to consider its linkage to the individual and consider a discourse in which societal and political referent objects are evident. Unauthorized leaks as a securitized

issue lend weight to this argument as they expose a duality showing how a state's use of secrecy has been securitized on the one hand, while on the other civil rights advocates have attempted to securitize privacy and transparency as a result of information contained in some leaks.

RESOLVING THE TWO APPROACHES

Although utilizing two uniquely different approaches to the analysis of secrecy and security, CS and Gibbs are not diametrically opposed. They offer two different understandings of the impact of secrecy in international relations. CS offer a model from which the scholar can analyze how speech actors, whether they are members of the elite or privacy advocates, attempt to remove or preclude an issue from entering the politicized realm and quarantine it in a securitized sphere. Gibbs' approaches seek to establish the motives as to why speech actors may securitize secrecy.

What CS does not offer, Gibbs can provide. CS do not explain motivating factors that contribute to why speech actors securitize an issue while Gibbs does not argue how secrecy is maintained. The two frameworks are complementary. More recent advances in theorizing the securitization framework have led to discussions concerning the image as a speech act that can trigger securitization, in addition to arguments concerning the study of cyber space as a new sector for analysis. These are two elements that can address areas not relevant before the advent of the hyper-connected digital era in which these leaks have taken place.

CHAPTER TWO: THE BLACK MARKET OF OFFICAL COMMUNICATION

THE FUNCTION AND ROLE OF LEAKS

There is nothing new about criticizing and scrutinizing the actions of authorities. In the eighth century BC, Hebrew prophets Hosea and Amos openly criticized rulers for their lack of social justice, thereby placing their own wellbeing under threat (Vinten 1994, 4). During the American War of Independence, two naval officers, Samuel Shaw and Richard Marven were accused of defamation after participating in the presentation of a petition to the fledging continental congress, which accused a naval commodore of torturing British prisoners of war. Their case resulted in the enacting of the first ever whistleblowing protection act, which made it a duty of individuals in service to the United States to report instances of 'misconduct' to the proper authorities (Kohn 2011).

Lacking universally accepted guidelines as to what constitutes whistleblowing, many academics or government departments have formulated their own working definitions. A select committee on Public Interest Whistleblowing, established in Canberra, defined whistleblowing as, "the disclosure by organization members (former or current) of illegal, immoral or illegitimate practices under the control of their employers to persons than may be able to effect action" (Select Committee on Public Interest Whistleblowing 1994, 7-12). Glazer and Glazer (1989, 3-4) refer to whistleblowers as a term used by the media to denote people who have risked their lives, careers and family security demonstrating an active concern for the public good to expose lawless acts. However, they personally refer to such people as ethical resistors, leaving room for people to blow the whistle when acts may not be illegal, but simply expose issues of potential public concern. Vinten's working definition refers to unauthorized disclosures when employees have a reasonable belief of contravention of laws or codes or practices. He illustrates that there are two forms of whistleblowing: first, in which wrong-doing is reported internally bypassing the

immediate chain of command; second, whereby disclosures are made to an outside agency, such as the media (Vinten 1994, 5).

In analyzing leaks and unauthorized disclosures through the lens of securitization, in which threats are social constructions defined by speech acts, it is crucial to distinguish between an act in which an individual believes that their leaks are for the public good rather than an act of espionage or treason. In considering what constitutes whistleblowing, this thesis is guided by the definition that whistleblowing involves the disclosing of information on illegitimate and unethical behavior, although not necessarily illegal, with the objective of causing change. It does not use the terms whistleblower and leak interchangeably yet accepts that the former is a variety of the latter.

Terril (2000, 222 – 225) identifies four main types of leaks: the venal, the ideological, the whistleblowing and the trial balloon. The trial balloon, he argues, can be considered a form of authorized leak in which an idea is spread in order to assess the reaction of an intended audience, usually the public. Generally such leaks allow reactions to be tested without it becoming widely known that the governing body is doing so. Take for instance the case of leaked documents showing defects in Australian warships under construction. The documents revealed numerous cable and combat system defects which required replacing and weld joints that were not of a satisfactory standard (Greene 2015). This came at a time when there was controversy over the cost of the warship building program, carried out ostensibly by Australian contractors, being massively over budget and more expensive than comparable projects carried out by foreign contractors abroad. The reaction to such a leak can determine whether the Australian government could contract national security matters to foreign companies with the advantage of saving money compared with using more expensive national contracts to conduct such services.

Venal leaks are described as attempts to damage a rival's reputation while promoting one's own interests. There are few possibilities to defend such leaks as they are a form of opportunism and are used to serve ambition or as a form of punishment. The CIA leaking scandal known as the Plame Affair in which a CIA operative, Valerie Plame, was publicly identified as an employee of the CIA, was one such example (Novak 2003). Her husband had travelled to Africa to verify intelligence that Saddam Hussein had attempted to source uranium and he later

published an article in the New York Times, stating that the findings of his trip to Africa had been manipulated and used by intelligence analysts to support the case for war when his report stated the opposite (Wilson 2003). It had been suggested by critics of the White House Administration that leaking Ms. Plame's name to the press was an attempt to punish Mr Wilson for his article in the New York Times (Lewis 2006). The leaker was not charged with disclosing the name of a CIA operative and a member of Vice-President Cheney's staff, who was convicted of lying to a federal grand jury in relation to this case, had his sentence commuted (Goldstein 2007).

Whistleblowing involves leakers who usually do not remain anonymous and who find legal sanctions in certain circumstances. Terril argues that the content of this type of leak, the merit of the embarrassment caused, and the alternative avenues available, will often define the ethical dimension, but that there are few laws where duty to the nation is best served by whistleblowing to external parties (Terril 2000, 223). A recent example is the exposure of corruption among the management of Australian offshore detention centres on the island of Nauru. The revelations of a whistleblower included nepotism, the conspiracy to use unreasonable force by security contractors, military imposters with unsatisfactory experience to be performing security roles, and allegations that an Australian senator, charged with investigating the detention centres on Nauru, was spied upon by the contracting security company (Main 2015). This case involved revelations of unlawful activities in an attempt to safeguard the wellbeing of individuals, both asylum seekers and expatriate security guards.

Finally there is the ideological leak, which has no legal tolerance and is not simply used to expose wrongdoing but may also be used to show an opposition to government policies, usually by senior, otherwise scrupulous public servants. This form of leak is the most common within the areas of national defence and security (Terril 2000, 224). A recent example includes cabinet leaks regarding divisions among MPs of the Liberal Party of Australia (LPA) and discussions concerning stripping the citizenship of Australian dual nationals who travel abroad to fight in terrorist organisations such as Islamic State. In this instance, there appeared to be a broad ideological opposition to the passing of this law - and possibly also an attempt to embarrass the leadership. The securitization of secrecy involves, for the most part,

whistleblowing and ideological leaks, as it is these leaks that have played the most prominent role in recent cases where whistleblowers have been pursued.

Although this thesis refers to many leaks and disclosures, the Snowden revelations and those of Bradley Manning published on Wikileaks are prominent. Considering where these leaks are placed in regard to the above definitions is pertinent. Bradley Manning's leaks can be separated into two categories: those that concern the conduct of US forces in Afghanistan and Iraq; and Cablegate, which concerns the conduct US citizens acting as diplomats. In the first instance, the information was a whistleblowing leak as both Manning and Assange believed that the data revealed acts of unlawfulness in a worst case scenario or illegitimate conduct at best. A video released online by Wikileaks under the title 'Collateral Murder' shows the deaths of a number of civilians, including two Reuters journalists, and frames the actions of US military personnel as unlawful (Boumelha 2010). Iraqi and Afghanistan war logs show numerous accounts of civilian deaths, which demonstrate that US military spokesmen had mislead enquiries into the number of deaths, both civilians and combatants, and that the war logs verified approximately 15000 additional casualties that had been previously unreported (Iraq body count 2010). There are grounds to argue that such a leak was made with genuine concerns about the legality of various military actions and that the leak was carried out as a whistleblowing leak.

On the other hand, Cablegate revealed not illegal activities as such, but rather the way in which diplomats of the US State Department conducted their business. Moreover, it showed the extent to which the State Department and diplomats were engaging in activities that, if not designed to, resulted in the acquisition of intelligence, contrary to the expected role of a diplomat.

Assange states that his aim in leaking the information is to, "allow people to understand more clearly these sort of broad activities of the US State Department, which acts not, of course, in the interest of the US people but in the interest of the State Department. It will allow other people to see that" (Stengel 2010). The release of this information cannot be defined as a whistleblowing leak but instead as an ideological leak, opposed to the way in which the US state department conducts its business and with an objective of changing these methods or at the very least to cause

embarrassment among state department officials and raise awareness among foreign citizens, whom these cables refer to.

THE DISORDERLY SITUATION TO THE END OF THE UNSPOKEN BARGAIN

In some instances, leaking can clearly be an effective tool of governance for upper echelons. This is particularly the case in trial balloon leaks and some that have originated from senior members of government and can be considered authorized. A lack of prosecutions historically is not necessarily the result of difficulties in tracking down culprits but rather reluctance due to other motives. Pozen writes that:

> It would be possible to stop a much higher percentage of disclosures. Leakiness is a product not only of external and organizational constraints but also for deliberate choices made by high-level officials within those constraints. These choices have helped an ever-growing executive to secure necessary leeway and legitimacy for governance (Pozen 2013, 518).

Some government tolerance of leaks has become acceptable so as not to upset the system. Pozen (2013, 635) refers to this tolerance as "a highly effective mechanism of information control, which has been refined through a nuanced system of social norms". To protect this mechanism, an uneasy accord was made as a result of the Daniel Ellsberg Trial and the release of the Pentagon Papers, perhaps the best-known case of unauthorized disclosures to the press in a pre-hyperconnected world. The Pentagon Papers were an investigation into relations between Vietnam and the United States leading up to the war. It revealed lies and misrepresentations that various administrations had reported to the American public concerning the ability of the South Vietnamese to govern Vietnam. In the wake of its publication, Daniel Elsberg and the New York Times, which published excerpts of the report, were charged with violating the espionage act. Stephen Bickel, who acted as legal counsel for the New York Times, described the unspoken bargain between the press and the government that came about as a result, coining the term the 'disorderly situation'. This refers to the restraint that the free press must display in publishing sensitive material so as not

to damage life or national security. Bickel believed it was preferable to an orderly situation as then either the press or the government would wield too much power:

> If we order it we would have to sacrifice one of two contending values - privacy or public discourse … If we should let the government censor as well as withhold, that would be too much dangerous power, and too much privacy. If we should allow the Government neither to censor nor to withhold, that would provide for too little privacy of decision-making and too much power in the press and in Congress (Rudenstine 1996, 350).

As a consequence of the most wide reaching and pervasive leaking scandal of that era, guidelines were established to demarcate the boundaries within which the established press had to remain. This agreement was of benefit to both parties since the government, historically speaking, had had little interest in pursuing legal battles with legitimate whistleblowers and the free press because they did not want to seem overly authoritarian, while the press now had guidelines to abide by so as not to threaten national security. Consequently the government was able to maintain its system of leaking as a tool of governance without the risk, or so it believed, of facing another Pentagon Papers type leak that would damage national security.

The first indications of an end to this accord can be seen during the second term of George W. Bush when the extensive surveillance capabilities of the NSA were revealed in the New York Times. Two journalists conducted interviews with senior officials within the NSA whose identities remained anonymous due to the extremely classified nature of the leak. It was revealed that the Bush administration had authorized warrantless telephone intercepts within the US to combat terrorism (Risen and Lictblau 2005). Outraged with the article, which went on to win a Pulitzer Prize in 2006 for national reporting, an investigation was conducted in which the Attorney General publicly announced the possibility that the New York Times and its journalists could face charges under statutes, widely believed to be the espionage act of 1917 (Pincus 2006). A senior Justice Department official outed himself as the leaker and referred to his actions as whistleblowing (Isikoff 2008). No legal actions were taken against the culprit (Savage 2011).

If the tipping point had not been reached under the Bush Administration, it was most certainly arrived at and passed during the Obama Administration. As of 2015,

the Obama administration has actively pursued, charged and sentenced six leakers of classified information pertaining to national security with an additional two cases pending, whereas there had been a mere three cases in previous administrations according to a member of the legislative council for the American Civil Liberties Union (Rottman 2014). The breakdown of this unspoken bargain can be traced to both an increase in the number of documents being marked as classified and the rise of non-traditional publishers willing to publish unredacted material. It can also be seen in the Obama administration's prosecutions of low-level government employees (McCraw and Gikow 2013, 485-492).

The emergence and growth of non-traditional publishers, such as Wikileaks and other platforms, is still a relatively new field of investigation. Their information is transmitted along communication networks that traverse the globe allowing any individual access to a publisher and the anonymity that whistleblowing requires. They can survive attempts at censoring and gagging laws existing in single jurisdictions. Attempts to take Wikileaks off-line in 2010 were responded to with over two hundred mirror sites being established, providing the same content as on Wikileaks' original website (Somaiya 2010). The quantity of classified data existing on information networks, and the leaking of this information being framed as a result of improper use of such networks, has propelled a gigantic new field of governmental securitization. It has resulted in a vast array of extraordinary and innovative measures aimed at silencing whistleblowers and leakers who would seek to share the secrets.

CHAPTER THREE: SECURITIZATION IN THE CONTEXT OF LEAKS

THE SPEECH ACT

The language used to describe leakers has either condemned them as traitors and criminals or hailed them as heroes depending on the views of the speech actor. Both sides invoke freedoms and ideals of liberal democracies to buttress their claims. Individuals have been demonized as attacking the freedoms that some contend a measure of secrecy assists. The utterances of government speech actors are carefully constructed to avoid portraying these actors as whistleblowers by questioning why they avoided using applicable protections.

When referring to Wikileaks and Julian Assange, Hilary Clinton referred to his leaking of American diplomatic cables as an "attack on the international community" (Sheridan 2010). Vice-President Joe Biden called Assange a "high tech terrorist". He initially said that the leaks did very little substantive damage, before revising his statement a day later saying that the leak had damaged the way the USA would conduct its diplomacy (MacAskill 2010). President Obama's strongest comments were made to the Turkish Prime Minister in 2010, calling the release of American diplomatic cables, "deplorable" (ABC News 2010).

Demonizing the leakers is a common first step in the speech act. This can be blatant, as in the case of Bradley Manning, who has been labeled "a traitor and not a whistleblower" by the prosecutors in his court case (Pilkington 2013). Conversely, it can be subtle as is the case of Snowden. Hilary Clinton has tried to convey a message of wrongdoing when discussing Snowden, instead of outright condemnation. She found it both "odd' and "strange" that Edward Snowden would flee the USA to leak confidential information when the USA afforded him protections as a whistleblower and that his destination of, firstly, China controlled Hong Kong and then Russia "puzzled her" (Roller 2014). In a press briefing by the State Department, attempts were made to define Snowden by what he is not, rather than what he is. According to the spokesperson "He's not a whistleblower. He's not a human rights activist. He's

wanted in a series of serious criminal charges" (Department of State 2013). By beginning to define the leakers these speech acts also begin to define the existential threat posed.

Demonizing a leaker is not enough to commence a securitizing move. Speech actors must speak security and through their discourse, state that the action of leaking information poses a credible risk to security. Generally this has been achieved by underscoring the damage leaking has caused. For instance, in the wake of the Cablegate leak, contrary to private discussions, US state department officials declared, "From our standpoint, there has been substantial damage. We believe that hundreds of people have been put at potential risk because their names have been compromised in the release of these cables" (Hosenball 2011). Potential risk to informants and people named in leaks is a commonly cited negative consequence in speech acts. After the release of the Afghan War Logs, a senior official at the Afghan Foreign Ministry said, "The leaks have put in real risk and danger lives and integrity of many Afghans" (Coghlan and Whittell 2010). Pentagon officials also made similar comments after the release of the Iraq war logs, saying that the lives of US troops and those of US allies would be put at risk after the leaking of US situation reports. (Spiegel Staff 2010) The chairman of the Joint Chiefs of Staff, Admiral Mike Mullen, expressed a similar opinion saying that the Iraq War logs leak was, "Another irresponsible posting of stolen classified documents by Wikileaks [which] puts lives at risk and gives adversaries valuable information (BBC 2010).

This alleged consequence, that enemies will have access to techniques and methods, is another oft-cited threat to security by speech actors when securitizing leaks. In his maiden speech, the newly appointed chief of the British intelligence agency MI5, Director General Andrew Parker, said of the Snowden revelations, "It makes enormous damage to make public the reach and limits of GCHQ techniques. Such information hands the advantage to the terrorists. It is the gift they need to evade us and strike at will" (Faulconbridge 2013). American counterparts make similar comments with the former deputy NSA Director from the period of the massive Snowden leak and the Director from the period around 9/11 both stating that terrorists such as those within ISIS have changed their communication methods and have been much more difficult to track. One Senate Committee member stated, "Our lax security has provided our adversaries with a gold mine of information about

tactics and procedures" (Scarborough 2014). Even lesser known cases have this strategic risk cited as a threat to security, illustrated by a recent leak of classified information in Canberra. A junior official, working as a graduate for the Department of Defence, leaked highly classified material marked 'secret five eyes', which referred to five western intelligence agencies and the sharing of agreements between them. An official from the Defence Intelligence Organisation stated that, "The leak risked serious harm to Australia's national security interest, and potentially undermined trust and reciprocal intelligence arrangements with other countries" (Knaus and Inman 2015). This junior graduate was charged with leaking the material online.

Whether the named risks are well grounded or not is not necessary to quantify when analyzing how leaks have been securitized. Rather, there appears to be a common thread in framing leakers as not having scrupulous motives and even betraying their countries, while asserting that the impact of the leaks can have disastrous consequences for national security. A comment that President Obama made in January 2014, specifically regarding Edward Snowden, summarizes the current administration's feelings towards all government employees in positions sensitive to national security:

> I will say that our nation's defense depends in part on the fidelity of those entrusted with our nation's secrets. If any individual who objects to Government policy can take it into their own hands to publicly disclose classified information, then we will not be able to keep our people safe or conduct foreign policy. Moreover, the sensational way in which these disclosures have come out has often shed more heat than light, while revealing methods to our adversaries that could impact our operations in ways that we may not fully understand for years to come (Mason 2014).

This encapsulates the general sentiment that Obama's administration holds towards those who disclose confidential government information without authorization. It frames leakers as a threat to security, making the secrecy required to govern effectively as the referent object of that security.

More speech acts were made following the Snowden revelations, aimed at bringing about further legislation that would strengthen and solidify many of the techniques and surveillance methods that the leaks sought to expose and undermine.

In a speech at Princeton University, the Director of the NSA attempted to securitize the encryption of data. He called for a system, termed Key escrow, which allowed for law enforcement agencies to have access to a key that would decrypt encrypted traffic along its networks (Perlroth 2015). The Director of the FBI has said that the efforts of Google, Apple and Facebook in adopting encryption software that, in some cases, even those companies are unable to decrypt, is making it more difficult to track the criminal activities of individuals within cyberspace. He has called for an extension of 1990 laws, which forced telecommunication companies to create infrastructure that allowed for wiretapping, to apply to IT companies also. In a speech, titled 'Going Dark: Are Technology, Privacy and Public Safety on a Collision Course?' that the Director made to a US think tank, he said, "if the challenges of real-time interception threaten to leave us in the dark, encryption threatens to lead all of us to a very dark place" (Franceschi-Bikerai 2015). According to Senator Grassley, a member of the Senate Judiciary Committee that will report on this issue, Comely had stated that the higher level of encryption found on the internet nowadays is allowing terrorist organisations such as Islamic State in Iraq and Syria (ISIL) to recruit Americans online and direct them to secure forums where they can communicate unhindered (Ybara 2015).

These attempts to securitize the issue have not gone unchallenged. Prominent players in the IT community have attempted to securitize privacy and have made their own speech acts to prevent Comely and others from achieving their aims of a decrypted internet. The specialist knowledge of these actors gives them the expertise to make securitizing moves and to speak with some authority. Hansen and Nissenbaum (2009) term this 'technification', the capacity of people with expert knowledge of cyberspace to act as securitizing actors. Power brokers from the IT community signed an open letter to President Obama asking that attempts to force companies to grant access to decryption keys for smart phones and other devices be abandoned. They argued that "Strong encryption is the cornerstone of the modern information economy's security" (Civil Society Organisations 2015). Such language frames the protection of privacy through encryption as a securitized issue – from the other side of the political contest. They have to some degree been substantiated by a report stating that the competiveness of American businesses has suffered due to the

failure of the government to address issues raised as a result of the Snowden revelations (Woolf 2015).

Lawmakers have also responded, urging the FBI to forego their proposals to gain access through decryption keys. A letter signed by both a Republican and a Democrat who were members of a subcommittee for House Oversight and Government reform on Information Technology stated three reasons why FBI proposals should not be implemented: such a move would change the dynamics of the relationship between private sector enterprise and the government; the security of communication devices made by American companies would become compromised; and such policies could easily be circumvented by criminals and terrorists who are the supposed targets of such policies (Hurd and Lieu 2015).

These voices, acting in opposition to the securitizing of secrecy, are an extension of the speech acts of leakers such as Snowden and Assange. The extent to which all leakers can be considered speech actors should be examined. While some, such as Bradley Manning, have been effectively silenced through incarceration, their leaks and images can also be considered as speech acts. For some observers, images of Manning handcuffed in his military uniform have the effect of portraying him as a martyr and hero. In the absence of oral discourse, Manning is also represented by other images, especially those that he leaked such as the Collateral Murder Video. In this instance, Hansen's (2011) argument of images having power because of their ambiguity has relevance. In the context of the video, Wikileaks was able to frame the image as a speech act, exposing immoral although not necessarily illegal, US conduct in the war in Iraq. As Hansen notes, "The ambiguity of the image grows as new audiences lack the cultural repertoire of the audience for whom the video was originally produced" (Hansen 2011, 59). The intended audience of the speech act was the general public across the world, and not the US military for which the video was originally intended. But most of the public lack the necessary context. They are unaware that a firefight had earlier taken place at the same location as the video. Ambiguity in this case serves to assist the attempt at securitizing greater transparency in conducting the war. This video also serves as a visual representation of (some of) the countless civilian deaths that are detailed in the cumbersome and complex Iraq war logs.

Since June 2012, speech acts by Assange have incorporated and integrated the image of isolation and imprisonment, whether from the balcony of the Ecuadorian Embassy, underscoring lack of freedom of movement, or on his short lived television show, *The World Tomorrow*, filmed within a single room of the embassy. Ambiguity assists the speech acts of Assange as the audience can interpret the imprisonment as a consequence of his political activities and not EU police warrants for questioning in Sweden.

Similarly, Snowden's image, now always seen in video links, serves as an image of exile and asylum, creating a context in which his revelations can be viewed: that he is a hunted man. Speaking via link during a Question and Answer session in March 2015, Snowden appealed to thirty influential members of the IT community for more 'end to end' encryption in messaging services. It was Snowden who instigated the community's backlash against the US government's decryption key demands, telling them that the future of internet freedoms rested in their control (Martin, AJ 2015). His speech act occurred in a Ted Talks special titled "Taking back the Internet". He spoke of security numerous times in an attempt to securitize government transparency and freedom of the internet. More specifically, he referred to issues revealed in documents that he leaked, such as direct access to internet communications, and implored companies to employ decryption. He framed the issue as an existential threat claiming:

> by reducing the security of our communications, [government agencies in collaboration with US IT companies] are putting America at risk in a fundamental way, because intellectual property is the basis, the foundation of our economy, and if we put that at risk through weak security, we're going to be paying for it for years (Ted Talks 2014)

Snowden places not only privacy as the referent object of security, but also western cultural identity as a symbol as well. On privacy, he states, "It is part of our cultural identity, not just in America, but in Western societies and in democratic societies around the world" (Ted Talks 2014). Snowden securitizes privacy in at least three sectors including the societal, economic and cyberspace.

ACCEPTING SPEECH ACTS TO SECURITIZE LEAKS OR PRIVACY

Buzan et al. write that securitization is not something which individuals decide by themselves in a vacuum but that it is a social construction which is ultimately decided not by those who make the speech act and speak security but by the audience (Buzan et al 1998, 29). In a democracy, it is not just the general population who is the intended audience of speech acts. Politicians often make decisions without the consensus of the voting public. A securitizing speech act can be considered politically successful if laws are passed through houses of governments, after an actor has invoked security in order to achieve such measures. In instances where democratic majorities are not necessary to implement reforms, such as within corporations, successful securitization can be measured by the ability of speech actors to convince company boards and directors to adopt what were previously considered actions outside the norm.

In order to ascertain whether secrecy and the leaking of classified information has been successfully securitized, or, while not necessarily in contrast, if it is privacy and transparency that have been securitized, it is necessary to analyze the data in regard to three main intended audiences. First, there is the political elite responsible for passing and implementing legislation, which, framed in this context either protects whistleblowers and privacy or safeguards the secrets that are disclosed through leaks. The passing of extraordinary measures such as data retention acts, and the legalizing or formalizing of invasive surveillance techniques, can be considered successful securitizations of secrecy by the political elite. Second, within liberal democracies, there is a need to assess whether the population at large accepts either the speech acts aimed at protecting secrecy or privacy. This can be assisted through analysis of polls and surveys related to various whistleblowers, and the surveillance techniques that are employed by government agencies. Third, as leaks in the modern age are ostensibly communicated over information networks, the government's ability to coerce or convince corporations to adopt extraordinary measures is a sign of a successful securitizing act. This can take the form of IT companies opening their networks for the government to trawl through or their success at persuading companies from boycotting whistleblowers or whistleblowing organisations financially.

THE POLITICAL ELITE

In 2015 the contentious Section 215 of the US Patriot Act expired. The legal challenge of the American Civil Liberties Union saw Directors of US Intelligence agencies and the US Attorney General named as Defendants. The US Court of Appeals ruled that Section 215 did not authorize warrantless electronic surveillance and demanded further proceedings be consistent with this opinion (United States Court of Appeal 2015). Despite earlier successes, the extraordinary measures of invasive surveillance techniques were being desecuritized; there no longer existed a state of exceptionalism to justify them. Their legality fell into question and their continued usage required the passing of further laws. The Freedom Act was then proposed as a substitute that would ratify the powers previously provided by Section 215 of the Patriot Act. After passing with a massive House of Representatives majority, the Freedom Act initially failed to reach the Senate majority threshold necessary to make it a law (Jacobs 2015). It is currently unclear to what extent this outcome can be regarded as the successful securitizing of privacy by its advocates. While Republican Senator Rand Paul opposed the bill in all its modifications, overall opposition in the Senate was not strong enough to prevent its passing with a majority of 67-32 (ABC NEWS 2015). The Bill prevented US agencies from warrantless surveillance of Americans and retention of metadata. The task of storing metadata activities was transferred to telephone companies.

Such laws have passed in other democratic countries with relatively broad bipartisan political support. Emergency powers were rushed through parliament in the UK despite some criticism over the speed (BBC 2014). In Australia, metadata retention acts were passed through parliament, ordering telephone companies to maintain data records for warrantless access by security agencies such as the Australian Secret Intelligence Organisation (ASIO) (Bennet 2015: A). There appears to be political support for the retention of data as a mechanism to protect matters of national security although when it comes to protecting journalists and their sources, their privacy is being safeguarded.

In contrast, the political establishment in the USA is diminishing the protections afforded to whistleblowers in areas where national security is concerned. A new regulation issued in June 2015, aimed at streamlining the investigative and adjudicative processes of Federal Government so as to make them more efficient and equitable, could be used as a retaliatory tool against whistleblowers in some agencies by curtailing their rights of appeal against dismissal or other such acts (Marcin 2015). If provisions for protection of whistleblowers decrease, the likelihood of them using specified legal and administrative avenues to voice their concerns will also decrease.

This is not to say that a successful act of securitization has occurred in all instances. Not only does an intended audience need to accept the speech act - in these cases the political elite is being referred to as the audience - but the extraordinary measures need to be implemented without impediment. As recently as July 2015, the British High court upheld a challenge to the legality of British data retention laws brought forward by both a Labor and a Conservative MP. The court ruled that the emergency laws are in opposition to EU law and that they must be repealed by March 2016 (Bowcott 2015). When passing data retention laws in the Australian Parliament, the governing coalition acquiesced to opposition demands to include a clause which protected the metadata of journalists, requiring a warrant before telephone companies need to relinquish their metadata, in order to protect the confidentiality and privacy of their sources and potential whistleblowers (Bennet 2015: B).

Various legislative acts make the securitization of data appear relatively successful. Legal challenges in the British High Court and other amendments provide *prima facie* evidence for the securitization of privacy having shared a similar level of success in the field of politics. It remains to be seen if further legislation addresses shortcomings in areas of national security.

THE GENERAL PUBLIC

The following sections examine the results of polls and surveys in the USA, Australia and the UK, which were chosen for their close intelligence ties and similar democratic sensibilities, and highlight the differences in attitudes towards Assange, Snowden and the secrets which they have revealed.

With regard to the Australian Assange, a poll conducted among the Australian population found 52% of respondents believe that he should not be prosecuted for publishing leaks, 26% thought the opposite, and the remainder were unsure. In 2012 only 40% viewed him favourably (Cooney 2012). Data regarding US public opinion shows a different story, with as many as 69% of those polled believing that Assange should face criminal prosecution for publishing classified material (IPSOS 2011). In one poll 52%, representative of the US public, responded that Bradley Manning is a traitor (Ramussen 2013). These survey examples suggest that attempts to securitize leaks pertaining to matters of military importance have been successful.

Pew Research Centre data on the publishing of Afghanistan War logs shows 42% of respondents believing Assange was supporting the public interest and 47% saying that he was harming it. Only 31% supported the release of Diplomatic Cables at the end of 2010. 60% opposed it (Pew 2010). This would suggest that Assange was more successful in securitizing greater transparency when the US public viewed his leaks as whistleblowing leaks but they were less supportive when his leaks were more ideological in nature and did not necessarily seek to expose crimes or unethical behaviour. Polls conducted in the United Kingdom show mixed results with 30% believing Assange should be prosecuted for releasing US diplomatic cables, 41% believing that he shouldn't be, and 29% unsure (Martinez 2010). The acceptance of speech acts differs globally, and may be a result of media depictions, national sentiment, or the specific language used in conducting speech acts.

Results also vary when respondents were asked about Edward Snowden and his revelations that NSA bulk data collection activities may be storing the metadata and telephone records of US citizens. Since then there is a general decline in support for NSA surveillance techniques among American voters, regardless of political affiliation. After President Obama addressed the American public concerning revisions to NSA surveillance tactics in January 2014, polls revealed that 40% approved of the Government's collection of telephone data with 53% disapproving. Six months earlier, 50% of Americans had approved with 44% disapproving (Pew 2014a). The same poll indicated that 45% believed that the public interest had been served while 43% believed it had been harmed. A majority of 56% wanted to a see a criminal case pursued against Snowden. Regardless of any normative value of Snowden's revelations, the securitizing move against these leaks was successful.

When asked about the NSA's surveillance tactics, publics in other countries express widespread disapproval. A collation of the global medians of surveyed countries revealed that 81% disapproved of monitoring citizens from their own countries, 73% disapproved of monitoring their leaders, and 62% disagreed with the monitoring of American citizens (Pew 2014b).

EXTRAORDINARY MEASURES

Successful securitization only occurs when a securitizing move, having been accepted, necessitates in the public mind the adoption of extraordinary measures. Simply adopting such measures, or the claim that an existential threat exists, does not constitute a successful act of securitization. It requires a causal relation between the two. Buzan et al. (1998, 25) argued that:

> the exact definition and criteria of securitization is constituted by the intersubjective establishment of an existential threat with a saliency sufficient to have substantial political effects … If by means of an argument about priority and urgency of an existential threat the securitizing actor has managed to break free of procedures or rules he or she would otherwise be bound by, we are witnessing an act of securitization.

What then can be identified as extraordinary measures to maintain secrecy when an 'existential threat' allegedly will result from the leaking of information? What emergency measures, if any, have been taken in the protection of privacy online or in gaining greater transparency from government? Can it be stated that such measures are not an act of securitizing privacy but desecuritizing another issue so that it (again) becomes politicized?

In regard to the first question, there is the charge of leakers aiding the enemy. Such an accusation had never been used to charge a leaker with a crime until the case of Bradley Manning. The threat to do so has also since been used against more traditional publishers (Schoenfeld 2010, 25). In Manning's case, prosecutors refused to drop the charge pre-trial. They argued that he had reasonable knowledge that terrorist organisations such as Al-Qaeda would have knowledge and access to the material he had leaked and would therefore constitute aiding the enemy (CBS 2013).

This can be viewed as an extraordinary measure as it breaks with the necessary and accepted procedures governing accusations of having aided an enemy. According to the trial judge, "general evil intent" must be demonstrated to justify this charge. However, no such evidence was produced and witnesses testified that Manning showed no sympathies towards al-Qaeda or other terrorist organisations (Amnesty 2013). Manning was eventually found not guilty of the charge of aiding the enemy (Pilkington 2013).

Second, the US Government resorted to invoking the Espionage Act of 1917 to prosecute leakers or threaten publishers. The espionage act was initially legislated in order to prevent German spies from operating in US territory during the First World War (Schoenfeld 2010, 24). With the exception of the Pentagon Papers case, the Espionage Act had only been used to prosecute spies who had obtained classified government material and had passed this to foreign governments. Under the Obama administration there has been less reluctance to prosecute leakers for activities that do not fit common definitions of espionage but have mainly involved attempts to expose unethical or illegal programs related to national security, resulting in information being passed to journalists not foreign governments. The Espionage Act was initially conceived of:

> broadly to prohibit and render criminal, attempts to obtain information respecting any aspect of the national defense for a use injurious to the United States, as well as attempts to communicate such information to foreign governments, or to any factions or parties within a foreign country, whether recognized or un recognized by the United States (Hyde 1918, 142).

Interpreting the act of a whistleblower or ethical resistor leaking information to publishers to prevent immoral actions, without the intent to harm the United States, can be considered an act outside of norms and general procedure. All individuals so far indicted with violating the espionage act have been government employees or contracted to government agencies. Section 793(e) potentially enables prosecution of anyone with control over classified documents willfully communicating them to unauthorized persons. The spectre of traitorous media and non-government employees is thereby raised. It is not clear if publishers such as Wikileaks have

willfully communicated anything within the meaning of that section of the act (Markham 2015, 8). Use of the Espionage Act to pursue whistleblowers and leakers is not in accordance with the norms originally governing the Act's application. Doing so is a clear example of an extraordinary measure under the securitization model.

Third, the adoption of new laws and regulations in various countries around the world that are granting intelligence agencies broad powers to maintain the secrecy of their operations and techniques can be seen as an extraordinary measure. The introduction of harsh penalties for people who reveal information, including journalists and leakers, attempts to prevent the dissemination of data leaks. For instance, laws implemented in Australia creating harsh penalties of up to ten years for revealing undercover operations of ASIO and the Australian Secret Intelligence Services (ASIS) (Wroe 2014). While there are already laws in place in Australia under Section 18 of the ASIO Act, which relates to disseminating information obtained in the employment of the Australian intelligence services, there had been no such provisions preventing the media from publishing the information. This would include examples such as the East Timor bugging affair in which an ASIS officer known as Witness K blew the whistle and alleged that he was part of an illegal operation (Allard 2013). This leak could effectively nullify a multi-billion dollar Australia-East Timor gas resources agreement. These newer laws will prevent further disclosures by traditional publishers. Other metadata retention acts have been established in Australia, Great Britain and France (Martin, S 2015; Powles 2015).

Government pressure on private corporations in the past and present has forced compliance with the silencing of whistleblowers or potentially revealing vital information about them. In the wake of the cablegate disclosures, Wikileaks was abandoned by many of the services that had previously catered for its needs. Paypal severed its donation link while Amazon stopped hosting its content (BBC 2010). Payment companies representing approximately 97% of the global market stopped processing donation payments to Wikileaks (Ball 2011). The only major company that does so is Mastercard, which reversed their decision as a result of a ruling in Icelandic courts (Wikileaks 2013).

Fewer in number are the extraordinary measures enacted as a result of the successful securitization of privacy. Google has responded to revelations by a program titled PRISM showing that it and other US Tech companies willingly

cooperated with US intelligence Agencies by giving them access to their servers. Google challenged a gag order in court so that it may be able to discuss the limits and extent of their cooperation with law enforcement agencies openly (Ehrenfreund 2013). Other tech companies, including Apple, Facebook and Yahoo have all denied complicity in PRISM and have gone as far as to release transparency reports detailing the number of times that law enforcement agencies have made requests to access data, well short of what is claimed in the Snowden revelations. Microsoft has conceded, "What we are permitted to publish continues to fall short of what is needed to help the community understand and debate this issue" (Lee 2014, 13), apparently support the stance taken by Google.

Companies are now implementing higher levels of encryption in their online services. For instance, Google has begun to encrypt searches with plans to roll out the services across the globe. A Google spokesman stated that the enhanced level of encryption is a direct response to the Snowden leaks: "The revelations of the past summer underscored our need to strengthen our networks. Among the many improvements we've made in recent months is to encrypt Google Search by default around the world … and encourage the industry to adopt stronger standards" (Vincent 2014). Snowden reversed his opinion on software giant Apple, hailing it as a "pioneer" as a result of the encryption now being used by default (Fingas 2015). These are examples of privacy advocates and IT companies implementing their own alternative extraordinary measures in response to government speech acts.

CHAPTER FOUR – SECRECY AND THE EXECUTIVE BRANCH

LEAKS AND THE ROLE OF SECRECY IN INTERNATIONAL RELATIONS

The current US administration's war on leaks indicates a belief in their potential impact on how government agencies conduct their business. Leaks are altering the way in which 'the enemy' is waging war. President Obama and leaders of law enforcement agencies have claimed that terrorist organisations have changed the way in which they communicate (Holden 2014; Risen 2014). These speech actors assert that secrecy is crucial to government affairs (Gibbs 1996).

Gibbs (2011, 15) argues that statements consistent with interest are far less reliable than statements that are made contrary to interest. The latter require independent verification in order to be dependable whereas the former, when they are self incriminating, are much more "compelling". Accordingly, statements made by President Obama and other speech actors within his administration are consistent with their interests and consequently require independent evidence for verification. In contrast, the revelatory accounts of whistleblowers and leakers who insiders are more credible when revealing potentially damaging information regarding their conduct and activities. Gibbs compares the revelations of an ex-CIA employee about a USA intervention in Indonesia during a military coup in 1965, with the claims of another CIA employee that intervention was limited. Gibbs argues:

> surely it would not be in the interest of [the ex-CIA agent] to claim that he worked for an institution that caused the deaths of half a million people. His statements seem self-incriminating to some degree and therefore more credible (Gibbs 2011, 15).

As an insider and employee (albeit a contractor) for the US government, Edward Snowden incriminated himself by exposing his organisation as being responsible for gross abuses of surveillance. The testimony of other ex-government employees turned whistleblowers, who spoke in support of Snowden calling him a patriot not a

traitor, are also a form of self-incrimination and thus a credible source of information (Democracy Now 2013). Gibbs does not address the point that these commentators are no longer with the organisations that they sought to expose. This is relevant because the level of self-incrimination could thereby be diminished. Moreover the hero status of leakers among some sectors of the public can be interpreted as an interest. In order to illuminate the concept and practice of secrecy through the study of leaks, independent verifiable evidence needs to be addressed in all instances, rather than the speech acts of those acting according to their own interests.

THE EXTERNAL ENEMY THREAT

Preventing secrets from reaching the hands or eyes of an enemy is of utmost importance for states. The contemporary enemy is often a vague, generalized terrorist figure, rarely specified as an identifiable individual. Etzioni contends that "Each piece of information released potentially helps adversaries and that terrorist enemies can change their tactics accordingly with the knowledge of which tactics function and which do not" (Etzioni 2015, 32-33). The 9/11 Commission report supports this assertion. It references an article by the Washington Times that revealed Osama bin Laden's communication methods had changed stating that "leadership had stopped using a particular means of communication almost immediately after a leak to the Washington Times. This made it much more difficult for the National Security Agency to intercept his conversations" (The 9/11 Commission Report, 127). This corroborates the speech act of President George W. Bush, who claimed that leaks pose an insurmountable security risk (Rosenbaum 2005). In defending itself, the Washington Times claimed the story was not based on a leak and that the information concerning Bin Laden's communication methods had been public knowledge for years, citing Times Magazine from 1996 and CNN (Washington Times 2005).

The claim that terrorist organisations have changed their tactics as a result of the Snowden revelations can be refuted in the same manner. A study conducted by Flashpoint Global partners, which specializes in monitoring the dark web, reached certain conclusions. First, there was no significant change in the use of encryption methods by Jihadis online. Second, the release of jihadi themed encryption packages

was more responsible for driving the interest in encryption than the Snowden revelations. Third, jihadis online had been aware of government surveillance techniques before the Snowden revelations and that leak merely confirmed their suspicions (Flashpoint 2014).

US and allied officials, and then Afghan President Harmad Karzai, condemned the Afghanistan war logs leak claiming that it put lives at risk. The chairman of the Joint Chiefs of Staff said Wikileaks had blood on its hands (Leigh 2010). Now retired Secretary of Defence Robert Gates said that although risks remained, no vital intelligence had been released that could give the enemy tactical knowledge of US operations (Levine 2010). According to Gibbs (2011) this evidence is more compelling as it is not consistent with the interests or point of view that is being expressed by the US government.

One claim is that US adversaries may use the information obtained via leaks to silence or eliminate US collaborators. Evidence regarding the extent to which this has already happened is contradictory. Newsweek reported a Taliban official claiming that Wikileaks documents were examined to create "hit-lists" for individual provinces, and that one tribal elder believed to have been in contact with US forces was killed by insurgent gunmen days after the release of the Afghan war logs (Moreau 2010). During Manning's trial, Gates testified that no individual collaborators were killed as a result of the leaks and that a single assassination thereafter was of a man not named in them. Taliban claims were likely propaganda to scare potential collaborators (Fuller 2013).

Another way in which US adversaries have used information obtained from leaks is in the recruitment of terrorists. Speaking as an expert on Islamic militancy at the trial of Manning, Aboul–Enein testified that al-Qaeda had used the collateral murder video, focusing on the injuries of an innocent boy, saying that "this could be your boy". Since 2011 the group's leadership had been mostly silent regarding Wikileaks (Ramstack 2013).

The external enemies approach is credible though it has not yet resulted in precisely determining how much Wikileaks or the Snowden revelations have actually assisted US enemies. Allegations of people's lives being at risk, including collaborators, are exaggerated. There has been very little in the leaks that was not

already known, or could not have been ascertained through careful observations of military activities and intelligence agencies' tactics.

'The enemy' is a somewhat obscure term that can refer to any entity at odds with the US and its allies. It may refer to hostile states or to non-state organisations such as Al-Qaeda or Islamic State (IS). It is difficult to confirm the veracity of claims that these terrorist entities have capitalized on leaked data, but it can be established that they had been operating under assumptions of the US having such capabilities, as the Snowden revelations showed. Consequently, despite appearing a valid theory, the external threat approach cannot be the sole reason that governments practice secrecy, but rather a credible subterfuge that masks another purpose.

THE INTERNAL ENEMY THREAT

As Gibbs explains, the main role of the internal enemy threat approach is the centralizing of power, through secrecy, at the executive level in order to control public opinion. There are elements in the leaks that support this notion. First, some of the claims in the Wikileaks disclosures, particularly the warlogs, reveal higher casualty figures, especially with regard to Iraqi citizens, than were being reported by officials to the media. UK and US spokespeople insisted there were no official records that revealed the number of non-combatant casualties. The war logs revealed that there were 66081 non-combatant fatalities out of a total of 109000, 15000 of which occurred in previously unrecorded instances (Batty 2010). Second, the war logs revealed that serious misconduct among military personnel was widespread and not as isolated as had been reported. In the wake of Abu Ghraib, despite admissions as the scandal expanded, the official line remained that there were "a small number of soldiers" who took part in acts of misconduct including 27 intelligence officials, 8 personnel who knew of the misconduct without acting to correct it, and that senior commanders were involved, according to the Fay report (BBC 2004). Yet the war logs suggest there were hundreds of reports of torture and mistreatment of prisoners and that suspects went uninvestigated by military authorities (Batty 2010).

Such discrepancies between the reported information and the secret data indicate a deliberate effort to conceal the truth from the public. One purpose may be to maintain support for the war. Hiding discrepancies and inconvenient information

has been an activity of certain government agencies for over fifty years. Rourke discussed such efforts describing public information units that are tasked with preventing disclosure of embarrassing leaks that could discredit the executive branch (Rourke 1957, 547). Such an assertion tends to support the Internal Enemy threats theory variant where misrepresentation to the public is a deliberate attempt to mislead them and concentrate power with an elite. Individual interests and concerns of an elite will generally influence ideas of what is in the public good (Gibbs 1995, 217).

Notwithstanding varying public opinion in the US regarding Snowden, the release of the data has made it more difficult for the USA to continue surveillance unhindered. In a democratic system, the explicit or tacit approval of a majority is necessary to govern effectively and implement policy. It has become more difficult for government to do this. The internal threats theory gains credibility in this light, when considering that some programs disclosed by Snowden have been eliminated or scaled back. They are not within the remit of the Patriot Act or Freedom Act. For instance, the NSA must now apply for a warrant to pursue the metadata of individuals and all requests must be targeted rather than the bulk collection and analysis that had occurred previously (Diamond 2015). If revelations of these programs had not occurred, it is likely that they would still be operating.

Support for further intervention in Iraq to combat insurgent elements such as IS is considerably lower than it was before the first invasion in 2003. 72% of respondents in a Pew Research Poll (Pew 2008) supported invasion in 2004 whereas only 39% of respondents in another poll supported intervention in Iraq in 2014 (Elkins 2014). While it cannot be categorically established that leaks exposing discrepancies between actual and reported data are primarily responsible for these changes in public opinion, it is highly probable that the leaks did little to foster support for foreign American intervention.

Selective use of statistics had suggested that the US public could accept thousands of casualties if the end result would be a free and democratic Iraq (Feaver & Gelpi 1999). However, the data hid the fact that casualty tolerance is much less. Median tolerance was 500 and the mode was only 100 (Reifler, Klarevas & Gelpi 2006, 190). Clearly, the impact of casualties on public opinion is substantial. Gartner (2008) also confirms that the number of casualties, and the nature of the social

relationship with the person being asked, can affect the dis/approval rating of the President. Where they contradict those reported in media briefings, casualty statistics reported in the Iraq and Afghan war logs are an embarrassment and concern for the executive branch. There is a real concern that it could influence a negative outcome at the next election.

The internal enemies approach provides a credible explanation of secrecy as a method to concentrate power at the executive level. It partly involves withholding information from the public to bolster electoral popularity. Through its reaching constituents, rather than enemies, some illegally leaked information has embarrassed the present US government, as well as some predecessors, and possibly successors.

POLITICAL BUREACRACY

The political bureaucracy approach to secrecy in IR interprets it as the usual order of things. Agencies habitually use secrecy as an element in maintaining operations. Many leaks barely deserve the level of classification attributed to them. Thomas Blanton, Director for the National Security Archive at George Washington University, estimated that between 50% and 90% of classified documents have been over classified or should have no classification whatsoever (Blanton 2010). There is a culture of classification where higher is better, regardless of the threat posed. Of 391 832 documents released in the Afghan and Iraq war logs, 97% were classified at 'secret', the second highest level of classification denoting a grave threat to national security if revealed, despite there being little information in them that was unknown or that could not have been obtained by observing battle field tactics (Stewart 2010).

This political bureaucracy approach or theory also points to agencies maintaining secrecy because of intra-agency rivalries. There is no overall coherence (Gibbs 1995, 214-215). Ironically, after criticism from the 9/11 Commission, which ruled that intelligence agencies had been negligent in not sharing information, it is the increased access later provided to intelligence that resulted in Manning's disclosures to Wikileaks. The Director of National Intelligence stated that the USA no longer operates under the principle of compartmentalization but rather shares intelligence so that it can be accessed by those who need it (Clapper 2011).

Secrecy has been an eternal element in the operations of government agencies. A culture of over-classifying material has developed in the belief that doing so makes it more secure. Recent leaks have confirmed these claims.

CONSOLIDATION OF THEORIES

Although Gibbs' three theories vary in the motivation for the use of secrecy, they share a common thread in the case of the data leaks. Secrecy allows executive government to pursue policies, especially foreign policies, while reducing hindrance and intervention. Disclosures have hindered the USA's ability to achieve its aims without interference from either internal or external opposition, though this is not to say that the external opposition need be an enemy. Cablegate has seriously undermined US efforts to obtain candid and honest information from foreign diplomatic sources due to fear of their comments being known openly (Page & Spence 2011, 235). The release of the cables also complicated American support of unscrupulous regimes. They show, for example, that the Mubarak regime's brutality was well known to the USA. Disclosure made further support of his government untenable (Mabon 2013, 1854). Whether Cablegate caused a change of government in Egypt is debatable, but it made it impossible for the White House to continue open support for Mubarak, despite any possible desires to continue it secretly.

The impact of the leaks elsewhere in the Middle East was varied. They were critical to the downfall of the Ben Ali government in Tunisia. Diplomatic cables revealed widespread corruption among the incumbent regime, though they presented nothing that the public did not know. Nonetheless, they sparked waves of unrest that led to the collapse of the Ali regime (Brevini et al 2013, 257). The fostering of a relationship between the USA and Tunisia was impeded, only reviving with the announcement of Tunisia being upgraded in its status as a Non-NATO ally of the US (Baker 2015). More importantly, the revolution in Tunisia sparked unrest all over the Middle East, contributing to the fall of Mubarak's government and inciting war and conflict that last until today. As in Syria, where lawlessness and insurgent activity is at a peak, none of these developments are in the interest of US foreign policy.

Demonstrable or potential threats from external or internal enemies are among the reasons why states maintain secrecy. The Snowden revelations have, at

the very least, verified the surveillance capabilities of the United States and her allies. Among Western Intelligence communities and executives, fear is a contributing factor motivating the securitization of secrecy and the hunting of unauthorized leakers. However, the greatest threat to executive interests comes not from external enemies, who in most cases are aware of the capacities and motivations of the executive, but rather internal enemies. This approach is most plausible as it is from within that the interests of the executive branch can be most threatened. The United States and her allies are powerful enough that few threats originating from abroad could be realized as a result of the information disclosed in the war logs, Cablegate, or by Snowden. It is primarily internal pressures that caused provisions and amendments to various acts and legislation governing the use of invasive surveillance techniques.

The maintenance of secrecy assists concentration of power at the executive level and minimizes intervention by external or internal others over decision-making. Rival agencies can be effectively sidelined, as theories of political bureaucracy emphasize.

CONCLUSION

The role of secrecy in democratic governments has been a closely guarded function of the executive branch. Through the CS framework of securitization it is observed that there has been a change in the way in which governments deal with leakers and the information that they leak. There are various types of leaks, and it is with whistleblowers that governments have been fiercest in their response. A tacit agreement between the free press and the government, established in the aftermath of the Pentagon Papers court case, has been largely abandoned. The US Government has unrelentingly pursued leakers and those who publish them. This breakdown, in part, is a result of the rise of non-traditional publishers such as Wikileaks, but the traditional free press is by no means excluded from this new landscape.

Simmel explored the nature of secrecy in societies and the power that it wields in relationships between individuals. That same power structure exists between governments and those that they interact with, necessitating the maintenance of secrecy. This is valid whether in relation to other states, the domestic population, or non-government organisations. Analysis of Gibbs' three approaches to secrecy in international affairs, and the application of these approaches to leaks, results in this thesis concluding that secrecy allows power to be concentrated at the highest echelons within democratic states. It has argued that secrecy is crucial to preclude constituents having enough information to make decisions that may be contrary to the wishes of government.

The CS framework that was applied to leaks has been useful in understanding how democratic governments seek to silence dissent. Invoking national security, and claiming that leaking secrets is a threat to this, has allowed governments in otherwise free and liberal democratic states to impose draconian laws that limit freedom and privacy of individuals. Conversely, the same framework shows that privacy advocates and tech companies have attempted to securitize the issue of data privacy and fought the government. Both sides have had varying degrees of success, whether it has been governments in passing data retention legislation or formalizing their powers to use invasive surveillance techniques, or tech companies that have responded by harnessing greater levels of encryption in the services provided to users. These

extraordinary measures, viewed within the CS framework, show how the US public has been convinced to support governments in their attempts to outlaw leaking, or to support tech companies in ensuring greater encryption methods.

In analyzing leaks through the CS framework, a greater understanding of new research in the field is achieved. This is particularly so in regards to furthering the discussion of images as a speech act and allowing the silent to initiate the process of securitization to bring about extraordinary measures. The thesis has also added to the discussion concerning cyberspace as a new sector for analysis, and deals with the way in which non-traditional publishers existing mostly online, have assisted in defining expansion of cyberspace and its influences into other sectors. The founders of the securitization model had not dealt with these factors.

In discussing the role of leaks in determining the function of secrecy, Gibbs has provided the why, and the CS framework has enabled the how. The two approaches complement each other in assisting an explanation of how and why leaks became such a widely contested contemporary political theme.

REFERENCES

PRIMARY SOURCES

The 9/11 Commission Report. http://www.9-11commission.gov/report/911Report.pdf (accessed 8.16.15).

Blanton 2010 Hearing on the Espionage Act and the Legal and Constitutional Implications of Wikileaks, Statement to the Committee on the Judiciary U.S. House of Representatives http://nsarchive.gwu.edu/news/20101216/Blanton101216.pdf (accessed 7.26.15).

Budinger, Z., Smith, J. 2011. Senate Committee on Homeland and Governmental Affairs Ten Years After 9/11: A status Report On information Sharing. http://fas.org/irp/congress/2011_hr/101211smith.pdf (accessed 8.16.15).

Civil Society Organisations. 2015. Letter Addressed to the President of the United States. https://static.newamerica.org/attachments/3138113/Encryption_Letter_to_Obama_final_051915.pdf (accessed 9.5.15).

Department Of State. The Office of Website Management, B. of P.A., 2013. Daily Press Briefing - July 12, 2013. U.S. Department of State. URL http://www.state.gov/r/pa/prs/dpb/2013/07/211891.htm (accessed 6.4.15).

Hurd and Lieu 2015. Letter to FBI Director Comely https://www.washingtonpost.com/r/2010-2019/WashingtonPost/2015/06/01/National-Politics/Graphics/LetterFBI.pdf (accessed 8.1.15).

Wikileaks, 2013. WikiLeaks. Amazon Web Services, Inc. URL //aws.amazon.com/message/65348/ (accessed 8.16.15).

SECONDARY SOURCES

ABC NEWS, 2015. Obama signs Freedom Act to limit domestic surveillance into law. ABC News. URL http://www.abc.net.au/news/2015-06-03/us-congress-passes-bill-to-limit-domestic-surveillance/6516826 (accessed 7.26.15).

ABC NEWS, 2010. Obama slams “deplorable” WikiLeaks ABC News. URL http://www.abc.net.au/news/2010-12-12/obama-slams-deplorable-wikileaks/2371518 (accessed 8.8.15).

A.P.I., 2014. How Americans get their news. American Press Institute. URL http://www.americanpressinstitute.org/publications/reports/survey-research/how-americans-get-news/ (accessed 7.27.15).

AMNESTY, 2013. Bradley Manning: US must drop "aiding the enemy" charge. https://www.amnesty.org/en/latest/news/2013/07/bradley-manning-us-must-drop-aiding-enemy-charge/ (accessed 9.5.15).

Allard, T., 2013. ASIO raids office of lawyer Bernard Collaery over East Timor spy claim. The Sydney Morning Herald. URL http://www.smh.com.au/federal-politics/political-news/asio-raids-office-of-lawyer-bernard-collaery-over-east-timor-spy-claim-20131203-2yoxq.html (accessed 8.16.15).

Ball, J., 2011. The bankers' blockade of WikiLeaks must end. The Guardian. http://www.theguardian.com/commentisfree/2011/oct/24/bankers-wikileaks-free-speech (Accessed 11.8.15)

Batty, D., 2010. Iraq war logs: live reaction and WikiLeaks address. The Guardian. URL http://www.theguardian.com/world/2010/oct/23/iraq-war-logs-wikileaks (accessed 8.29.15).

BBC, 2014 Parliament passes emergency Data Retention Bill http://www.bbc.com/news/uk-politics-28352673 (accessed 7.26.15).

BBC, 2010. Wikileaks: Iraq war logs "reveal truth about conflict" http://www.bbc.com/news/world-middle-east-11612731 (accessed 8.9.15).

BBC, 2004. Blame widens for Abu Ghraib abuse, 2004. http://news.bbc.co.uk/2/hi/americas/3596686.stm (accessed 7.26.15).

Baker, P., 2015. Obama Upgrades Tunisia's Status as a U.S. Ally. The New York Times. http://www.nytimes.com/2015/05/22/us/tunisia-to-become-major-non-nato-ally-obama-says.html?_r=0 (accessed 8.1.15).

Bennett, J., 2015:A PM agrees to Opposition demand to modify data retention bill. ABC News. URL http://www.abc.net.au/news/2015-03-16/pm-agrees-to-modify-legislation-to-protect-journalists-sources/6323544 (accessed 6.21.15).

Bennett, J., 2015:B ASIO "pleased" with passing of data retention laws. ABC News. URL http://www.abc.net.au/news/2015-04-01/asio-pleased-by-passing-of-data-retention-laws/6363374 (accessed 6.4.15).

Bentham, J., 1843. The Works of Jeremy Bentham Volume II. Edinburgh: William Tait, Simpkin, Marshall & Co. London. Accessed from https://play.google.com/store/books/details?id=QF5GAAAAYAAJ&rdid=book-QF5GAAAAYAAJ&rdot=1 (Accessed 3/18/15).

Boumelha, J., 2010. US must deliver justice on friendly fire. The Guardian. http://www.theguardian.com/commentisfree/cifamerica/2010/apr/10/us-friendly-fire-justice-iraq (accessed 8.16.15).

Bowcott, O., 2015. High court rules data retention and surveillance legislation unlawful. the Guardian. URL http://www.theguardian.com/world/2015/jul/17/data-retention-and-surveillance-legislation-ruled-unlawful (accessed 7.26.15).

Brevini, B., Hintz, A., McCurdy, P. (Eds.), 2013. Beyond WikiLeaks. Palgrave Macmillan, Basingstoke.

Buzan, B., Wæver, O., Wilde, J. de, 1998. Security: a new framework for analysis. Lynne Rienner Pub, Boulder, Colo.

Buzan, B., 2007. People, states & fear: an agenda for international security studies in the post-cold war era, 2. ed. ed, ECPR classics. ECPR Press, Colchester.

CBS, 2013. Bradley Manning acquitted of aiding the enemy for giving secrets to WikiLeaks. URL http://www.cbsnews.com/news/bradley-manning-acquitted-of-aiding-the-enemy-for-giving-secrets-to-wikileaks/ (accessed 8.13.15).

Coghlan, T., Whittell, G., 2010. Leaked details put informant lives in danger. TheAustralian. URL http://www.theaustralian.com.au/news/world/leaked-details-put-informant-lives-in-danger/story-e6frg6so-1225898206990 (accessed 8.9.15).

Colaresi, M.P., 2014. Democracy declassified: the secrecy dilemma in national security. Oxford University Press, Oxford□; New York.

Cooney, P., 2012. Most Australians back Assange, poll finds. The Sydney Morning Herald. URL http://www.smh.com.au/federal-politics/political-news/most-australians-back-assange-poll-finds-20120808-23uwh.html (accessed 7.26.15).

Cowan, J., 2013. WikiLeaks source painted as fame-seeking traitor who wanted to please Julian Assange. URL http://www.abc.net.au/lateline/content/2013/s3812286.htm (accessed 6.21.15).

Clapper, J.R., 2011. How 9/11 Transformed the Intelligence Community. Wall Street Journal. http://www.wsj.com/articles/SB10001424053111904537404576554430822300352 (accessed 7.26.15).

Democracy Now, 2013. "Edward Snowden is a Patriot": Ex-NSA CIA, FBI and Justice Whistleblowers Meet Leaker in Moscow. Democracy Now! URL http://www.democracynow.org/2013/10/14/edward_snowden_is_a_patriot_ex (accessed 8.24.15).

Diamond, J., 2015. Senate passes NSA reform measure - CNNPolitics.com. CNN. URL http://www.cnn.com/2015/06/02/politics/senate-usa-freedom-act-vote-patriot-act-nsa/index.html (accessed 9.5.15).

Dorling, P., 2015. WikiLeaks Exclusive: Secret core text from Trade in Services Agreement negotiations. The Saturday Paper. URL https://www.thesaturdaypaper.com.au/news/politics/2015/07/01/wikileaks-exclusive-secret-core-text-trade-services-agreement-negotiations (accessed 7.2.15).

Ehrenfreund, M., 2013. Google, responding to Edward Snowden's leaks, challenges gag order on NSA. The Washington Post. https://www.washingtonpost.com/world/national-security/google-responding-to-edward-snowdens-leaks-challenges-gag-order-on-nsa/2013/06/19/e6bdea0a-d8ef-11e2-a9f2-42ee3912ae0e_story.html (accessed 8.16.15).

Elkins, E., 2014. Poll Reveals Americans Supported Iraq War in 2003 Far More Than They Admit Today - Reason-Rupe Surveys. Reason.com. URL http://social.reason.com/poll/2014/10/16/poll-reveals-americans-supported-iraq-wa (accessed 9.5.15).

Etzioni, A., 2015. NSA: National Security vs. Individual Rights. Intelligence and National Security 30, 100–136. doi:10.1080/02684527.2013.867221

Faulconbridge, G., 2013. MI5 chief warns Snowden data is a "gift" for terrorists. Reuters UK. URL http://uk.reuters.com/article/2013/10/08/uk-usa-security-britain-idUKBRE99711K20131008 (accessed 8.9.15).

Feaver, P., Gelpi, C., 1999 A Look at … Casualty Aversion: How many Deaths are Acceptable? A surprising Answer. Washington Post .http://www.washingtonpost.com/wp-srv/WPcap/1999-11/07/061r-110799-idx.html (accessed 8.1.15).

Fingas, R., 2015. Edward Snowden hails Apple as "pioneering" for iOS 8 security measures. URL http://appleinsider.com/articles/15/06/05/edward-snowden-hails-apple-as-pioneering-for-ios-8-security-measures (accessed 8.16.15).

Flashpoint 2014 Measuring the Impact of the Snowden Leaks on the Use of Encryption by Online Jihadists https://fpjintel.com/public-reports/measuring-the-impact-of-the-snowden-leaks-on-the-use-of-encryption-by-online-jihadists/ (accessed 7.26.15).

Gartner, S.S., 2008. Ties to the Dead: Connections to Iraq War and 9/11 Casualties and Disapproval of the President. American Sociological Review 73, 690–695. doi:10.1177/000312240807300408 (accessed 8.9.15).

Gibbs, D.N., 1995. Secrecy and International Relations. Journal of Peace Research 32, 213–228. doi:10.1177/0022343395032002007

Gibbs, D.N., 2011. Sigmund Freud as a theorist of government secrecy, in: Maret, S. (Ed.), Government Secrecy. Emerald Group Publishing Limited, pp. 5–22.

Goldstein, A., 2007. Bush Commutes Libby's Prison Sentence. The Washington Post. http://www.washingtonpost.com/wpdyn/content/article/2007/07/02/AR2007070200825.html

Greene, A., 2015. Leaked documents expose problems with Air Warfare Destroyer program. ABC News. URL http://www.abc.net.au/news/2015-05-09/leaked-documents-reveal-further-problems-with-awd-program/6456848 (accessed 8.1.15).

Hansen, L., 2000. The Little Mermaid's Silent Security Dilemma and the Absence of Gender in the Copenhagen School. Millennium - Journal of International Studies 29, 285–306.

Hansen, L., Nissenbaum, H., 2009. Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly 53, 1155–1175.

Hansen, L., 2011. Theorizing the image for Security Studies Visual securitization and the Muhammad Cartoon Crisis*. European Journal of International Relations 17, 51–74. doi:10.1177/1354066110388593

Holden, M., 2014. Terrorists have changed methods since Snowden leaks: UK official. Reuters. http://www.reuters.com/article/2014/04/29/us-britain-snowden-idUSBREA3S0FQ20140429 (accessed 7.26.15).

Hosenball, M., 2011. US officials privately say WikiLeaks damage limited. Reuters. http://www.reuters.com/article/2011/01/18/us-wikileaks-damage-idUSTRE70H6TO20110118 (accessed 4.5.15).

Hyde, C., 1918. Editorial Comment. Am. J. Int'l L. 12, 142.

IPSOS Global advisor, 2011. Julian Assange and Wikileaks: Global Citizens in 24 Countries Assess the website and its actions. https://www.ipsos-na.com/download/pr.aspx?id=10833 (accessed 8.1.15).

Iraq Body Count, 2010. Iraq War Logs: What the numbers reveal. https://www.iraqbodycount.org/analysis/numbers/warlogs/ (accessed 8.9.15).

Isikoff, M., 2008. The Whistleblower Who Exposed Warrantless Wiretaps. Newsweek. URL http://www.newsweek.com/whistleblower-who-exposed-warrantless-wiretaps-82805 (accessed 7.19.15).

Jacobs, B., 2015. USA Freedom Act fails as senators reject bill to scrap NSA bulk collection. The Guardian. URL http://www.theguardian.com/us-news/2015/may/23/usa-freedom-act-fails-as-senators-reject-bill-to-scrap-nsa-bulk-collection (accessed 7.26.15).

Joscelyn, 2013. House Intel Chair: Snowden Leaks Tipped Off Al Qaeda. URL http://www.weeklystandard.com/blogs/house-intel-chair-snowden-leaks-tipped-al-qaeda_765838.html (accessed 6.28.15).

Kant, I., 1917. Perpetual Peace. London: George Allen. Accessed online http://lf-oll.s3.amazonaws.com/titles/357/0075_Bk.pdf (accessed 4.5.15).

Kohn, S.M., 2011. The Whistle-Blowers of 1777. The New York Times.

http://www.nytimes.com/2011/06/13/opinion/13kohn.html?_r=0 (accessed 7.26.15).

Knaus, Ch., Inman, M., 2015. A junior Defence staffer allegedly took home an intelligence report and posted it online. Canberra Times. URL http://www.canberratimes.com.au/act-news/a-junior-defence-staffer-allegedly-took-home-an-intelligence-report-and-posted-it-online-20150804-gir4rq.html (accessed 8.9.15).

Fuller, N., 2013. Reaction to WikiLeaks: no sources killed due to war log releases: trial report, day 24. Chelsea Manning Support Network. http://chelseamanning.org/news/reaction-to-wikileaks-releases-no-sources-killed-due-to-war-log-releases-trial-report-day-24 (accessed 6.21.15).

Franceschi-Bicchierai, L., 2015. FBI Director: Encryption Will Lead to a "Very Dark Place". Mashable. URL http://mashable.com/2014/10/16/fbi-director-encryption-going-dark-speech/ (accessed 8.6.15).

Leigh, D., 2010. WikiLeaks "has blood on its hands" over Afghan war logs, claim US officials. The Guardian. http://www.theguardian.com/world/2010/jul/30/us-military-wikileaks-afghanistan-war-logs (accessed 7.26.15).

Levine, A., 2010. Gates: Leaked documents don't reveal key intel, but risks remain - CNN.com. URL http://edition.cnn.com/2010/US/10/16/wikileaks.assessment/ (accessed 9.11.15).

Lewis, N.A., 2006. Source of C.I.A. Leak Said to Admit Role. The New York Times. http://www.nytimes.com/2006/08/30/washington/30armitage.html?_r=0 (accessed 7.26.15).

Mabon, S., 2013. Aiding Revolution? Wikileaks, communication and the "Arab Spring" in Egypt. Third World Quarterly 34, 1843–1857. doi:10.1080/01436597.2013.851901

MacAskill, E., 2010. Julian Assange like a hi-tech terrorist, says Joe Biden. the Guardian. URL http://www.theguardian.com/media/2010/dec/19/assange-high-tech-terrorist-biden (accessed 6.4.15).

Marcin, T., 2015. New Whistleblower Rule Issued 2 Years After Snowden Disclosures: Protections For Future Whistleblowing May Be Limited. International Business Times. URL http://www.ibtimes.com/new-whistleblower-rule-issued-2-years-after-snowden-disclosures-protections-future-1959151 (accessed 7.26.15).

Main, L., 2015. "Corrupt and incompetent": Ex-guard details allegations against Nauru security provider. ABC News. URL http://www.abc.net.au/news/2015-06-04/nauru-whistleblower-details-allegations-against-wilson-security/6478492 (accessed 8.1.15).

Martin, S., 2015. Journalist jail threat in metadata law. The Australian. URL http://www.theaustralian.com.au/business/media/journalist-jail-threat-in-metadata-law/story-e6frg996-1227270296737 (accessed 9.5.15).

Markham, C.J., 2014. Punishing the Publishing of Classified Materials: The Espionage Act and Wikileaks. B.U. Pub. Int. L.J. 23, 1.

Martin, A.J., 2015. Snowden tells tech bigwigs: It's up to you to thwart mass surveillance. URL http://www.theregister.co.uk/2015/03/16/snowden_thwarting_mass_surveillance_falls_to_service_providers/ (accessed 6.13.15).

Martinez, M., 2010. Poll: Almost half of Britons feel WikiLeaks sex charges are "excuse". URL http://edition.cnn.com/2010/WORLD/europe/12/13/uk.poll.wikileaks/ (accessed 7.26.15).

Mason, J., 2014. Obama takes swipe at Snowden in spy reform speech. Reuters. http://www.reuters.com/article/2014/01/17/us-usa-security-obama-snowden-idUSBREA0G1DW20140117 (accessed 7.26.15).

McCraw, D., Gikow, S., 2013. End to an Unspoken Bargain: National Security and Leaks in a Post-Pentagon Papers World, The. Harv. C.R.-C.L. L. Rev. 48, 473.

Moller, F., 2007. Photographic Interventions in Post-9/11 Security Policy. Security Dialogue 38, 179–196.

Moreau, R., 2010. Taliban Seeks Vengeance in Wake of WikiLeaks. Newsweek. URL http://www.newsweek.com/taliban-seeks-vengeance-wake-wikileaks-71659 (accessed 8.29.15).

Morris, B., 2015. Simply Transcribed: Quotations from Fausto Cercignani. (ebook) www.lulu.com

Lee, N., 2014. Facebook nation: total information awareness. Springer, New York.

Novak, R.D., 2003. Mission To Niger. The Washington Post. http://www.washingtonpost.com/wp-dyn/content/article/2005/10/20/AR2005102000874.html (accessed 7.26.15).

Page, M., Spence, J.E., 2011. Open Secrets Questionably Arrived At: The Impact of Wikileaks on Diplomacy. Defence Studies 11, 234–243. doi:10.1080/14702436.2011.590046

Perlroth, N., 2015. Security Experts Oppose Government Access to Encrypted Communication. The New York Times. http://www.nytimes.com/2015/07/08/technology/code-specialists-oppose-us-and-british-government-access-to-encrypted-communication.html (accessed 7.26.15).

Pew Research:A, 2014 Obama's NSA Speech Has Little Impact on Skeptical Public. Pew Research Center for the People and the Press. http://www.people-press.org/2014/01/20/obamas-nsa-speech-has-little-impact-on-skeptical-public/ (accessed 9.5.15).

Pew Research:B, 2014 Global Opposition to U.S. Surveillance and Drones, but Limited Harm to America's Image http://www.pewglobal.org/files/2014/07/2014-07-14-Balance-of-Power.pdf (accessed 9.5.15).

Pew Research, 2010. Most Say WikiLeaks Release Harms Public Interest. Pew Research Center for the People and the Press. http://www.people-press.org/2010/12/08/most-say-wikileaks-release-harms-public-interest/ (accessed 9.5.15).

Pew Research , 2008. Public Attitudes Toward the War in Iraq: 2003-2008. Pew Research Center. (accessed 9.5.15).

Pincus, W., 2006. Prosecution of Journalists Is Possible in NSA Leaks. The Washington Post. http://www.washingtonpost.com/wp-dyn/content/article/2006/05/21/AR2006052100348.html (accessed 7.26.15).

Pilkington, E., 2013. Bradley Manning verdict: cleared of "aiding the enemy" but guilty of other charges. The Guardian. http://www.theguardian.com/world/2013/jul/30/bradley-manning-wikileaks-judge-verdict

Powles, J., 2015. France and the UK are on the edge of Kafkaesque surveillance. The Guardian. http://www.theguardian.com/technology/2015/jul/28/surveillance-law-france-uk-kafka (accessed 6.21.15).

Pozen, D.E., 2013. The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information. URL http://harvardlawreview.org/2013/12/the-leaky-leviathan-why-the-government-condemns-and-condones-unlawful-disclosures-of-information/ (accessed 6.3.15).

Ramstack, T., 2013. Manning's WikiLeaks breach helped al Qaeda recruiting: witness. Reuters India. URL http://in.reuters.com/article/2013/08/12/usa-wikileaks-manning-idINDEE97B0FR20130812 (accessed 8.29.15).

Ramussen 2013 52% View WikiLeaks Suspect Bradley Manning As A Traitor http://www.rasmussenreports.com/public_content/politics/general_politics/june_2013/52_view_wikileaks_suspect_bradley_manning_as_a_traitor (accessed 6.21.15).

Reifler, J., Klarevas, L., Gelpi, C., 2006. Casualties, Polls, and the Iraq War. International Security 31, 186–198.

Risen, J., Lichtblau, E., 2005. Bush Lets U.S. Spy on Callers Without Courts. The New York Times. http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html (accessed 9.5.15).

Risen, T., 2014. Pentagon Report Says Snowden's NSA Leaks Risk Lives. US News & World Report. URL http://www.usnews.com/news/articles/2014/01/09/pentagon-report-says-snowdens-nsa-leaks-risk-lives (accessed 9.5.15).

Risen, J., Lichtblau, E., 2005. Bush Lets U.S. Spy on Callers Without Courts. The New York Times.
http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html?_r=0 (Accessed 6/27/15).

Rottman, G., 2014. On Leak Prosecutions, Obama Takes it to 11. (Or Should We Say 526?). American Civil Liberties Union. URL https://www.aclu.org/blog/leak-prosecutions-obama-takes-it-11-or-should-we-say-526 (accessed 6.21.15).

Roller, E., 2014 Hillary Clinton: Edward Snowden's Leaks Helped Terrorists. www.nationaljournal.com. URL http://www.nationaljournal.com/defense/hillary-clinton-edward-snowden-s-leaks-helped-terrorists-20140425 (accessed 6.28.15).

Rosenbaum, D.E., 2005. Bush Account of a Leak's Impact Has Support. The New York Times. http://www.nytimes.com/2005/12/20/politics/bush-account-of-a-leaks-impact-has-support.html (accessed 7.26.15).

Rourke, F.E., 1957. Secrecy in American Bureaucracy. Political Science Quarterly 72, 540. doi:10.2307/2146193

Rudenstine, D., 1996. The day the presses stopped: a history of the Pentagon papers case. University of California Press, Berkeley, Calif.

Savage, C., 2011. No Prosecution Seen for Official in N.S.A. Leak. The New York Times.
http://www.nytimes.com/2011/04/27/us/27nsa.html (accessed 9.5.15).

Schmitt, E., Schmidt, M.S., 2013. Qaeda Plot Leak Has Undermined U.S. Intelligence. The New York Times. http://www.nytimes.com/2013/09/30/us/qaeda-plot-leak-has-undermined-us-intelligence.html?_r=0 (accessed 6.28.15).

Select Committee on Public Interest Whistleblowing, In the Public Interest, Senate, Canberra, 1994,
pp. 7–12. http://www.aph.gov.au/binaries/library/pubs/rn/2004-05/05rn31.pdf (accessed 7.26.15).

Schoenfeld, G., 2011. Necessary secrets: national security, the media, and the rule of law. W. W. Norton & Co., New York.

Scarborough, R., 2014. Islamic State using Edward Snowden leaks to evade U.S. intelligence: NSA official. The Washington Times. URL http://www.washingtontimes.com/news/2014/sep/4/islamic-state-using-edward-snowden-leaks-to-evade-/ (accessed 8.9.15).

Sheridan, M.B., 2010. Hillary Clinton: Wikileaks release an "attack on international community." The Washington Post. http://www.washingtonpost.com/wp-dyn/content/article/2010/11/29/AR2010112903231.html (accessed 6.21.15).

Simmel, G., 1906. The Sociology of Secrecy and of Secret Societies. American Journal of Sociology 11, 441. doi:10.1086/211418

Somaiya, R., 2010. Wikileaks Mirror Sites Appear by the Hundreds. The New York Times. http://www.nytimes.com/2010/12/06/world/europe/06wiki.html?_r=0 (accessed 6.21.15).

Spiegel Staff. 2010. The Wikileaks Iraq War Logs: Greatest Data Leak in US Military History. Spiegel Online. http://www.spiegel.de/international/world/the-wikileaks-iraq-war-logs-greatest-data-leak-in-us-military-history-a-724845.html (accessed 6.28.15).

Stengel, R., 2010. TIME's Julian Assange Interview: Full Transcript/Audio. Time. http://content.time.com/time/world/article/0,8599,2034040-1,00.html (accessed 4.5.15).

Stewart, S., 2010. Wikileaks and the Culture of Classification. Stratfor. URL https://www.stratfor.com/weekly/20101027_wikileaks_and_culture_classification (accessed 9.5.15).

Ted Talks, 2014. Here's How we Take back the Internet. Ted Talks. http://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet?language=en (accessed 9.5.15).

Terrill, G., 2000. Secrecy and openness: the federal government from Menzies to Whitlam and beyond. Melbourne University Press, Carlton South, Vic.

Theoharis, A.G. (Ed.), 1998. A culture of secrecy: the government versus the people's right to know. University Press of Kansas, Lawrence, Kan.

United States Court of Appeal, 2015. ACLU –v- Clapper http://pdfserver.amlaw.com/nlj/NSA_ca2_20150507.pdf (accessed 8.29.15).

Vincent, J., 2014. Google to encrypt searches globally in reaction to Edward Snowden revelations. The Independent. URL http://www.independent.co.uk/life-style/gadgets-and-tech/google-to-encrypt-searches-globally-in-reaction-to-edward-snowden-revelations-9192402.html (accessed 8.16.15).

Vinten, G. (Ed.), 1994. Whistleblowing: subversion or corporate citizenship? Paul Chapman, London.

Vuori, J.A., 2010. A Timely Prophet? The Doomsday Clock as a Visualization of Securitization Moves with a Global Referent Object. Security Dialogue 41, 255–277.

Washington times, 2005. Times faulted by 9/11panel . The Washingtion Times. URL http://www.washingtontimes.com/news/2005/dec/21/20051221-121117-9232r/ (accessed 8.29.15).

Williams, M.C., 2003. Words, Images, Enemies: Securitization and International Politics. International Studies Quarterly 47, 511.

Williams, M.C., 2015. Securitization as political theory: The politics of the extraordinary. International Relations 29, 114–120. doi:10.1177/0047117814526606c

Wilson, J.C., 2003. What I Didn't Find in Africa. The New York Times. http://www.nytimes.com/2003/07/06/opinion/what-i-didn-t-find-in-africa.html (accessed 8.29.15).

Woolf, N., 2015. Tech industry groups urge US to avoid policies that would weaken encryption. The Guardian. http://www.theguardian.com/technology/2015/jun/09/tech-industry-groups-obama-policies-encryption (accessed 9.5.15).

Wroe, D., 2014. Tougher ASIO laws could jail journalists for revealing operations. The Sydney Morning Herald. URL http://www.smh.com.au/national/tougher-asio-laws-could-jail-journalists-for-revealing-operations-20140926-10mrg1.html (accessed 8.16.15).

Ybarra, M., 2015. James Comey, FBI director: Encryption technology fosters furtive terrorist talks. The Washington Times. URL http://www.washingtontimes.com/news/2015/jul/7/fbi-encryption-fosters-furtive-terrorism/ (accessed 8.6.15).