Secrecy and Society

ISSN: 2377-6188

Volume 2
Number 2 *Teaching Secrecy*

Article 6

January 2021

The Rhetorical Devices of the Keepers of State Secrets

Stephane Lefebvre
Independent Researcher, stephane.lefebvre@rogers.com

The Rhetorical Devices of the Keepers of State Secrets

Abstract

This article examines a set of rhetorical devices forming a linguistic practice that are used repeatedly by secret keepers in the United States and the United Kingdom when legally and popularly arguing against the disclosure of state secrets. Each of these devices (using lists, using the future conditional, arguing from ignorance and authority, arguing from consequences, and arguing by analogy) play a role in shaping our social understanding of state secrecy. More importantly, these devices provide secret keepers a means by which to assert their knowledge and expertise, and to legitimize, if judges agree with them, the nondisclosure of state secrets. Once they have been created and have become commonly known to secret keepers, and validated by the judiciary through court precedents, they can be reproduced and passed on from a generation to the next. This article documents the use of these devices and their interrelationships.

Keywords

analogy, arguments, consequences, discourse, harm, ignorance, knowledge, listing, rhetorical devices, secrecy, state secrets, temporality

Cover Page Footnote

The author wish to express his appreciation for the thoughtful and useful comments and suggestions made by the three peer-reviewers.

The Rhetorical Devices of the Keepers of State Secrets

Stéphane Lefebvre[1]

Abstract
This article examines a set of rhetorical devices forming a linguistic practice that are used repeatedly by secret keepers in the United States and the United Kingdom when legally and popularly arguing against the disclosure of state secrets. Each of these devices (using lists, using the future conditional, arguing from ignorance and authority, arguing from consequences, and arguing by analogy) play a role in shaping our social understanding of state secrecy. More importantly, these devices provide secret keepers a means by which to assert their knowledge and expertise, and to legitimize, if judges agree with them, the nondisclosure of state secrets. Once they have been created and have become commonly known to secret keepers, and validated by the judiciary through court precedents, they can be reproduced and passed on from a generation to the next. This article documents the use of these devices and their interrelationships.

Keywords
analogy, arguments, consequences, discourse, harm, ignorance, knowledge, listing, rhetorical devices, secrecy, state secrets, temporality

"You can't handle the truth! . . .
You have the luxury of not knowing what I know! . . .
My existence, while grotesque and
incomprehensible to you, saves lives!"

Colonel Nathan R. Jessup (Jack Nicholson) in the movie *A Few Good Men.*[i]

1 Independent Researcher, Ottawa, Canada. Stéphane Lefebvre previously spent over 20 years working in various intelligence and research-related positions in Canada's federal government. He has published extensively in the fields of intelligence studies and Slavic military studies. His latest work on state secrecy was published in 2018 and 2019: "Why Are State Secrets Protected from Disclosure? The Discourse of Secret Keepers," *The International Journal of Intelligence, Security, and Public Affairs* 20 (2018): 204-229 and "What Do Judges Say on the Protection of Intelligence Secrets?" *Intelligence and National Security* 34 (2019): 62-77. The views expressed herein are his own and do not reflect the official position of any of the government of Canada departments or agencies he has worked for.

This article examines a set of rhetorical devices used by American and British secret keepers to legally and popularly argue against the disclosure of state secrets. Here, I use the terms "secret keepers" to refer to state officials who are formally entrusted with classified information and legally bound to prevent their unauthorized disclosures, and "state secrets" to refer to information that is classified by the state's classifying authorities.[ii] Secrecy, of course, concerns the concealment of information and material the contents or substance of which would cause harm if revealed to anyone not entrusted with their safekeeping.[iii]

The devices under review - the use of lists, temporal expressions, arguing from ignorance and authority, consequences, and analogy - collectively play a role in shaping our social understanding of state secrecy.[iv] Secret keepers use these devices as a linguistic practice to appeal to logic and rationality, emotion, ethics (in the sense of establishing credibility in the eyes of one's audience), and time in order to convince their audiences, judges, and the public that they are correct in opposing the disclosure of state secrets.[v] Rhetorical devices are validated by judicial decisions and precedents so they can be reproduced and passed on from one generation of secret keepers to the next.[vi] As key components of the secret keepers' discourse on state secrecy, they help present a reality that is expressed through usage regularities.

Taken together as a linguistic practice producing authoritative meaning, rhetorical devices, as the samples I selected for this article show, have by design a *truth production* component about the effects of disclosing state secrets and a *prescriptive* component about what to do with them. They are also not easily disentangled. Too often, two or more devices are used together in the same utterance as a coherent construct. Looking at them individually should help readers to better understand how the practice works.

Up to this point, the literature on secrecy has shown that secrecy in all its forms is pervasive in society and constitutive of the material nature of state power. In a post-9/11 context, claims of state secrecy have been increasingly normalized, and its breaches have produced a large amount of research material. The claims that the state make to justify the non-disclosure of state secrets and punish those who disclose them are generally accepted by most scholars and other observers as essential to the proper functioning of democracies. As such, there is agreement with the secret keepers of the state that a certain amount of secrecy can be justified; where that threshold is, of course, is subject to intense debates in both the literature and the courts. Yet, the sets of reasons or rationalities that secret keepers use to justify the non-disclosure of state secrets remains understudied, especially where it matters most: the legal environment. It is a prime site for such an investigation and what follows because it is there that these reasons are best articulated, especially in opinions (United States)

and judgments (United Kingdom). I supplement this large collection of legal texts with other genres such as the media, memoirs, and official documents because together that they reveal "recurrent linguistic behaviour."[vii] Without knowing how state secrecy claims are justified through discourse, no counter discourse can be properly articulated and deployed.

This article thus makes two contributions to the literature. First, it offers a novel way to understand the reasons offered by secret keepers to prevent the disclosure of state secrets. By focusing on how secret keepers use particular rhetorical devices as forms of persuasion, it highlights the social nature of secrecy, and offers one explanation of the workings of state secrecy with respect to a disciplinary field that, in the words of Urban, "has remained disappointingly general, universalistic, and largely divorced from social and historical context."[viii] As "practices of classification powerfully shape the boundaries of public knowledge," critical attention to the production and reproduction of state secrecy is, I would suggest, warranted.[ix] Second, it contributes to the study of discourse by characterizing the use of rhetorical devices by particular agents (secret keepers) in relation to a particular discourse (state secrecy) in both a primary site (law) and genre (legal documents). In doing so, it lays out the groundwork for the view that the ubiquity of rhetorical devices are useful to secret keepers in persuading others to make sense of the social world of state secrecy the same way they do.

Using Lists

Listing is an ancient linguistic expression.[x] By omitting distracting details, and by bringing together a set of reasons that justifies the nondisclosure of state secrets, lists provide a way to describe a particular aspect of the social world of state secrecy.[xi] The lists developed by secret keepers conform to the defining characters of lists that Jayyusi lays out in *Categorization and the Moral Order*.[xii] First, the items have a relationship to each other; that is, they are all reasons used to justify the nondisclosure of state secrets. Second, the lists have a purpose, which is instrumental as they are meant to persuade judges and the public that secret keepers are justified in safeguarding state secrets from disclosure. Third, the reasons listed are not totally interchangeable for other purposes; they can be differentiated for the purpose of protecting state secrets. Finally, the lists are adequate in the sense that they meet the stated purpose of their existence, which is to prevent the disclosure of state secrets.

The reasons stated on the lists were selected by state officials to be seen as standing together, and as such, there is a high degree of consistency across lists. Read together, these reasons give the impression of totality (what else could go wrong, one would ask?) and of a complexity that would be difficult to reduce to simple and direct cause-to-effect relationships because the possibilities that harm would follow the disclosure of state secrets are essentially limitless.[xiii]

The lists differ slightly from country to country, as one would reasonably expect, but resemble one another in scope and possibilities of harm. They regularly make reference to sets of reasons that include: the need to protect the identity of intelligence personnel and human sources, the need to protect methods by which state secrets were obtained, the need to protect intelligence relationships with foreign entities, the need to protect the effectiveness of security agencies, and the need to protect seemingly innocuous information from negative exploitation by adversaries of the state such as spies, terrorists, or criminals.

Here are three examples of such lists, one from the United States and two from the United Kingdom[xiv]:

Example 1. A lawyer who worked for the George W. Bush administration provided this list in testimony before the US Congress:

> Leaks of national security information can compromise all aspects of our national security program. They can compromise specific national security operations, as happened in 2006 with the disclosure of the Treasury Department's secret program for tracking terrorist finances. They can compromise human sources, as apparently happened when it was recently reported that a Saudi source had helped to foil al Qaeda's recent airplane bombing plot. And keep in mind that whenever a source's identity or existence is leaked, it not only negates the effectiveness of that particular source, it also undermines our ability to develop and cultivate sources in the future.
>
> Leaks can also compromise our methods, as apparently happened with the recent disclosure of our alleged use of malware to attack the Iranian nuclear weapons program. They can certainly endanger our government personnel, like the CIA chief of station who was publicly outed and then killed by terrorists in Athens in the 1970's [sic]. And, importantly, they can weaken our alliances, those operational relationships

> between us and foreign services that are so vital to our national security operations around the world.
>
> Finally, it's worth noting that government employees with clearances give a personal promise that they will protect the government's classified information. The integrity of public service is diminished whenever that promise is broken. [xv]

Example 2. In the context of inquest proceedings during which a coroner asked for evidence in the hands of the Security Service (MI5) and the Secret Intelligence Service (MI6), the Secretary of State signed a Public Interest Immunity (PII) certificate in which she listed the following reasons against disclosure:

> 10. The reason why disclosure of the documents in Bundle A would bring about a real risk as described is that those documents include national security information of one or more of the following kinds:
>
> a) information relating to operations and capabilities of the security forces, law enforcement agencies and security and intelligence agencies, disclosure of which would reduce or risk reducing the effectiveness of those operations or of other operations either current or future;
>
> b) information relating to the identity, appearance, deployment or training of current and former members of the security forces, law enforcement agencies and security and intelligence agencies, disclosure of which would endanger or risk endangering them or other individuals or would impair or risk impairing their ability to operate effectively or their ability to recruit and retain staff in the future;
>
> c) information received in confidence by the security forces, law enforcement agencies and security and intelligence agencies from foreign liaison sources, disclosure of which would jeopardise or risk jeopardising the provision of such information in the future;
>
> d) other information likely to be of use to those of interest to the security forces, law enforcement agencies and security and intelligence agencies in pursuit of their functions, including

> terrorists and other criminals, disclosure of which would impair or risk impairing the security forces, laws enforcement agencies and security and intelligence agencies in their performance of their functions.
>
> 11. It is not possible for me to be more specific in this certificate about the particular information in Bundle A, or the precise harm that its disclosure risks causing, since my doing so would be liable to risk causing the very damage that the certificate seeks to avoid.[xvi]

Example 3. This list was included in a certificate to the court by the Secretary of State:

> 4.1. Secrecy is essential to the work of the Security Service. Many individuals who cooperate with the Service - such as agents - only do so under guarantee of complete confidentiality and anonymity. If their identity became known not only would it jeopardise the work in hand and their future co-operation but also it would put them at personal risk. Such a risk is not fanciful, as a large part of the Security Service's work comprises the investigation of terrorists. Clearly, the same risks apply to members of the Security Service itself.
>
> 4.2. Secrecy is also essential because the Security Service undertakes investigations covertly. The Service's effectiveness lies in its ability to obtain and exploit secret intelligence, which those under investigation may go to some lengths to keep hidden. As well as the use of agents mentioned above, sources of secret intelligence include: a. the interception of communications, b. eavesdropping, and c. surveillance. Clearly, such techniques lose much if not all of their effectiveness if it is known when and how they are used.[xvii]

In each of these examples, it would very difficult for anyone to thoroughly assess the validity of the claims put forward due to their lack of specificity.[xviii] Ultimately, these lists tell us little. They simply state the types of disclosure that, in the view of secret keepers, would be injurious to national security. They do not explain, beyond generalities, why the release of a particular kind of secrets would be injurious in a particular case; that is,

readers must assume a cause-to-effect relationship that is not directly demonstrated.

These lists are characterized by their use of plain English, including the absence of multiple negatives and complex legal terminology, and abundantly use conditional terms such as if and would, and verbs associated with harm, such as jeopardize, endanger, risk, weaken, lose, and compromise. The order by which the reasons are listed is not important, as each reason can find itself just about anywhere on a list. But as they stand together, they exhibit cumulativity, display a sense of finality, and completeness. To anyone unfamiliar with the social world of state secrecy, the effect of listing may be overwhelming: how could so many reasons be rebutted? With so much harm at stake, are these reasons not only necessary but sufficient? If harm can and would result from the disclosures of state secrets that should remain undisclosed, is mitigation even possible? The significant and overwhelming use of anticipated future harm in these lists is directly interrelated to the temporality aspect brought to the fore by secret keepers, which I now turn to.

Using the Future Conditional[xix]

Secret keepers, grounded in human existence, are clearly conscious of time and its implications.[xx] In arguing for the protection of secrets, they offer a particular sense of time that frames our understanding of the anticipated effects of disclosures.[xxi] These effects are based on past experiences that are known to secret keepers, and "used to explain

(foresee) the future," a future that has no delimitations, which is built out of instances of anticipation.[xxii] These instances are also the product of their behavior in their daily lives, what they take for granted, the routines they follow without thinking about them, and the common sense knowledge they use in protecting state secrets from disclosure.[xxiii] Secret keepers acquire this habitus through socialization, or social conditioning, and reproduce it throughout their careers.[xxiv] As Hoy notes, "[t]he bodily habitus incorporates dispositions that are then projected as expectations for the future."[xxv]

The use of the future conditional by secret keepers is eschatological.[xxvi] Harm could happen tomorrow, a long time from now, and mitigation is assumed to be impossible. Secret keepers do not differentiate with respect to when or where the harm resulting from the disclosure of state secrets they believe should remain undisclosed could occur.[xxvii] But by generally invoking an indefinite dimension of time, secret keepers exclude other "equally plausible understandings of temporality"[xxviii] such as the notion that "secrecy does not necessarily need to persist for lengthy periods of time and certainly not in perpetuity."[xxix]

The form the device takes is classic: if P [the release of state secrets], then Q [harm will ensue], which in turn implies that if not-P, then not-Q, embedded in subjunctive conditional sentences with the consequent having "would" or "could" as its principal operator.[xxx] As we will see in the next section, the grounds for accepting these conditionals lie in the experience and expertise of the secret keepers.

In addition to the temporal effect explicit in the lists established by secret keepers, a similar temporal effect can be seen in arguments made by secret keepers to protect very specific information from disclosure. This includes information pertaining to the identity of human sources providing information to the state, the identity of certain state officials, the identity of individuals under investigation, the sources and methods used by security agencies to gather intelligence or conduct particular activities, reports produced from the intelligence collected, and the existence, nature,and extent of intelligence liaison relationships with partner countries. The first, lengthy, example is typical of those found in US affidavits submitted to the courts.[xxxi]

In a lawsuit launched against Ishmael Jones (a pen name), the author of *The Human Factor: Inside the CIA's Dysfunctional Intelligence Culture*, CIA presented commonly used reasons for keeping his identity, and by extension, of any other CIA officers, a state secret. First, the CIA argued that if the identity of its officers were known, they would not be able "to effectively and securely collect foreign intelligence and conduct clandestine foreign intelligence activities around the world […]."[xxxii] Second, CIA emphasized that if the identity of its officers were known, "foreign governments, enterprising journalists, and amateur spy-hunters would be able to reconstruct" their travels and where they lived, possibly causing anger, embarrassment, or hostility against the United States in other countries. Actions these countries could take include "limiting joint

endeavors, reducing intelligence sharing, deferring negotiations on matters of importance to the United States, or demanding that CIA officers known or declared to the foreign government leave the country.[xxxiii] Third, by knowing the identity of CIA officers as well as where and when they lived abroad, other countries "foreign governments; enterprising journalists, and amateur spy-hunters would be able to unearth and publicly disclose the cover methods," CIA officers used to conceal their true status as CIA officer, and in so doing prevent the CIA from using these methods in future and putting publicly unknown officers operating undercover at risk of discovery.[xxxiv]

These shorter US-focused examples further illustrate how temporality is typically articulated:

Example 1: "Exposing a covert officer's ties to the CIA could jeopardize the physical safety of past, present, and prospective human sources."[xxxv]

Example 2: "[…] if the CIA released the information related to foreign governments, those government may be less willing and able to assist the CIA in the future - and the CIA's breach of trust may affect the willingness of potential future sources or entities to assist the CIA. Additionally, if the CIA disclosed particular activities, sources, or methods, they would become less effective and their continued use by the CIA would be jeopardized."[xxxvi]

Example 3: "This information would tend to reveal, among other things, whether or not the CIA has been granted the authority to engage in drone strikes, what role the Agency plays (if any) in the execution of drone strikes - especially in comparison to other agencies, and/or the amount of

resources it devotes to this area. The unauthorized disclosure of this information reasonably could be expected to harm the national security of the United States […]."[xxxvii]

Example 4: "Moreover, courts give the utmost deference to the Executive Branch's 'predictive judgment' in evaluating both the risk that disclosure might pose to national security and the 'acceptable margin of error in assessing' that risk because of the Executive's superior position to make such determinations."[xxxviii]

In the United Kingdom, similar arguments are encountered. For example, a former British Intelligence & Security Coordinator spoke in no uncertain terms about the future harm to the very existence of intelligence agencies that would result if their secret techniques and sources were disclosed:

> I understand the argument that the reason the Security and Intelligence Agencies are obsessed with secrecy is because they want to avoid accountability. But as former Intelligence & Security Coordinator and Agency Head I know it to be wrong. Intelligence organisations that cannot protect their techniques and sources will not survive for long. Compromise them and they will dry up and we will be less safe.[xxxix]

Secret keepers, of course, usually do not shy away from admitting to the courts that such underspecified and undifferentiated temporal impact is on par with the course: "The articulation of threatened harm in the future always will be somewhat speculative and a showing of actual harm is unnecessary."[xl] In the following example, which dates to the presidency of

John F. Kennedy, future harm is highly speculative due to the age of the documents in question:

> The name of a clandestine human intelligence source classified as secret was withheld from a JFK document. […]. Even today, such a disclosure would provide foreign intelligence services with valuable insights into the CIA's activities, sources, and methods. Moreover, the disclosure of the source's identity also could endanger the source and his or her family and associates and subject them to reprisals, even if the source is deceased. […] With regard to intelligence sources and methods, as was recognized in *Sims*, 471 US at 175, the "forced disclosure [by the courts] of the identities of its intelligence sources could well have a devastating impact on the Agency's ability to carry out its mission."[xli]

Secret keepers certainly know that history is giving them reasons to be worried when the names of intelligence officers and sources are disclosed without authorization, either through leakage or espionage.[xlii] In her testimony before Congress, then CIA case officer Valerie Plame Wilson, whose cover had been blown by a White House staffer and the Deputy Secretary of State, succinctly made reference to that knowledge while stressing the gravity of exposing the identity of undercover CIA officers[xliii]:

> The CIA goes to great lengths to protect all of its employees, providing at significant taxpayers' expense painstakingly devised and creative "covers" for its most sensitive staffers. The harm that is done when a CIA cover is blown is grave but I cannot provide details beyond this in a public hearing. But the concept is obvious. Not only have breaches of national security endangered CIA officers, it has jeopardized and even destroyed entire networks of foreign agents who, in turn risked their own lives and those of their families - to provide the United States with needed intelligence. Lives are literally at stake.[xliv]

Plame's comment on the difficulty of providing concrete examples or details in a public hearing is common in the United States as it is in the

United Kingdom.[xlv] This limits the amount of material available for analysis, but, more importantly, it shapes the discourse of secret keepers in such a way that the harm they argue would ensue in cases of disclosures is framed as speculative, that is, usually weakly supported by facts, and focused instead on potential risks. Hence, "would" and "could" predominate in the language at play. As Tetlock has aptly noted, a term like "could" is ambiguous by definition:

> When you ask research subjects what "could" means, it depends enormously on the context: "we could be struck by an asteroid in the next 25 seconds," which people might interpret as something like a .0000001 probability, or "this really could happen," which people might interpret as a .6 or .7 probability. It depends a lot on the context. Pundits have been able to insulate themselves from accountability for accuracy by relying on vague verbiage. They can often be wrong, but never in error.[xlvi]

The most interesting aspect of the temporal reasoning put forward by secret keepers is the implicit notion that their access to privileged knowledge of what has happened in the past gives them authority and legitimacy in assessing what would likely happen if state secrets are disclosed. In other words, it is from the understanding of their respective domain of knowledge that secret keepers derive their predictions. This is essentially an intertwined argument from both ignorance and authority, to which I now turn.

Arguing from Ignorance and Authority

The argument from ignorance assumes that because we do not know that something is false, then it is true. Secret keepers use this rhetorical device to argue that the disclosure of state secrets would lead to yet

unknown but highly anticipated risks.[xlvii] Their argument conforms to the traditional structure: 1. Secret keepers do not know for sure, and may have no indications whatsoever, that harm would result from the disclosure of state secrets. 2. The consequences of disclosing state secrets, however, could be catastrophic (among the possible harms, lives could be lost). 3. Therefore, secret keepers and judges should not disclose state secrets in order to prevent harm.[xlviii] The effectiveness of this rhetorical device is compounded by the additional argument that, in the absence of convincing evidence, secret keepers are best positioned, given their expertise and experience, their access to secrets and the magnitude of risks, to determine the likelihood of harm resulting from the disclosure of state secrets (an argument from authority).[xlix] The CIA best expressed it in a defense motion: "Only the nation's intelligence community has a complete picture of which disclosures pose a danger to national security."[l] As Hoeken, Timmers and Schellens note, "[t]he argument from authority can support claims about the desirability of a consequence by stating that the claim is in accordance with the opinion of an expert in this field."[li] The reasoning employed by secret keepers is thus one of deductive competence (here an "extra logical factor that modifies the interpretation of premises" 1 to 3).[lii]

These arguments have the effect of closing dialogue and debate as there is no one to seriously engage with.[liii] Often, these arguments are used bluntly. In this British example, the Home Department told the Information Tribunal that "the [Security] Service was best placed, through its experience

and expertise, to make the relevant decisions."[liv] In this civil case example, the CIA argued that the assessment of harm is properly located with the Agency:

> Indeed, given that "the assessment of harm to intelligence sources, methods and operations is entrusted to the Director of Central Intelligence," […] plaintiff cannot credibly purport that his own judgment about the consequences of disclosure in this case is superior to that of Acting DCI [Director of Central Intelligence] McLaughlin.[lv]

This argument has been repeated over and over again, often in the exact same language of superiority. But as the DC Circuit made clear, there is nothing wrong with this practice of using "the same or similar language in different affidavits supporting FOIA [Freedom of Information Act] exemptions" because, "when the potential harm to national security in different cases is the same, it makes sense that the agency's stated reasons for nondisclosure will be the same."[lvi] In its more detailed expression, a US assistant attorney general asserts the argument in the following manner, making ample use of precedents:

> […] judicial deference [to the executive] is rooted in three well-established principles. First, the primacy of the Executive Branch in matters of national security and foreign relations is enshrined in the Constitution and in judicial precedent […]. Accordingly, courts have recognized that the Executive Branch's ability to maintain secrecy is essential. See Curtiss-Wright Export Corp., 299 US at 320. Moreover, the Executive Branch's familiarity with matters of foreign relations and national security means that it has accumulated an expertise on the impact of the disclosure of particular classified information. […].
>
> Second, in contrast to the Executive Branch's experience, courts have recognized that judges are in no position to second-guess the national security and foreign relations concerns articulated by the Executive Branch. […] ("Judges, moreover, lack the

> expertise necessary to second-guess such agency opinions in the typical national security FOIA case."; […]
>
> Third, judicial deference to executive classification decisions is especially important because of the severity of the consequences that may result from the disclosure of classified information. "It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation." […].[lvii]

The following, shorter and US-focused, examples similarly embrace the argument from ignorance and the argument from authority:

Example 1: "Courts normally will defer to the expert opinion of the agency, because Courts 'lack the expertise necessary to second-guess such agency opinions in the typical national security FOIA case.' […]."[lviii]

Example 2: "[…] it is important to note that the information sought by Plaintiffs directly 'implicat[es] national security, a uniquely executive purview.' […] courts […] defer to an agency's determination in the national security context, acknowledging that 'the executive ha[s] unique insights into what adverse affects might occur as a result of public disclosure of a particular classified record.' […]. Courts have specifically recognized the 'propriety of deference to the executive in the context of FOIA claims which implicate national security'."[lix]

Example 3: "It is well-established that the Judiciary gives the utmost deference to the Executive Branch's classification decisions, including the Executive's assessment of the national security risk of disclosing classified information."[lx]

Example 4: "Indeed, the Supreme Court has cautioned that 'weigh[ing] the variety of complex and subtle factors in determining whether

disclosure of information may lead to an unacceptable risk of compromising' national security is a task best left to the Executive Branch. […]('[T]he judiciary is in an extremely poor position to second-guess the executive's judgment in [the] area of national security.'); […] ('Judges * * * lack the expertise necessary to second-guess * * * agency opinions in the typical national security FOIA case.')."[lxi]

Example 5: "Recognizing that national security is a uniquely executive purview, courts typically defer to such an agency determination. […]. ('Few judges have the skill or experience to weigh the repercussions of disclosure of intelligence information.'); […] ('Judges . . . lack the expertise necessary to second-guess [] agency opinions in the typical national security FOIA case'). Thus, the Court should defer here to Mr. Bradley's and Ms. Janosek's assessments of the likely repercussions to the national security from disclosure of the information withheld pursuant to exemption (b)(1)."[lxii]

Examples of the use of the argument from ignorance and the argument from authority abounds in US legal documents prepared by secret keepers (affidavits) and their government attorneys (motions, etc.). While less frequent, it also appears in other jurisdictions. Counsels for the executive in the United Kingdom's have used the argument as effectively. One notable example has seen the counsel for the Secretary of State for the Home Department arguing to the presiding judge, using precedents just like his counterparts do in the United States, that the executive was, because of its experience and expertise,[lxiii]

> in the best position to judge what national security requires, and the correct approach in law is to entrust decision of this sort to them: Rehman v SSHD [2001] 3 WLR 877. Mr Tam also referred to us the decision of Mr Justice David in Ewing (20 December 2002 unreported).[lxiv]

Secret keepers have extended the argument of ignorance and the argument from authority to actors beyond the judiciary. Former British Foreign Secretary Jack Straw, for example, accused the *Guardian* newspaper of showing "extraordinary naivety and arrogance" for publishing intelligence documents leaked by Edward Snowden, a former US National Security Agency contractor. He told the BBC:

> They're blinding themselves about the consequence and also showing an extraordinary naivety and arrogance in implying that they are in a position to judge whether or not particular secrets which they have published are not likely to damage the national interest, and they're not in any position at all to do that.[lxv]

Snowden, a former secret keeper, has also been criticized for not having the knowledge and expertise to make the decision to leak classified documents. His Booz Allen Hamilton supervisor at the National Security Agency in Hawaii made that argument:

> He never actually had access to any of that data. All of the domestic-collection stuff that he revealed, he never had access to that. So he didn't understand the oversight and compliance, he didn't understand the rules for handling it, and he didn't understand the processing of it... In my mind Ed's not a hero.[lxvi]

The argument from ignorance and the argument from authority are compelling, especially when secret keepers can show it has legitimacy through judicial precedents. It is also compelling because they are framed around the notion of national security, which unarguably is a duty of the

executive; governments regularly assert in courts that their first duty is to protect the security of their citizens from foreign and domestic threats.

Arguing from Consequences

Arguing from consequences is a common form of argumentation drawing on causal reasoning. It requires that allegedly foreseeable consequences be cited in response to a proposed action, which would determine whether it is pursued or not. These consequences can of course either be positive or negative.[lxvii] When arguing from consequences, secret keepers stress negative consequences using a language of fear to illustrate the harm the disclosure of state secrets would cause. In doing so, they seek the arousal of emotions that would rally their listeners to their point of view by fostering empathy for potential victims of harm.[lxviii] Secret keepers take it as evident that harm would ensue if state secrets were disclosed. In making this assertion, they portray a belief that no one would be so insensitive to the possibility of a fellow human being seriously harmed to support the release of state secrets. As it happens, there is scientific support behind that belief:

> results from studies within persuasion research suggest that people are more sensitive to differences in desirability [such as that no one be harmed from the disclosure of state secrets] than to differences in likelihood [that such harm would actually occur].[lxix]

Their argument from consequences has two intertwined prongs. One directly links the protection of state secrets to national security, and the other to matters of life and death. National security is instinctively

understood by most citizens: it is the state that protects them from external and internal threats that could cause them grave harm. So when the state invokes national security on the basis of knowledge that only it possesses, citizens are expected to defer to its authority and sense of duty: after all, it is in their interest to do so if they want to be secure in their person and property.[lxx] By incorporating threats of harm to real individuals or to the effectiveness of national security agencies into their discourse and using value-oriented lexical terms, secret keepers appeal to fear of consequences should these threats materialize, and as such continue to engage in a legitimizing exercise that started on the basis of their competence and authority.[lxxi]

In this section, I present examples in which secret keepers directly link foreseeable consequences to matters of life and death, using their extra-legal reactions to the major leaks of Chelsea Manning and Edward Snowden.[lxxii] I also present examples highlighting the foreseeable consequences of leaking state secrets for the secret keepers themselves, their sources and methods, and for the efficiency of the national security system, and ultimately its ability to keep both secret keepers and citizens safe. There is an obvious overlap between these consequences as they are often used together.

Protecting Lives

Governments traditionally and regularly asserts that their first duty is to protect the security of its citizens from foreign and domestic threats.[lxxiii] Secret keepers take that duty seriously and from time to time have reminded themselves that unauthorized disclosures of state secrets endanger lives. As Richard Moberly noted,

> after the raid that killed Osama bin Laden […in 2011], Leon Panetta, then the Director of the CIA, sent a memo to CIA employees stating, "Disclosure of classified information to anyone not cleared for it—reporters, friends, colleagues in the private sector or other agencies, former Agency officers—does tremendous damage to our work. At worst, leaks endanger lives."[lxxiv] [emphasis added]

Secret keepers have seized the unauthorized disclosures of state secrets by Private Bradley (now Chelsea) Manning and Edward Snowden to highlight the serious harm both have arguably caused to the national security of the United States and to the lives of particular individuals. They characterize Manning's unauthorized disclosures of the Afghan and Iraqi war logs (records of ongoing significant military and insurgent activities) in criminal terms, indeed a monstrous crime committed against the national security of the United States. Given that Manning was formally charged and tried and subsequently convicted, this immediately became a dominant narrative in mainstream media.[lxxv]

When Wikileaks released the Afghan war logs (over 91,000 battlefield reports, most of them secret) in July 2010, the response of the US government highlighted possible losses of lives. White House spokesperson Robert Gibbs said that the release of the logs "has a potential to be very

harmful" to US and allied military forces engaged in the fight in Afghanistan, and that it "poses a very real and potential threat to those that are working hard every day to keep us safe."[lxxvi] Gibbs was supported by Secretary of Defense Robert Gates, who said that Wikileaks was "morally guilty for putting lives at risk."[lxxvii] In a released statement, the Obama administration said that the leaks of the Afghan war logs "could put the lives of Americans and our partners at risk, and threaten our national security."[lxxviii] As the argument went, the leaked documents contained the names of Afghans nationals who had collaborated with the United States.[lxxix] This meant, said Admiral Mike Mullen, the Chairman of the US Joint Chiefs of Staff, that Wikileaks' Julian Assange and his source [Manning] "might already have on their hands the blood of some young [US] soldier or that of an Afghan family."[lxxx] Zahibullah Mujahid, a spokesperson for the Taliban, certainly gave ammunition to Mullen when he was quoted as saying the Taliban were indeed looking at the logs in the search for Afghan informants:

> We knew about the spies and people who collaborate with US forces. We will investigate through our own secret service whether the people mentioned are really spies working for the US If they are US spies, then we know how to punish them.[lxxxi]

Two weeks after the Afghan war logs were released, a Pentagon spokesperson acknowledged that as of that date no one in Afghanistan had been harmed as a direct result of the unauthorized disclosure, but that it could only be a matter of time [a play on temporality] because "there is in all likelihood a lag between exposure of these documents and jeopardy in the field."[lxxxii]

The reactions of secret keepers to the unauthorized leak of the Iraqi war logs (391,832 battlefield reports) in October 2010 were similar to the release of the Afghan war logs a few months earlier. For example, Pentagon spokesman Geoff Morell stressed the illegal aspect of the disclosure and the fact that the logs were now in the hands of America enemies. As the Taliban claimed to have done with the Afghan war logs, Morell pointed out that the Iraq war logs could be mined as well, thus risking the lives of American and allied soldiers deployed in Iraq; "this security breach," he said, "could very well get our troops and those they are fighting with killed."[lxxxiii]

With respect to the 251,287 US State Department diplomatic cables that Manning leaked to Wikileaks, approximately 130,000 were unclassified, 100,000 CONFIDENTIAL, 15,000 SECRET, and none TOP SECRET[lxxxiv;] Manning Harold Koh, the US State Department legal adviser, said to Wikileaks' Julian Assange that his organization obtained the cables illegally and their release "would place at risk the lives of countless individuals" and endanger the ability of the US government to conduct its business in a cooperative manner with other states, including with respect to life and death matters such as terrorism, pandemic diseases and nuclear proliferation.[lxxxv]

The Snowden leaks were of a different kind than Manning's. The documents concerned signals intelligence gathered by the United States National Security Agency (NSA) and allied services for surveillance purposes that Snowden did not agree philosophically with, such as the collection of

metadata on American citizens ostensibly to catch terrorists.[lxxxvi] Most of the leaked documents were of a highly technical nature and difficult for anyone not well versed in intelligence matters to decipher. Because Snowden purported to reveal abuses of authority and highlight issues he believed are matters of general public interest, he received support from an eclectic range of people. Inevitably, secret keepers were Snowden's harshest critics, due to high sensitivity of the documents and classification at the TOP SECRET level. At the time of his leaks, Snowden himself was a secret keeper sworn to uphold his oath of secrecy and loyalty to the United States. He was an insider who, in the eyes of secret keepers, betrayed all. Yet, Snowden had set limits on what he would and would not disclose. He had no intent, for instance, to endanger anyone's life, such as a CIA human asset: "Most of the secrets the CIA has are about people, not machines and systems, so I didn't feel comfortable with disclosures that I thought could endanger anyone."[lxxxvii]

Fully aware as a secret keeper that unauthorized disclosures could cause harm, Snowden was decidedly vocal in expressing concerns for possible harm to others and wanting to avoid any harmful outcomes. Snowden claimed to have vetted every document he leaked to ensure they would not cause harm to national security or any individuals.[lxxxviii] Yet, just like Manning, he was accused of being a source of great harm. Former CIA Director R. James Woolsey, Jr. bluntly repeated to the media that Snowden "has blood on his hands."[lxxxix] However, at no time did Snowden expose the

identity of US intelligence officers operating covertly in violation of the *Intelligence Identities Protection Act*.[xc]

The British government was likewise concerned about the possible consequences of the leaks and went as far as issuing a Defence (D) Advisory Notice (D Notice) to editors, warning them to self-censor their coverage of Snowden's leaks so as not to "jeopardise both national security and possibly UK personnel."[xci] A few weeks later, after David Miranda, an associate and the spouse of *Guardian* journalist Glenn Greenwald who had extensively written on the leaks, was detained while transiting London's Heathrow airport on his way to Brazil from Germany. Home Secretary Theresa May responded to criticism by directly associating the documents leaked by Snowden with possible harm to peoples' lives:

> I think it is right, given that it is the first duty of the government to protect the public, that if the police believe somebody has in their possession highly sensitive stolen information which could help terrorists which could lead to a loss of lives then it is right that the police act. That is what the law enables them to do.[xcii]

May was backed by Scotland Yard, who, after taking a look into the contents of Miranda's computer, that its contents were "highly sensitive," and "could put lives at risk" if made public.[xciii] At a subsequent Divisional Court hearing, Oliver Robbins, UK's Deputy National Security Adviser, stated that Miranda's computer's hard drive had approximately 58,000 highly classified documents, some with information on British intelligence officers; the unauthorized disclosure "would result in a risk to the lives of them and their families and the risk their becoming recruitment targets for terrorists

and hostile spy agencies."[xciv] Nick Clegg, the Deputy Prime Minister, similarly justified the destruction by the Government Communications Headquarters (GCHQ) of the *Guardian* computers containing documents leaked to the newspaper by Snowden:

> I believed at the time, and still do, that it was entirely reasonable for the government to seek to get leaked documents back or have them destroyed. Along with the information the *Guardian* had published, it had information that put national security and lives at risk. It was right for us to want that information destroyed.[xcv]

Snowden's unauthorized disclosures led secret keepers to argue that they could cause harm to the lives of many individuals. The latter fall into two categories: officials formerly or currently employed by intelligence agencies and whose names appear on leaked documents, and the population at large, whose protection is now diminished by terrorists now knowing how to avoid being tracked, monitored and surveilled. John Naughton well captured how the discourse surrounding Snowden's leaks went:

> "Kafkaesque" seems more appropriate to the situation in which we find ourselves. The conversation between the state and the citizen has been reduced [that] goes like this.
> State: Although intrusive surveillance does infringe a few liberties, it's necessary if you are to be protected from terrible things.
> Citizen (anxiously): What terrible things?
> State: Can't tell you, I'm afraid, but believe us they are truly terrible. And, by the way, surveillance has already prevented some terrible things.
> Citizen: Such as?
> State: Sorry, can't go into details about those either.
> Citizen: So how do I know that this surveillance racket isn't just bureaucratic empire building?
> State: You don't need to worry about that because it's all done under legal authority.
> Citizen: So how does that work?

State: Regrettably, we can't go into details because if we did so then the bad guys might get some ideas.[xcvi]

Protecting the Effectiveness of Intelligence Agencies

Protecting the identity of intelligence officers, in particular those deployed abroad for the purpose of gathering intelligence, is of paramount importance to secret keepers. Then President George W. Bush confirmed this assertion in a speech to Central Intelligence Agency (CIA) employees in 1999, stating bluntly that those who leak the identity of intelligence operatives are the "most insidious of traitors."[xcvii] In a lawsuit launched against one of its former employees,[xcviii] the CIA presented commonly used reasons for keeping his identity (and by extension, of any other CIA officers) a state secret. First, it argued that if the identity of its officers were known, they would not be able "to effectively and securely collect foreign intelligence and conduct clandestine foreign intelligence activities around the world [...]."[xcix] Second, it emphasized that if the identity of its officers were known, "foreign governments, enterprising journalists, and amateur spy-hunters would be able to reconstruct" their travels and where they lived, possibly causing anger, embarrassment or hostility against the United States in other countries. Actions these countries could take include "limiting joint endeavors, reducing intelligence sharing, deferring negotiations on matters of importance to the United States, or demanding that CIA officers known or declared to the foreign government leave the country.[c] Third, by knowing the identity of CIA officers as well as where and when they lived abroad,

other countries "foreign governments; enterprising journalists, and amateur spy-hunters would be able to unearth and publicly disclose the cover methods" CIA officers used to conceal their true status as CIA officer, and in so doing prevent the CIA from using these methods in future and putting publicly unknown officers operating undercover at risk of discovery.[ci]

What the CIA described in the Jones' case might actually have happened a few years before, although no firm evidence surfaced publicly. In her testimony before Congress, former CIA case officer Valerie Plame Wilson, whose cover had been blown by a White House staffer I. Lewis Libby and the Deputy Secretary of State,[cii] succinctly made reference to these arguments while stressing the gravity of exposing the identity of undercover CIA officers:

> The CIA goes to great lengths to protect all of its employees, providing at significant taxpayers' expense painstakingly devised and creative 'covers' for its most sensitive staffers. The harm that is done when a CIA cover is blown is grave but I cannot provide details beyond this in a public hearing. But the concept is obvious. Not only have breaches of national security endangered CIA officers, it has jeopardized and even destroyed entire networks of foreign agents who, in turn risked their own lives and those of their families - to provide the United States with needed intelligence. Lives are literally at stake.[ciii]

During the trial for perjury of I. Lewis Libby, CIA officer Craig Schmall testified in a language very similar to that used by Plame. In answering a question from the prosecutor, Schmall said that

> now that Valerie Wilson's name is out in the press, foreign intelligence services in countries where she served now have the opportunity to investigate everyone she came in contact [with] while she was in those countries. And, in many countries, those people, innocent or otherwise, can be harassed along with their

> families. They can lose their jobs. They can be arrested, tortured or killed. So in my mind, it was a very grave danger involved.[civ]

As Plame stressed, the unauthorized disclosure of the identity of an intelligence officer who has recruited or obtained information from human sources can potentially be as damaging as revealing the identity of the sources themselves. Ishmael Jones explained it thus:

> I have dealt with hundreds of people in countries such as Russia, Ukraine, Iran, Iraq, Pakistan, and Libya. Those who provided secrets to the United States, especially on terrorist organizations, nuclear weapons programs, and organized crime, are at risk once my identity and association with the CIA become known. Revealing my identity and thus the connection of these people can result in their arrest and/or execution. Many of the people I have dealt with had no espionage role, such as hotel clerks, visa providers, and social and cover company business contacts, but they too will be suspected of espionage and can be arrested, harassed, and/or executed.[cv]

In order to be effective and fulfill their mandate, security agencies not only rely on their own employees but also on a variety of other human sources and employ many methods.[cvi] The identity of human sources and the exact ways and means by which intelligence is collected are among the most highly guarded secrets of the state. As former CIA Director and then Secretary of Defense Robert Gates said, "[g]rowing up in the intelligence business, protecting your sources is sacrosanct."[cvii] Former senior FBI officer Andrew McCabe said as much when he wrote:

> In the FBI, a confidential informant is someone who regularly provides information to the FBI but whose role as a source can never be revealed. Exposing the informant's relationship with the FBI could place the source and his or her family in great danger. Protecting the identity of a confidential informant is one of an agent's most sacred responsibilities.[cviii]

Sources and methods are legally protected and any attempt at disclosure is strongly contested in the United Kingdom and the United States. Heads of state and senior officials have regularly stressed the necessity of their protection. US President Bill Clinton was unequivocal about this:

> I agree that unauthorized disclosures can be extraordinarily harmful to United States national security interests and that far too many such disclosures occur. I have been particularly concerned about their potential effects on the sometimes irreplaceable intelligence sources and methods on which we rely to acquire accurate and timely information I need in order to make the most appropriate decisions on matters of national security.[cix]

So was David Omand, who served as the highest levels of Britain's intelligence system:

> I understand the argument that the reason the Security and Intelligence Agencies are obsessed with secrecy is because they want to avoid accountability. But as former Intelligence & Security Coordinator and Agency Head I know it to be wrong. Intelligence organisations that cannot protect their techniques and sources will not survive for long. Compromise them and they will dry up and we will be less safe.[cx]

Human intelligence sources providing information to security agencies are always at risk of discovery.[cxi] In the case of foreign human intelligence sources, their own government, if aware of their identities and activities, can be a source of danger to "themselves, their families, and their associates."[cxii] Therefore, before they give information to a security agency or another country human intelligence sources will need assurances that their identity and activities will be protected from public disclosure. If such assurances

cannot be given, or unauthorized disclosures occur, the security agencies relying on these sources would lose credibility and encounter increasing difficulties in recruiting and retaining new sources.[cxiii] As a former intelligence officer told Congress of his experience at the time of the Church Committee in the 1970s:

> Colonel ALLARD. […]. Ma'am, I was a young intelligence officer in Germany during the Church Committee hearings back in the 1970's [sic]. I had sources look at me and say, you know what, I am not going to do that for you because I don't want to see my name on the front page of *The New York Times* or *Washington Post*. I now know how they felt. And let me tell you something. When you have that reluctance of sources to believe in the confidence of the United States, that is a huge blow. It takes years to overcome this.[cxiv]

As then Deputy Director of the Central Intelligence Agency, Stephen R Kappes, explained:

> For example, if an unauthorized disclosure of classified CIA information regarding a human intelligence source were made, that disclosure could jeopardize the source. If the CIA were to officially acknowledge the information, however, that additional step could further jeopardize the source and could deter other clandestine human intelligence sources from cooperating with the CIA. Existing and future human intelligence sources would note that the CIA was willing to confirm publicly a clandestine human intelligence source's involvement with the CIA. These human sources would factor that additional risk into their own decision on whether to provide information to the CIA and could decide that the risks are too great to cooperate with the CIA.[cxv]

The situation is the same with respect to domestic as foreign sources. As former senior FBI officer Andrew McCabe explains:

> Not giving up your people: This is important. It is crucially important not only to the FBI but to the country's safety and security. The ability to identify and develop relationships with human sources is oxygen to the FBI. The Bureau cannot live without that. It is the first step toward the activation of any of

> our other, more sophisticated investigative authorities. You do not get to search warrants, you don't get to subpoenas, you don't get to listen in on a subject's communications through a FISA [*Foreign Intelligence Surveillance Act*] or Title III court order, without people telling you what they know. And if you can't credibly tell them that you will protect and conceal their identity if they are willing to go out on a limb, if they are willing to risk their own and their families' lives and welfare—if they can't trust that you will protect them—then they will not cooperate with you.[cxvi]

The protection of human sources is taken so seriously as necessitating that alleged criminals not be confronted with state secrets as evidence. As David Anderson, Britain's independent reviewer of terrorism legislation, stated in such a situation in 2013, had British prosecutors used key evidence that was classified and in the hands of intelligence agencies against terrorism suspects, it would have endangered the human sources from whom the evidence originated:

> The reasons why these people [terrorism suspects] weren't prosecuted - or were prosecuted without reference to all the intelligence - was more about a reluctance to use human source reporting in an open criminal trial for fear of compromising or even endangering a source.[cxvii]

In addition to protecting its human sources, the United States has stubbornly fought any disclosure that could help its adversary figuring out its capabilities.[cxviii] One post-9/11 example is the detention sites operated by the CIA in foreign countries. Conscious that information concerning the existence of these sites would eventually come out in public, as it did, CIA warned of the implications for the continuous use of that method of gathering intelligence. In an internal memorandum, CIA officials explained that:

> As captured terrorists may be held days, months, or years, the likelihood of exposure will grow over time [...]. Media exposure could inflame public opinion against a host government and the US, thereby threatening the continued operation of the facility.[cxix]

Later learning that the media had information about a detainee being in a specific country, the CIA preventively shut down that country's detention site.[cxx] After leaks on detention sites occurred anyhow, another country asked that the CIA detention center on its territory be closed within hours.[cxxi]

There are many pre-9/11 examples of methods being compromised. For example, Robert Hanssen, the FBI special agent who spied against the United States for the Soviet Committee on State Security (KGB) and its successor, the Russian Foreign Intelligence Service (SVR), revealed the existence of a tunnel beneath the Soviet Embassy in Washington, DC used to listen to Soviet communications. The damage of this disclosure was significant:

> Hanssen told the Soviets about the existence of the tunnel, rendering it completely useless. Worse yet, because the Americans didn't know that the tunnel had been compromised and continued to scarf up any tidbit of information they could glean, the Russians were able to feed the US sleuths misleading information through the tunnel. Eventually, the FBI had little choice but to fill in the tunnel at a cost in the millions of dollars.[cxxii]

While secret keepers never go into detail about past and future damages in cases of unauthorized disclosures, media discussions and speculations often force their hand. Illustrative of this situation is the response given by the Cabinet Office to questions about the impact of Snowden's disclosures:

> It is obviously not possible in an open statement to go into detail about the real and serious damage already caused by the disclosures based on Mr Snowden's misappropriations, nor about what further damage may follow. However, given the volume of media reporting published over the past three months, and public statements from the UK and US Governments, I can say with confidence that the material seized [by Snowden] is highly likely to describe techniques that have been crucial in life-saving counter-terrorism operations, the prevention and detection of serious crime, and other intelligence activities vital to the security of the UK. The compromise of these methods would do serious damage to UK national security, and ultimately put lives at risk.[cxxiii]

Secret keepers certainly know that history is giving them reasons to be worried when the names of intelligence officers and sources are disclosed without authorization, either through leakage or espionage.[cxxiv] On 23 December 1975, Richard S. Welch, the CIA station chief in Athens, was assassinated on his doorstep by the terrorist group Revolutionary Organization of November 17. His assassination was the result of a leak that led to the adoption in 1982 of the *Intelligence Identities Protection Act* (Pub L 97-200) (IIPA).[cxxv] In a pre-9/11 context, CIA officer Aldrich Ames's espionage on behalf of Russia resulted in the executions of at least ten intelligence sources of the FBI and CIA and the imprisonment of others, while the espionage on behalf of Russia of FBI officer Robert Hanssen resulted in the death of at least two intelligence sources.[cxxvi] While both Ames and Hanssen were not charged under the IIPA due to the severity of their crimes, the IIPA has been used twice, both times leading to convictions pursuant to guilty pleas. In the first instance dating to the 1980s, a CIA source was believed to have been killed when a CIA clerk gave classified

information to a Ghanaian agent she was romantically involved with.[cxxvii] In the second instance a few years ago, a CIA officer gave the name of a covert agent to a journalist, but no loss of life resulted from the unauthorized disclosure.[cxxviii]

In testimony to Congress in 2012, Ken Wainstein, protected secrets as a FBI officer and Assistant Attorney General for National Security, cited the Welch's death to illustrate the point that leaks cause harm to life:

> Obviously, leaks can also prove dangerous or fatal to our [US government] personnel in sensitive positions, as was tragically demonstrated by the murder of the CIA's Chief of Station in Athens by terrorists in the 1970's after his outing by a former CIA employee.[cxxix]

Arguing by Analogy

The use of analogies in discourses as a "method of argumentation in the social and political arena" is pervasive.[cxxx] As a mental tool that assists reasoning, analogies help make sense of the world by making the unfamiliar known.[cxxxi] Analogies do this by comparing one thing with something else when there are components, or relationships between these components, in both that play comparable roles, irrespective of each's knowledge domain.[cxxxii] What analogies do can be instructive, but also manipulative in favour of their users' ends.[cxxxiii] This is particularly so when they are used as a problem solving tool, whereby they offer a "top-down mechanism for constructing mental models."[cxxxiv] As Holland and his colleagues explain,

> In the case of problem solving, analogy is used to generate new rules applicable to a novel target problem by transferring

> knowledge from a source domain that is better understood. The usefulness of an analogy depends on the recognition and exploitation of some significant similarity between the target and the source.[cxxxv]

Secret keepers use an inter-domain analogy, which they refer to as the mosaic theory or effect, terms that are used interchangeably as an argument to protect state secrets from disclosure. Secret keepers use the everyday life knowledge that people have about solving traditional jigsaw/picture puzzles and apply it to state secrecy where each individual secret being a piece of the puzzle. In doing so, secret keepers want judges and the general public to understand the possible harmful effects that the release of innocuous state secrets, individually or grouped together, could cause. The analogy works because it can arguably stand on its own due its simplicity and widespread understanding, but also because it is rooted in the experience and knowledge of secret keepers, which gives them the authority to determine what state secrets fall under the analogy.[cxxxvi] The mosaic theory thus "holds that the executive branch is best qualified to ascertain the importance of discrete bits of information as part of 'the whole picture' in matters of national security."[cxxxvii] Specifically, the theory posits that

> Disparate items of information, though individually of limited or no utility to their possessor, can take on added significance when combined with other items of information. Combining the items illuminates their interrelationships and breeds analytic synergies, so that the resulting mosaic of information is worth more than the sum of its parts. In the context of national security, the mosaic theory suggests the potential for an adversary to deduce from independently innocuous facts a strategic vulnerability, exploitable for malevolent ends. […] The relevant pieces of information might come from the government,

> other public sources, the adversary's own sources, or any mixture thereof.[cxxxviii]

The mosaic theory is commonly asserted in the United States and the United Kingdom, typically in legal disputes regarding access to information request. Secret keepers in the United States are particularly fond of the mosaic effect. They have described it as a reconstituted jigsaw puzzle that give a complete picture of a state secret that must be protected:

> Minor details of intelligence information may reveal more information than their apparent insignificance suggests because, much like a piece of jigsaw puzzle, [each detail] may aid in piecing together other bits of information even when the individual piece is not of obvious importance in itself.[cxxxix]

Former senior CIA and FBI officer Philip Mudd made this point as follow:

> On the surface and in isolation, some of the information we collected might be viewed as minutiae, bits of data collected for their own sake. This judgment misses the crux of the intelligence work we did: the fragment of a name from a training camp years ago, matched with other data, might yield the beginnings of an identification of that individual. In the world of intelligence, this is gold.[cxl]

In order to fully avoid the mosaic effect, before the court the CIA stressed that indirect references to sources and methods should be protected from disclosure. After all, adversaries of the United States

> have the capacity and ability to gather information from myriad sources, analyze it, and deduce means and methods from disparate details to defeat the CIA's collection efforts [a reference to loss of efficiency]. [...] Thus, even seemingly innocuous, indirect references to an intelligence source or method could have significant adverse effects when juxtaposed with other publicly-available data.[cxli]

In a declaration submitted in the course of a FOIA civil action, the FBI used the mosaic argument to prevent the release of file numbers and subfile names:

> Applying a mosaic analysis, suspects could use these numbers (indicative of investigative priority), in conjunction with other information known about other individuals and/or techniques, to change their pattern of activity to avoid detection, apprehension, or create alibis for suspected activities, etc [a reference to loss of efficiency].[cxlii]

And to prevent that the identity and/or location of FBI units be released:

> The FBI asserted exemption (b)(7)(E)-4 to protect methods and techniques involving the location and identity of FBI units and/or joint units that were involved in this investigation. The office location and units are usually found in the administrative headings of internal FBI documents. These headings identify the locations of the office and unit that originated or received the documents. Disclosure of the location of the units conducting the investigation would reveal the targets, the physical areas of interest of the investigation, and when taken together with the other locations if identified, could establish a pattern or 'mosaic' that identification of a single location would not. If the locations are clusters in a particular area, it would allow hostile analysts to avoid or circumvent those locations, especially if one or more location appeared with frequency or in a pattern [a reference to loss of efficiency]. This would disrupt the method of the investigative process and deprive the FBI of valuable information [a reference to loss of efficiency]. The withholding of the units involved is justifiable as well under a similar rationale.[cxliii]

The United Kingdom used the mosaic argument several times over the years.[cxliv] In the highly publicized *Spycatcher* case, it made the argument as follows:

> The dangers could arise notwithstanding that the information disclosed was unclassified and is on its face and in isolation apparently innocuous. Such information may take on a wider significance if put together with other information in possession of other persons and thereby, for example, enable them to check the veracity of their sources of information. Furthermore,

> information which appears to be innocuous at a particular date or to a particular officer may at a later date become significant.[cxlv]

The line of argument developed in *Spycatcher* remains valid. In 2007, the Director of Information (Exploitation) at the British Ministry of Defence asserted in an access to information case that the government had "an active concern about what he called the 'mosaic effect,' e.g., the risk that pieces of information released in different contexts could be joined together in order to build up a larger picture."[cxlvi] In 2014, the Cabinet Office argued in favour of the mosaic effect too, this time dismissing the notion that a journalist could pass judgment on this argument:

> Indeed it is impossible for a journalist alone to form a proper judgment about what disclosure of protectively marked intelligence does or does not damage national security... The fragmentary nature of intelligence means that even a seemingly innocuous piece of information can provide important clues to individuals involved in extremism or terrorism.[cxlvii]

Conclusion

The rhetorical devices discussed in this article are parts and parcels of the discourse of secret keepers, which give meaning to the social world of state secrecy. Taken together, they form a linguistic practice that is reproduced from one case to another, from one generation of secret keepers to another. More importantly, these devices provide secret keepers means by which to assert their knowledge and expertise, and to legitimize (if judges use these devices to decide against disclosure[cxlviii]) the nondisclosure of state secrets. By using arguments from ignorance and authority, secret keepers

claim to secure a monopoly of knowledge, which has the effect of establishing a sharp divide between sacred and profane knowledge and of constituting others as profane.[cxlix]

The use of subjunctive conditionals has at least two major effects: first, they are used for a clear moral purpose, that is, to avoid harm. Second, they purport to reflect how the actual world of state secrecy was, is or will be "causally hooked up."[cl] Claiming future harm, for instance, manufactures fear (*ultimately, you see, someone could die*) and raises the first duty of the state, which should not be interfered with but honoured by the court. In the end, the linguistic devices used by secret keepers are means by which they can manage their credibility while convincing others (judges and the public) of the necessity of sharing their viewpoint and proposed course of action on nondisclosure.[cli] The claim of future harm is central to the argument from consequences.

When arguing from consequences, secret keepers use verbs and adjectives evoking fear and emotions and the loss of national security protection effectiveness to claim that harm can be avoided and everyone kept safe by the nondisclosure of state secrets. To that effect, secret keepers have used value-oriented lexical terms such as "jeopardy," "disaster," "risk," "protection," "stake," "threat," "harmful," "damages," "endanger," "safe," "blood," "killed," "destroyed," "countless," "death," "incarceration," "loss," "lives," "families," "national security," "arrest," "arrested," "tortured," "execution," "harassment," "harassed," "important,"

"sacrosanct," "sacred," "survive," "dry up," "blow," "deter," "compromising," "useless," "life-saving," "assurance," "assistance," "expose," "usefulness," "prejudice," "affect," "dangerous" and "fatal," and qualifiers such as "great deal," "grave," "serious," "huge," "very," "crucial," "vital," "tremendous," "worst," "real" and "extraordinarily." The emotional and fear value of the terms used is usually greater outside the court that within, as we have seen in the examples on the reactions to Manning's and Snowden's disclosures, where affidavits and testimonies by secret keepers and their legal representatives are more measured and adjusted to respect the decorum and rules of the court.[clii] Finally, to impress on their listeners how important it is not to release what appears to be innocuous states secrets, secret keepers resort to a basic inter-domain analogy, the mosaic theory, that can be understood by just about anyone. Once again, the primary purpose of using this analogy is to show judges and the general public that the disclosure, in this case of apparently innocuous state secrets, could lead to harmful consequences.

In the manner in which they are used, rhetorical devices have an indeterminate temporal and spatial element. The harmful consequences that could result from the disclosure of state secrets could be imminent or far off into the future. Spatially, these harmful consequences could be felt very close at home or in a far distant location. In other words: if not now, then tomorrow; if not here, then over there. Ultimately, the possibility of harmful consequences is always going to be contingent and indeterminate. For secret

keepers, there is only one course of action open in such a circumstance: do not disclose.

Rhetorical devices have by design a truth production component about the effects of disclosing state secrets and a prescriptive component about what to do with them. Secret keepers expect these effects and prescription of nondisclosure to be acceptable to judges and the public under certain conditions: when they represent the official position of the state, when the official position of the state has a recognized status before the court and before the public, and when the representatives of the states speak with authority and within the confines of their recognized responsibilities. Ultimately, "[I]t matters what one says and how one says it, […] the power of words is both in their message and their form."[cliii]

---

i Quoted in Melley, *The Covert Sphere*, 15.

ii State secrets are information or material that the state is (1) taking measures to safeguard, (2) deliberately concealing from public view, and (3) refusing to disclose because it would be against the national interests of the state to do so. A state secret is stamped - or classified - Confidential, Secret or Top Secret by secret keepers on the basis of the degree of injury it would cause to a state's national interest (usually in the areas of national security, national defense and international relations) if it were disclosed without authorization to anyone not authorized to be in its possession. The most guarded state secrets are usually those that "might reveal what government knows about terrorists [and spies], or might compromise intelligence sources and methods, thereby reducing the flow of intelligence [from domestic and foreign sources]" if inappropriately disclosed. See Shapiro and Siegel, "Is this Paper Dangerous?, 75. Thus, the secrets of sub-national governments, private sector information of a confidential nature, and information sensitive in other than the national interest (such as private information) are not state secrets for the purposes of this article.

iii I particularly like Eco's definition, even if it excludes classified material: "A secret is information that is not revealed, or must not or should not be revealed, because if it were, that revelation would cause harm to whoever divulged it and sometimes even to those who received it." Eco, *On the Shoulders of Giants*, 222.

iv I use the term device in this article as it is most commonly used, that is, to include what is made or adapted for a particular purpose. Each of the devices under review are

used in the discourse carried out by secret keepers for a particular purpose (the nondisclosure of state secrets) and can be adapted as required (in tone, gravity, length, etc.). See also Burr, *An Introduction to Social Constructionism*, 61.

v Smith, *Advanced Legal Writing*, 11–13.

vi It is true of course that when linguistic expressions have once been created and have become the common possession of a given society, with meanings determined by convention, they can be repeated and handed on from generation to generation." Copleston, *A History of Philosophy, Volume IX*, 405.

vii Spitzmller and Warnke, "Discourse as a 'Linguistic Object'," 76.

viii Urban, "The Torment of Secrecy," 212-213. Social scientists, especially, have spent little time theorizing about the "origins, nature, workings, and consequences of secrecy within social systems." Lowry, "Toward a Sociology of Secrecy and Security Systems," 298.

ix Walters and Luscombe, "Hannah Arendt and the Art of Secrecy," 7.

x Eco, *Inventing the Enemy*, 117.

xi Jayyusi, *Categorization and the Moral Order*, 75.

xii Ibid, 75-76.

xiii This is a similar situation as that encountered with lists associated with the practice of security more generally. As MacDonald and Hunter have noted: "This strategy of generating lists of disparate practices and processes, gives the impression of a 'hyper-complexity' associated with the practice of security, although the precise relations between the disparate elements are often left unspecified." MacDonald and Hunter, "Security, Population and Governmentality," 128.

xiv I previously used these examples, in Lefebvre, "Why Are State Secrets Protected from Disclosure? The Discourse of Secret Keepers."

xv United States, *National Security Leaks and the Law*, at 10-11, 13 (Wainstein).

xvi *Secretary of State for the Home Department v. HM Senior Coroner for Surrey & Ors*, [2016] EWHC 3001 (Admin) at para 29.

xvii *Hitchens v. Secretary Of State For The Home Department*, [2003] UKIT NSA5. Perhaps put more straightforwardly by the Secretary of State, quoting Lord Griffiths, in *Liberty (The National Council of Civil Liberties) v. The Government Communications Headquarters & Ors*, [2014] UKIPTrib 13_77-H at para 13, who said: "Secrecy is essential to the necessarily covert work and operational effectiveness of the Intelligence Services, whose primary function is to protect national security." *Attorney General v. Guardian Newspapers Ltd (No.2)*, [1990] 1 AC 109 at 269F (Lord Griffiths).

xviii "One problem with assessing the validity of claims of damage is their lack of specificity - a result of the evidence being classified." Richelson, "Intelligence Secrets and Unauthorized Disclosures," 655.

xix "'[T]emporality' is time insofar as it manifests itself in human existence." Hoy, *The Time of Our Lives*, xii.

xx "Clearly human experience is temporal, whether or not we are conscious of the temporal. Also, it seems hard to deny that we can be conscious of the temporality of existence." Ibid., xv.

xxi As May and Thrift note, "the nature and experience of social time is multiple and heterogeneous, so it follows that the manner of its construction - the means by which a particular sense of time comes into being and moves forward to frame our understandings and actions - is in turn both multiple and dynamic." May and Thrift, "Introduction," 3.

xxii Horwich, *Asymmetries in Time*, 15, 199-200. These points by Horwich are stressed in Jaszczolt, *Representing Time*, 19.

xxiii Bourdieu, *Outline of a Theory of Practice*, 78-83.

xxiv Wacquant, "Pratique, pouvoir et science, 201-202. Bourdieu, *The Logic of Practice*, 53.

xxv Hoy, *The Time of Our Lives*, 180.

xxvi "Eschatology […] suggests a sudden, disruptive occurrence such that when it happens is irrelevant. The eschatological event could happen tomorrow or centuries from now." Hoy, *The Time of Our Lives*, 141.

xxvii As Wells notes, "[o]fficials make no genuine attempt to identify the danger, or even possible alternative dangers, posed by the information. Rather, the government's argument suggests in some sort of shadowy way that the very existence of the information poses the danger; thus, it cannot fall into the wrong, or any, hands." Wells, "*CIA v. Sims*, 873.
xxviii Jarvis, *Times of Terror*, 17.
xxix Newell, "Technopolicing, Surveillance, and Citizen Oversight," 429. Melley makes a similar point, arguing that over time big secrets tend towards disclosure: "Whereas small operations often remain secret, larger initiatives are more difficult to conceal, particularly over time. Secrecy, that is, has a temporal dimension." Melley, *The Covert Sphere*, 13.
xxx See Bennett, "Conditionals and Explanations," 1.
xxxi This example is from Lefebvre, "Why Are State Secrets Protected from Disclosure?," 204.
xxxii *United States v. Ishmael Jones*, Civil Action No 1:10cv765-GBL-TRJ (ED Va 2010), 4-6 (Declaration of Ralph S DiMaio, Information Review Officer, National Clandestine Service, Central Intelligence Agency), 4-6.
xxxiii Ibid.
xxxiv Ibid.
xxxv *Larry Klayman v. Central Intelligence Agency*, Civil Action No. 14-00472 RDM (D DC, 3 June 2015) (Declaration of Martha M. Lutz, Information Review Officer, Central Intelligence Agency), 25.
xxxvi Declaration of Antoinette B. Shiner, Information Review Officer for the Litigation Information Review Office at the CIA, quoted in *Mattathias Schwartz v Department of Defense et al*, Case 1:15-cv-07077-ARR-RLM (30 September 2016) (Defendant's Memorandum of Law in Support of their Motion for Summary Judgment), 22.
xxxvii *American Civil Liberties Union v CIA*, Civil Action No. 1:10-cv-00436-RMC (D DC 8 August 2013) (Declaration of Martha M. Lutz, Chief of the Litigation Support Unit, Central Intelligence Agency), 20.
xxxviii *In Re Motion for Release of Court Records*, Docket Number: MISC. 07-01 (Foreign Intelligence Surveillance Court [FISC] 31 August 2007) (Opposition to the American Civil Liberties Union's Motion for Release of Court Records), 8.
xxxix Omand, "Our Security and Intelligence Agencies Must Be Held To Account."
xl *Jefferson Morley v. Central Intelligence Agency*, USCA Case #10-5161 (DC Cir 28 February 2012) (Brief for Appellee), 35.
xli Ibid, 33.
xlii I previously used this paragraph in Lefebvre, "Why Are State Secrets Protected from Disclosure? The Discourse of Secret Keepers."
xliii Because her husband, a former diplomat who was sent to Niger by the CIA, had embarrassed the While House by publicly denying one of its claims about Iraq's weapons of mass destruction. See Wilson, *The Politics of Truth*.
xliv Plame Wilson, *Fair Game*, 301.
xlv There are, of course, well known instances where harm resulted from unauthorized disclosures. The assassination on his doorstep of Richard S. Welch, the CIA station chief in Athens, by the terrorist group Revolutionary Organization of November 17 as a result of a leak in 1975 is well known, and so are the damages caused by CIA officer Aldrich Ames and FBI officer Robert Hanssen, who both spied on behalf of Russia: 10 intelligence sources of the FBI and CIA were executed and many others imprisoned as a result of Aldrich's actions, and at least three intelligence sources were killed as a result of Hanssen's actions. Lefebvre, "Why Are State Secrets Protected from Disclosure?" 213. Hanssen also revealed the existence of a tunnel beneath the Soviet Embassy in Washington, DC, used to listen to Soviet communications. The damage of this disclosure was significant: "Hanssen told the Soviets about the existence of the tunnel, rendering it completely useless. Worse yet, because the Americans didn't know that the tunnel had been compromised and continued to scarf up any tidbit of information they could glean, the Russians were able to feed the US sleuths misleading information through the tunnel. Eventually, the FBI had little choice but to fill in the tunnel at a cost in the millions of dollars." Ashcroft, *Never Again*, 86-87.

xlvi Tetlock, "How to Win at Forecasting," 22.
xlvii Of course, "[i]n some cases, the argument from ignorance can be completely reasonable." Zarefsky, *Rhetorical Perspectives on Argumentation*, 159.
xlviii Ibid, 163.
xlix As Kitrosser observes in the US context: "Attempts to diminish this information monopoly [of the state] themselves are frequently blocked by claims that only the President and certain subordinates know when information is too dangerous to be disclosed." Kitrosser, "What If Daniel Ellsberg Hadn't Bothered?" 97.
l *Franz Boening v Central Intelligence Agency*, Civil Action No. 07-0430 (EGS) (Memorandum of Points and Authorities in Support of Defendant's Motion to Dismiss Under Rule 12 And Motion for Summary Judgment Under Rule 56), 30.
li Hoeken, Timmers and Schellens, "Arguing about desirable consequences," 402.
lii Beller and Spada, "The logic of content effects in propositional reasoning," 362.
liii Too often, German and Stanley write, "courts accept government claims about the potential risk to national security as absolute, without independently scrutinizing the evidence or seeking alternative methods to give plaintiffs or victims an opportunity to discover non-privileged information with which to prove their cases." German and Stanley, *Drastic Measures Required*, 9.
liv *Gosling v Secretary Of State For The Home Department*, [2003] UKIT NSA4 at para 33.
lv *Steven Aftergood v. Central Intelligence Agency*, Civil Action No. 01-2524 (RMU) (DC) (Defendant's Cross-Motion for Summary Judgment, 15 September 2004), 14.
lvi *Larson v. Department of State*, 565 F (3d) 857, 868 (DC Cir 2009).
lvii *Franz Boening v. Central Intelligence Agency*, Case 1:07-cv-00430-EGS (D DC 20 July 2007) (Memorandum of Points and Authorities in Support of Defendant's Motion to Dismiss Under Rule 12 and Motion for Summary Judgment Under Rule 56), 28-30.
lviii *Jefferson Morley v. Central Intelligence Agency*, USCA Case #10-5161 (DC Cir 28 February 2012) (Brief for Appellee), 35.
lix *American Civil Liberties Union v. CIA*, Civil Action No. 1:10-cv-00436-RMC (D DC 1 October 2010) (Defendant CIA's First Motion for Summary Judgment), 6, 10. The same reasoning was repeated in the second motion: *American Civil Liberties Union v. CIA*, Civil Action No. 1:10-cv-00436-RMC (D DC 9 August 2013) (Defendant CIA's Second Motion for Summary Judgment), 10, 22.
lx *In Re Motion for Release of Court Records*, Docket Number: MISC. 07-01 (Foreign Intelligence Surveillance Court [FISC] 31 August 2007) (Opposition to the American Civil Liberties Union's Motion for Release of Court Records), 7.
lxi *American Civil Liberties Union v. CIA*, USCA Case #11-5320 (21 May 2012) (Brief for Appellee), 21.
lxii *Electronic Frontier Foundation v. Department of Justice*, Civil Action No. 12-1441-ABJ (1 April 2013) (Memorandum of Points and Authorities in Support of the Department of Justice's Motion for Summary Judgment), 21. For additional examples, see *Mattathias Schwartz v. Department of Defense et al*, Case 1:15-cv-07077-ARR-RLM (30 September 2016) (Defendant's Memorandum of Law in Support of Their Motion for Summary Judgment), 27, *Electronic Privacy Information Center v. Office of the Director of Central Intelligence*, Case No. 17-cv-0163 RC (D DC 26 June 2017) (Defendant's Memorandum of Points and Authorities in Support of Its Motion for Summary Judgment), 10, *National Security Archive v. Central Intelligence Agency*, Case 1:11-cv-00724-GK (26 September 2011) (Defendant's Motion for Summary Judgment), 7, and *Electronic Frontier Foundation v. Department of Justice*, Case Civil No. 07-00403 (TFH) (D DC 25 June 2007) (Defendant's Opposition to Plaintiff's Motion for In Camera Review and Reply in Support of Defendant's Motion for Summary Judgment), 6.
lxiii "Mr. Tam pressed the following argument upon us. He submitted that the Service was best placed, through its experience and expertise, to make the relevant decisions." Para 33 of Annex A of *Hitchens v. Secretary Of State For The Home Department* [2003] UKIT NSA5 (4 August 2003).

lxiv *Hitchens v. Secretary Of State For The Home Department* [2003] UKIT NSA5 (4 August 2003), para 32.
lxv Dehghan, Watt and Travis, "We Should Talk Sensibly about Spying Clinton," 1.
lxvi Quoted from the September 2016 Cipher Brief newsletter. "You're US government property" *The Economist* (12 November 2016) special report, 8.
lxvii "This type of argument supports a claim about the desirability of a certain action by pointing out the advantageous outcomes the action may have. Conversely it can also support a claim about the undesirability of a certain action by pointing out its disadvantages." Hoeken, Timmers and Schellens, "Arguing about desirable consequences," 397. See also Walton, *Fundamentals of Critical Argumentation*, 104, and Tindale, *Fallacies and Argument Appraisal*, 183.
lxviii As Constable aptly notes, "As persuasive utterances, the legal speech acts of representatives of official law as well as the claims of their critics are performative and passionate, *designed to evoke in their respective hearers a shared sense of obligation that is not only conventionally performed but also a matter of desire*" [emphasis added]. Constable, *Our Word Is Our Bond*, 103.
lxix Hoeken, Timmers and Schellens, "Arguing about desirable consequences," 399.
lxx Defence counsel Gareth Peirce has framed this process as follow: "We still live, in the 21st century, in a world whose political configuration is that of nation-states. For those exercising political power, the matter of a nation's security, its 'national security', is of immense importance. The state is invariably referred to as a source of the security necessary for protection against threats from others, or from internal violence, and this idea is shared by and large by the population. There may be disagreement about the existence or gravity of any alleged threat and the appropriate response to it, but the concept of the state as the protector and guarantor of security is seldom doubted. 'Security' is such a dramatic yet ill-defined concept that those in power are able to curb criticism and shut down debate by invoking it and by claiming to possess vital knowledge (which cannot, of course, be safely revealed) to support their actions or policies. Those in power draw on traditions of deference and non-partisanship when it comes to security, making it unnecessary for governments to provide reasoned justification when security is said to be at stake. There is therefore a dangerous circularity to the entire process. Deference is fed in part by ignorance, and ignorance is fed in turn by claims that secrecy is indispensable. The public receives only the barest of justifications, which it is supposed to take on trust, while the government machine ignores or short-circuits normal democratic processes." Peirce, "Make sure you say that you were treated properly."
lxxi Similar discourses of legitimization involving a threat element have been recognized and studied by Cap, *The Language of Fear*.
lxxii As this part of the discourse on state secrecy aims to arise emotions in support of secret keeping by demonizing leakers, it is usually found in non-judicial texts, which are the primary material for this set of examples.
lxxiii This was argued early on by Adam Smith in 18th Century Britain. Kennedy, *Adam Smith's Lost Legacy*, 216, Stone, "Public Economic Policy," 66. While this is a popular view, it is not universally shared. Otteson, for example, has argued that the first duty of the state is to secure justice. Otteson, *Actual Ethics*, 105. So did François Laurent in the 19th Century in *Droit civil international*, Volume 3 (Paris: 1850), 14, cited in Frey and Frey, *The History of Diplomatic Immunity*, 341. Those who advocate cosmopolitan citizenship also disagree with this notion. Linklater, "Cosmopolitan Citizenship," 322.
lxxiv Moberly, "Whistleblowers and the Obama Presidency," 74.
lxxv "Across media and news outlets, a juridical narrative attempts to accomplish the task of secreting Manning's revelations on the basis of her actions' ostensible threat to national security. There is an irony built into this modality: The juridical narrative becomes more powerful to the extent that Manning is represented as having made an agentive, political choice to disclose military secrets. Thus, when coverage is narrowed strictly to what Manning did, the frame is a repressive one. […]. This story, like many others, is laser-

focused on Manning's actions as a crime." Cloud, "Private Manning and the Chamber of Secrets," 89.
lxxvi Mitchell and Gosztola, *Truth and Consequences*, 47.
lxxvii Ibid, 47.
lxxviii Nicks, *Private*, 191.
lxxix The mainstream media redacted names to protect any US source from harm. Wikileaks' decision not to redact these names was not internally unanimous: "Smari McCarthy, a former Wikileaks volunteer, later told London's *The Independent* that even internally at the group there were 'serious disagreements over the decision not to redact the names of Afghan civilians.'" Mitchell, *The Age of Wikileaks*, 53.
lxxx Nicks, *Private*, 191-192.
lxxxi Mitchell, *The Age of Wikileaks*, 67.
lxxxii Nakashima, "Pentagon."
lxxxiii Mitchell and Gosztola, *Truth and Consequences*, 53.
lxxxiv Ibid, 60.
lxxxv Leigh and Harding, *Wikileaks*, 192-193.
lxxxvi He was motivated by his opposition to automated mass surveillance, which he saw as a threat to democracy, private life and a free Internet. Lefébure, *L'affaire Snowden*, 30, 38.
lxxxvii Quoted by Harding, *The Snowden Files*, 36.
lxxxviii Lefébure, *L'affaire Snowden*, 20, 29, 39.
lxxxix Quoted by Gallagher, "ISIS Using Encrypted Apps for Communications."
xc Berghel, "Mr. Snowden's Legacy," 67.
xci Halliday, "MOD Serves News Outlets with D Notice Over Surveillance Leaks," 8.
xcii Watt, Ackerman, Halliday and Mason, "US and Britain at odds as NSA row deepens," 1.
xciii Campbell, Wright, Cusick and Sengupta, "UK's Secret Mid-East Internet Surveillance Base is Revealed in Edward Snowden Leaks," 1.
xciv Quoted by Booth, "Case Reveals British Delays over Snowden Data," 2. Robbins kept the same discourse a few months later during another court appearance: "The compromise of top secret information would be likely to have one or more of the following consequences; to threaten the internal stability of the UK or friendly countries, to lead directly to widespread loss of life." Quoted by Whitehead, "GCHQ Leaks 'Damaged UK Security and Risked Lives'," 1.
xcv Clegg, "A Fine Line We Mustn't Cross," 50.
xcvi Naughton, "If You Think These Spying Revelations Don't Matter, It's Time to Think Again," 29.
xcvii United States, Senate Permanent Select Committee on Intelligence, *Requesting the President to Transmit to the House of Representatives Not Later Than 14 Days After the Date of the Adoption of this Resolution Documents in the Possession of the President Relating to the Disclosure of the Identity and Employment of Ms. Valerie Plame*, 7.
xcviii Ishmael Jones (a pen name) authored without pre-publication approval *The Human Factor*. I previously used this paragraph in Lefebvre, "Why Are State Secrets Protected from Disclosure? The Discourse of Secret Keepers."
xcix *United States v. Ishmael Jones*, Civil Action No 1:10cv765-GBL-TRJ, (ED Va 2010), 4-6 (Declaration of Ralph S. DiMaio, Information Review Officer, National Clandestine Service, Central Intelligence Agency).
c Ibid.
ci Ibid.
cii Because her husband, a former diplomat who was sent to Niger by the CIA, had embarrassed the While House by publicly denying one of its claims about Iraq's weapons of mass destruction. See Wilson, *The Politics of Truth*.
ciii Plame Wilson, *Fair Game*, 301.
civ Quoted in Waas, ed, *The United States v. I. Lewis Libby*, 86.

cv *United States v. Ishmael Jones*, Civil Action No 1:10cv765-GBL-TRJ, (ED Va 2010), 2-3 (Declaration of Ishmael Jones).
cvi The following statement is of general application to security and foreign intelligence organizations: "Intelligence sources and methods are the basic practices and procedures used by the CIA to accomplish its mission. They can include human assets, foreign liaison relationships, sophisticated technological devices, collection activities, cover mechanisms, and other sensitive intelligence tools." *American Civil Liberties Union v. Dept of Justice*, 808 F Supp (2d) 280, 291 (DC Cir 2011) (Affidavit of Ms. Cole, CIA's Information Review Officer).
cvii Quoted by Schmitt and Sanger, "Gates Cites Peril in Leak of Afghan War Logs by WikiLeaks." Then CIA Director Richard Helms preferred to lied to Congress while under oath rather than exposing sources and methods to the detriment of the nation's national security. Persico, "Company Man."
cviii McCabe, *The Threat*, 58.
cix Statement by President William J Clinton.
cx Omand, "Our Security and Intelligence Agencies Must Be Held To Account."
cxi I previously used this paragraph and Allard's and Kappes' examples in in Lefebvre, "Why Are State Secrets Protected from Disclosure? The Discourse of Secret Keepers."
cxii *United States v. Ishmael Jones*, Civil Action No 1:10cv765-GBL-TRJ, (ED Va 2011), 4-5 (Second Declaration of Mary Ellen Cole, Information Review Officer, National Clandestine Service, Central Intelligence Agency).
cxiii "Having lost a source of intelligence through an error in judgment in terms of protecting that source, we then run the risk that we no longer will be able to attract additional sources. In a sense, in the intelligence world, we lose our credibility; and, having lost our credibility, we lose our capability to attract." Donnalley, "Declassification in an Open Society," 12.
cxiv United States, *National Security Leaks and the Law*, 46 (Kenneth Allard).
cxv *Wilson v. CIA*, 586 F(3d) 171 (2nd Cir 2009) at 199 (Judge Katzmann quoting declaration of Stephen R. Kappes, Deputy Director, Central Intelligence Agency).
cxvi McCabe, *The Threat*, 60.
cxvii Quoted in "Terrorism Suspects Go Free 'Because MI5 Won't Let Spies Speak'," 2.
cxviii I previously used this paragraph and example in Lefebvre, "Why Are State Secrets Protected from Disclosure? The Discourse of Secret Keepers."
cxix Memorandum for DCI from J. Cofer Black, Director of Counterterrorism, via Deputy Director of Central Intelligence, General Counsel, Executive Director, Deputy Director for Operations and Associate Director of Central Intelligence/Military Support, entitled, "Approval to Establish a Detention Facility for Terrorists." Quoted in US Senate, *The Senate Select Committee on Intelligence Report on Torture*, 29.
cxx US Senate, *The Senate Select Committee on Intelligence Report on Torture*, 38.
cxxi Ibid, 138.
cxxii Ashcroft, *Never Again*, 86-87.
cxxiii *Miranda v Secretary of State for the Home Department & Ors* [2014] EWHC 255 (Admin), para. 52 (Affidavit from Mr Robbins, Deputy National Security Adviser for Intelligence, Security and Resilience).
cxxiv I previously used this paragraph and the next in Lefebvre, "Why Are State Secrets Protected from Disclosure? The Discourse of Secret Keepers."
cxxv Monje, *The Central Intelligence Agency*, xxxix, Smith, *Encyclopedia of the Central Intelligence Agency*, 244.
cxxvi Elsea, "Criminal Prohibitions on Disclosing the Identities of Covert Intelligence Assets," 2, United States, Senate Select Committee on Intelligence, *An Assessment of the Aldrich H. Ames Espionage Case and Its Implications for US Intelligence*, 1, Tucker, "Bradley Manning," C1. Former US Attorney General John Ashcroft writes that at least two KGB agents working for the FBI -Valery Martynov and Sergei Motorin - were executed after having been betrayed by Hanssen. Ashcroft, *Never Again*, 86.

cxxvii Engelberg, "Officials Think Spying Led to Death of C.I.A. Informant in Ghana," A6, Elsea, "Criminal Prohibitions on Disclosing the Identities of Covert Intelligence Assets," 2.
cxxviii Elsea, "Criminal Prohibitions on Disclosing the Identities of Covert Intelligence Assets," 2.
cxxix United States, *National Security Leaks and the Law*, 13 (K. Wainstein).
cxxx Gentner and Maravilla, "Analogical Reasoning," 187.
cxxxi Halpern, *Thought & Knowledge*, 409.
cxxxii "Analogy," in *Chambers Concise Dictionary*, 38; Gentner and Maravilla, "Analogical Reasoning," 186.
cxxxiii "We swim in a vast ocean of analogies, which we both manipulate for our ends and are unwittingly manipulated by." See Domingos, *The Master Algorithm*, 200.
cxxxiv Holland, Holyoak, Nisbett and Thagard, *Induction*, 288.
cxxxv Ibid, 287.
cxxxvi "In law as in life, analogical argument is a valid, albeit undemonstrable, form of reasoning that stands on its own and has its own credentials, which are not derived from abstract reason but are rooted in the experience and knowledge of the lawyers and judges who employ it." See Weinreb, *Legal Reason*, 11.
cxxxvii Greenlee, "National Security Letters and Intelligence Oversight," 185.
cxxxviii Pozen, "The Mosaic Theory," 630. Perkins uniquely refers to it as the "sophisticated intelligence analyst standard." Perkins, "The State Secrets Privilege and the Abdication of Oversight," 245-248.
cxxxix *Wilner v. NSA*, 592 (F3d) 60, 73 (2d Cir 2009) (Affidavit from the National Security Agency), subsequently quoted in *American Civil Liberties Union v. Dept. of Justice*, 681 (F 3d) 61, 71 (2d Cir. 2012).
cxl Mudd, *Takedown*, 63.
cxli *American Civil Liberties Union v Dept of Justice*, 808 F Supp (2d) 280, 291 (DC Cir 2011) (Affidavit of Mary Ellen Cole, Information Review Officer for the CIA's National Clandestine Service).
cxlii *Laura Poitras v. United States Department of Justice, et. al*., Case 1:15-cv-01091-KBJ (Declaration of David M. Hardy), 40.
cxliii Ibid, 41.
cxliv I previously used this paragraph and example in Lefebvre, "Why Are State Secrets Protected from Disclosure? The Discourse of Secret Keepers."
cxlv *Her Majesty's Attorney General v. Guardian Newspapers Limited & Ors*, [1987] UKHL 13, 14, [1987] 1 WLR 1248 (Lord Templeman).
cxlvi *Ministry of Defence v. Information Commissioner and Evans* [2007] UKIT EA_2006_0027 (20 July 2007), para. 35.
cxlvii *Miranda v. Secretary of State for the Home Department & Ors* [2014] EWHC 255 (Admin), para. 58 (Affidavit of Mr. Robbins, Deputy National Security Adviser for Intelligence, Security and Resilience).
cxlviii "The law is constantly in the process of creating its illusion of formality and autonomy by means of the various rhetorical devices at its disposal." Thurschwell, "Reading the Law," 299.
cxlix This distinction is from Bourdieu, *Language and Symbolic Power*, 145.
cl See Bennett, "Conditionals and Explanations," 19.
cli As Cap aptly remarks, "In the words of Habermas ([*The Theory of Communicative* Action]1981), public communication—including state political discourse as well as voices of various non-governmental bodies and 'grass-roots' initiatives—has the continual goal of maximizing the number of 'shared visions', that is, common conceptions of current reality as well as its desired developments." Cap, *The Language of Fear*, 2.
clii As Bourdieu notes, the authoritative discourse of an authorized spokesperson "is more subject to the norms of official propriety than any other, and it condemns the occupants of dominated positions either to silence or to shocking outspokeness […]" (as I have shown outside to be the case the court with the examples related to the disclosures of state secrets by Manning and Snowden). Bourdieu, *Language and Symbolic Power*, 138.

cliii Stoler, *Race and the Education of* Desire, xiv.

Bibliography

"Analogy." In *Chambers Concise Dictionary.* Edinburgh: Chambers, 2004.

Ashcroft, John. *Never Again: Securing America and Restoring Justice.* New York: Center Street, 2006.

Bangerter, Adrian, and Joep Cornelissen. "Studying Discourse Processes in Institutional Contexts." In *The Routledge Handbook of Discourse Processes*, edited by Michael F. Schober, David N. Rapp and M. Anne Britt, 69-96. New York: Routledge, 2018.

Beller, Sieghard, and Hans Spada. "The Logic of Content Effects in Propositional Reasoning: The Case of Conditional Reasoning with a Point of View." *Thinking & Reasoning* 9, no. 4 (2003): 335-378.

Bennett, Jonathan. "Conditionals and Explanations." In *Fact and Value: Essays on Ethics and Metaphysics for Judith Jarvis Thomson*, edited by Alex Byrne, Robert Stalnaker and Ralph Wedgwood, 1-28.Cambridge: The MIT Press, 2001.

Berghel, Hal. "Mr. Snowden's Legacy." *Computer*, April 2014, 67.

Booth, Robert. "Case Reveals British Delays Over Snowden Data." *The Guardian*, August 31, 2013, 2.

Bourdieu, Pierre. *Outline of a Theory of Practice.* Translated by Richard Nice. Cambridge: Cambridge University Press, 1977.

___. *The Logic of Practice.* Translated by Richard Nice. Stanford: Stanford University Press, 1990.

___. *Language and Symbolic Power.* Edited by John B. Thompson. Translated by Gino Raymond and Matthew Adamson. Cambridge: Polity Press, 1991.

Burr, Vivien. *An Introduction to Social Constructionism.* New York: Routledge, 1995.

Campbell, Duncan, Oliver Wright, James Cusick, and Kim Sengupta. "UK's Secret Mid-East Internet Surveillance Base is Revealed in Edward Snowden Leaks." *The Independent*, August 23, 2013. https://www.independent.co.uk/news/uk/politics/exclusive-uk-s-secret-mid-east-internet-surveillance-base-is-revealed-in-edward-snowden-leaks-_8781082.html

Cap, Piotr. *The Language of Fear: Communicating Threat in Public Discourse.* London: Palgrave Macmillan, 2017.

Clegg, Nick. "A Fine Line We Mustn't Cross." *The Guardian*, August 24, 2013, 50.

Clinton, William J. *Statement to the House of Representatives.* November 4, 2000. http://www.fas.org/sgp/news/2000/11/wh110400.html

Cloud, Dana L. "Private Manning and the Chamber of Secrets." *QED: A Journal in GLBTQ Worldmaking* 1, no. 1 (2014): 80-104.

Constable, Marianne. *Our Word Is Our Bond: How Legal Speech Acts*. Stanford: Stanford Law Books, 2014.

Copleston, Frederick. *A History of Philosophy, Volume IX. Modern Philosophy: From the French Revolution to Sartre, Camus, and Lévi-Strauss.* New York: Doubleday, 1974.

Dehgahn, Saeed Kamali, Nicholas Watt, and Alan Travis. "We Should Talk Sensibly about Spying Clinton." *The Guardian*, October 12, 2013, 1.

Domingos, Pedro. *The Master Algorithm.* New York: Basic Books, 2018.

Donnalley, Gail F. "Declassification in an Open Society." *Studies in Intelligence* 18, no. 3 (1974): 11-18.

Eco, Umberto. *Inventing the Enemy and Other Occasional Writings.* Translated by Richard Dixon. Boston: Mariner Books, 2012.

___. *On the Shoulders of Giants*. Cambridge, MA: The Belknap Press of Harvard University Press, 2019.

Elsea, Jennifer K. *Criminal Prohibitions on Disclosing the Identities of Covert Intelligence Assets*. Congressional Research Service, Legal Sidebar, February 6, 2018. https://fas.org/sgp/crs/intel/LSB10072.pdf

Engelberg, Stephen. "Officials Think Spying Led to Death of C.I.A. Informant in Ghana." *The New York Times*, July 13, 1985, A6.

Frey, Linda S., and Marsha L. Frey. *The History of Diplomatic Immunity.* Columbus: Ohio State University Press, 1999.

Galdia, Marcus. *Lectures on Legal Linguistics.* Frankfurt: Peter Lang, 2017.

Gallagher, Sean. "ISIS Using Encrypted Apps for Communications; Former Intel Officials Blame Snowden." *Ars Technica*, November 16, 2015. http://www.arstechnica.com/ information-technology/2015/11/isis- encrypted-communications-with-paris-attackers-french-officials-say

Gentner, Dedre, and Francisco Maravilla. "Analogical Reasoning." In *The Routledge International Handbook of Thinking and Reasoning*, edited by Linden J. Ball and Valerie A. Thompson, 186-203. London: Routledge, 2018.

German, Mike, and Jay Stanley. *Drastic Measures Required: Congress Needs to Overhaul US Secrecy Laws and Increase Oversight of the Security Establishment.* New York: The American Civil Liberties Union, 2011.

Greenlee, Michael J. "National Security Letters and Intelligence Oversight." In *US National Security, Intelligence and Democracy: From the Church Committee to the War on Terror*, edited by Russell A. Miller, 184-204. London: Routledge, 2008.

Halliday, Josh. "MOD Serves News Outlets with D Notice Over Surveillance Leaks." *The Guardian*, June 18, 2013. https://www.theguardian.com/world/2013/jun/17/defence-d-bbc-media-censor-surveillance-security

Halpern, Diane F. *Thought & Knowledge: An Introduction to Critical Thinking.* 4th ed. Mahwah: Lawrence Erlbaum Associates, Publishers, 2003.

Harding, Luke. *The Snowden Files: The Inside Story of the World's Most Wanted Man.* London: Guardian Books, 2016.

Her Majesty's Government. *Security, Law Enforcement and Criminal Justice: A Future Partnership Paper*. September 18, 2017. https://www.gov.uk/government/publications/security-law-enforcement-and-criminal-justice-a-future-partnership-paper

Hoeken, Hans, Rian Timmers, and Peter Jan Schellens. "Arguing about Desirable Consequences: What Constitutes a Convincing Argument?" *Thinking & Reasoning* 18, no. 3 (2012): 394-416.

Holland, John H., Keith J Holyoak, Richard E Nisbett, and Paul R Thagard. *Induction: Processes of Inference, Learning, and Discovery.* Cambridge: The MIT Press, 1989.

Horwich, Paul. *Asymmetries in Time: Problems in the Philosophy of Science.* Cambridge: The MIT Press, 1987.

Hoy, David Couzens. *The Time of Our Lives: A Critical History of Temporality.* Cambridge: The MIT Press, 2009.

Jarvis, Lee. *Times of Terror: Discourse, Temporality, and the War on Terror.* Palgrave Macmillan 2009.

Jaszczolt, K. M. *Representing Time: An Essay on Temporality as Modality.* Oxford: Oxford University Press, 2009.

Jayyusi, Lena. *Categorization and the Moral Order.* Boston: Routledge & Kegan Paul, 1984.

Jones, Ihsmael. *The Human Factor: Inside the CIA's Dysfunctional Intelligence Culture*. New York: Encounter Books, 2008.

Kennedy, Gavin. *Adam Smith's Lost Legacy.* New York: Palgrave Macmillan, 2005.

Kitrosser, Heidi. "What If Daniel Ellsberg Hadn't Bothered?" *Indiana Law Review* 45 (2011): 89-129.

Lefébure, Antoine. *L'affaire Snowden : Comment les États-Unis Espionnent le Monde*, Paris: La Découverte, 2014.

Lefebvre, Stéphane. "Why Are State Secrets Protected from Disclosure? The Discourse of Secret Keepers." *The International Journal of Intelligence, Security & Public Affairs* 20, no. 3 (2018): 204-229.

Leigh, David, and Luke Harding. *Wikileaks: Inside Julian Assange's War on Secrecy.* New York: PublicAffairs, 2011.

Linklater, Andrew. "Cosmopolitan Citizenship." In *Handbook of Citizenship Studies*, edited by Engin F. Isin and Bryan S. Turner, 317-332. London: SAGE Publications, 2002.

Lowry, Ritchie P. "Toward a Sociology of Secrecy and Security Systems." In *Secrecy: A Cross-Cultural Perspective*, edited by Stanton K. Tefft, 297-316. New York: Human Sciences Press, 1980.

MacDonald, Malcolm N., and Duncan Hunter. "Security, Population and Governmentality: UK Counter-terrorism Discourse (2007-2011)." *Critical Approaches to Discourse Analysis across Disciplines* 7, no. 1 (2013): 123-140.

May, Jon, and Nigel Thrift. "Introduction." In *Timespace: Geographies of Temporality*, edited by Jon May and Nigel Thrift, 1-46. London: Routledge, 2001.

McCabe, Andrew. *The Threat: How the FBI Protects America in the Age of Terror and Trump.* New York: St. Martin's Press, 2019.

Melley, Timothey. *The Covert Sphere: Secrecy, Fiction, and the National Security State*. Ithaca: Cornell University Press, 2012.

Mitchell, Greg. *The Age of Wikileaks: From Collateral Murder to Cablegate (and Beyond).* New York: Sinclair Books, 2011.

Mitchell, Greg, and Kevin Gosztola. *Truth and Consequences: The US vs. Bradley Manning*, 2nd ed. New York: Sinclair Books, 2013.

Moberly, Richard. "Whistleblowers and the Obama Presidency: The National Security Dilemma." *Employee Rights and Employment Policy Journal* 16, no. 1 (2012): 51-141.

Monje, Scott C. *The Central Intelligence Agency: A Documentary History*. Westport: Greenwood Press, 2008.

Mudd, Philip. *Takedown: Inside the Hunt for Al Qaeda.* Philadelphia: University of Pennsylvania Press, 2013.

Nakashima, Ellen. "Pentagon: Undisclosed Wikileaks Documents 'Potentially' More Explosive." *The Washington Post*, August 11, 2010. http://voices.washingtonpost.com/checkpoint-washington/2010/08/pentagon_undisclosed_wikileak.html

Naughton, John. "If You Think These Spying Revelations Don't Matter, It's Time to Think Again." *The Observer*, June 23, 2013, 29. https://www.theguardian.com/commentisfree/2013/jun/22/gchq-internet-snooping-kafkaesque

Newell, Bryce Clayton. "Technopolicing, Surveillance, and Citizen Oversight: A Neorepublican Theory of Liberty and Information Control." *Government Information Quarterly* 31, no. 3 (2014): 421-431.

Nicks, Denver. *Private: Bradley Manning, Wikileaks, and the Biggest Exposure of Official Secrets in American History.* Chicago: Chicago Review Press, 2012.

Omand, Sir David. "Our Security and Intelligence Agencies Must Be Held To Account. But Without Secrecy, a Secret Service Cannot do its Job." *Independent on Sunday*, March 3, 2013, http://www.independent.co.uk/voices/commentators/our-security-and-intelligence-agencies-must-be-held-to-account-but-without-secrecy-a-secret-service-8517915.html

Otteson, James R. *Actual Ethics.* Cambridge: Cambridge University Press, 2006.

Peirce, Gareth. "Make Sure You Say That You Were Treated Properly." *London Review of Books* 31, no. 9, May 14, 2009, http://www.lrb.co.uk/v31/n09/gareth-peirce/make-sure-you-say-that-you-were-treated-properly

Perkins, Jared. "The State Secrets Privilege and the Abdication of Oversight." *Brigham Young University Journal of Public Law* 21 (2006): 235-265.

Persico, Joseph. "Company Man." *The New York Times*, May 4, 2003, http://www.nytimes. com/2003/05/04/ books/company-man.html

Plame Wilson, Valerie. *Fair Game: How a Top CIA Agent Was Betrayed by Her Own Government.* New York: Simon & Schuster Paperbacks, 2008.

Pozen, David E. "The Mosaic Theory, National Security, and the Freedom of Information Act." *Yale Law Journal* 115 (2005): 628-679.

Richelson, Jeffrey T. "Intelligence Secrets and Unauthorized Disclosures: Confronting Some Fundamental Issues." *International Journal of Intelligence and CounterIntelligence* 25, no. 4 (2012): 639-677.

Schmitt, Eric, and David E. Sanger, "Gates Cites Peril in Leak of Afghan War Logs by WikiLeaks." *The New York Times*, August 1, 2010, https://www.nytimes.com/2010/08/02/world/02wiki.html

Searle, John R. *Rationality in Action.* Cambridge: The MIT Press, 2001.

Shapiro, Jacob N. and David A. Siegel. "Is this Paper Dangerous? Balancing Secrecy and Openness in Counterterrorism." *Security Studies* 19 (2010): 66-98.

Shuy, Roger W. *The Language of Bribery Cases.* Oxford: Oxford University Press, 2013.

Smith, Michael R. *Advanced Legal Writing: Theories and Strategies in Persuasive Writing.* 3rd ed. New York: Wolters Kluwer Law and Business, 2013.

Smith, W. Thomas. Jr. *Encyclopedia of the Central Intelligence Agency.* New York: Facts on File, Inc., 2003.

Spitzmller, Jrgen, and Ingo H. Warnke. "Discourse as a 'Linguistic Object': Methodical and Methodological Delimitations." *Critical Discourse Studies* 8, no. 2 (2011): 75-94.

Stoler, Ann Laura. *Race and the Education of Desire.* Durham: Duke University Press 1994.

Stone, Richard. "Public Economic Policy: Adam Smith on What the State and Other Public Institutions Should and Should Not Do." In *Adam Smith's Legacy: Its Place in the Development of Modern Economics,* edited by Michael Fry, 65-84. London: Routledge, 1992.

"Terrorism Suspects Go Free 'Because MI5 Won't Let Spies Speak.'" *The Daily Telegraph*, March 20, 2013, 2.

Tetlock, Philip. "How to Win at Forecasting." In *Thinking: The New Science of Decision-Making, Problem-Solving and Prediction*, edited by John Brockman, 18-38. New York: Harper Perennial, 2013.

Thurschwell, Adam. "Reading the Law." In *The Rhetoric of Law*, edited by Austin Sarat and Thomas R. Kearns, 275-332. Ann Arbor: University of Michigan Press, 1996.

Tindale, Christopher W. *Fallacies and Argument Appraisal*. Cambridge: Cambridge University Press, 2007.

Tucker, Neely. "Bradley Manning: How Do We Weigh His Crimes?" *The Washington Post*, August 1, 2013, C1.

United States. *An Assessment of the Aldrich H. Ames Espionage Case and Its Implications for US Intelligence.* Senate Select Committee on Intelligence, 103rd Congress, Senate Print No. 103-90. Washington, DC: Government Printing Office, 1994.

___. *National Security Leaks and the Law: Hearing Before the Subcommittee on Crime, Terrorism, and Homeland Security of the Committee on the Judiciary, House of Representatives*, 112th Congress, Washington, DC: Government Printing Office, 2012. https://www.govinfo.gov/app/details/CHRG-112hhrg74977/CHRG-112hhrg74977

___. *The Senate Select Committee on Intelligence Report on Torture.* Brooklyn: Melville House, 2014.

United States, Senate Permanent Select Committee on Intelligence. *Requesting the President to Transmit to the House of Representatives Not Later Than 14 Days After the Date of the Adoption of this Resolution Documents in the Possession of the President Relating to the Disclosure of the Identity and Employment of Ms. Valerie Plame.* 109th Congress, House Report 109-228. Washington, DC: Government Printing Office, 2005.

Urban, Hugh B. "The Torment of Secrecy: Ethical and Epistemological Problems in the Study of Esoteric Traditions." *History of Religions* 37, no. 3 (1998): 209-248.

Waas, Murray, ed. *The United States v. I. Lewis Libby.* New York: Union Square Press, 2007.

Wacquant, Loïc. "Pratique, Pouvoir et Science: Quelques Clés Pour Comprendre Bourdieu." In *La Théorie Sociale Contemporaine*, edited by Razmig Keucheyan and Gérald Bronner. Paris: Presses universitaires de France, 2012.

Walters, William and Alex Luscombe, "Hannah Arendt and the Art of Secrecy; Or, the Fog of Cobra Mist." *International Political Sociology* 11 (2017): 5-20.

Walton, Douglas. *Fundamentals of Critical Argumentation*. Cambridge: Cambridge University Press, 2005.

Watt, Nicholas, Spencer Ackerman, Josh Halliday, and Rowena Mason. "US and Britain at odds as NSA Row Deepens." *The Guardian*, August 21, 2013, 1.

Weinreb, Lloyd L. *Legal Reason: The Use of Analogy in Legal Argument.* 2nd ed. Cambridge: Cambridge University Press, 2016.

Wells, Christina E. "*CIA v. Sims*: Mosaic Theory and Government Attitude." *Administrative Law Review* 58 (2006): 845-880.

Whitehead, Tom. "GCHQ Leaks 'Damaged UK Security and Risked Lives.'" *The Daily Telegraph*, October 10, 2013, 1. https://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/10367228/GCHQ-leaks-have-already-caused-real-damage-warns-security-adviser.html

Wilson, Joseph. *The Politics of Truth: Inside the Lies that Led to War and Betrayed My Wife's CIA Identity.* New York: Carroll & Graf Publishers, 2004.

"You're US Government Property." *The Economist*, November 12, 2016, special report, 8. https://www.economist.com/sites/default/files/20161112_espionage.pdf

Zarefsky, David. *Rhetorical Perspectives on Argumentation: Selected Essays by David Zarefsky.* Cham: Springer International Publishing Switzerland, 2014.

Legal Documents

American Civil Liberties Union v. CIA, Civil Action No. 1:10-cv-00436-RMC (DDC October 1, 2010) (Defendant CIA's First Motion for Summary Judgment).

American Civil Liberties Union v. CIA, Civil Action No. 1:10-cv-00436-RMC (DDC August 8, 2013) (Declaration of Martha M. Lutz, Chief of the Litigation Support Unit, Central Intelligence Agency).

American Civil Liberties Union v. CIA, Civil Action No. 1:10-cv-00436-RMC (DDC August 9, 2013) (Defendant CIA's Second Motion for Summary Judgment).

American Civil Liberties Union v. CIA, USCA Case #11-5320 (May 21, 2012) (Brief for Appellee).

American Civil Liberties Union v. Dept. of Justice, 681 (F 3d) 61 (2d Cir 2012).

American Civil Liberties Union v. Dept of Justice, 808 F Supp (2d) 280 (DC Cir 2011) (Affidavit of Ms. Cole, CIA's Information Review Officer).

Attorney General v. Guardian Newspapers Ltd (No.2), [1990] 1 AC 109.

Electronic Frontier Foundation v. Department of Justice, Case Civil No. 07-00403 (TFH) (D DC June 25, 2007) (Defendant's Opposition to Plaintiff's Motion for In Camera Review and Reply in Support of Defendant's Motion for Summary Judgment).

Electronic Frontier Foundation v. Department of Justice, Civil Action No. 12-1441-ABJ (April 1, 2013) (Memorandum of Points and Authorities in Support of the Department of Justice's Motion for Summary Judgment).

Electronic Privacy Information Center v. Office of the Director of Central Intelligence, Case No. 17-cv-0163 RC (D DC 26 June 2017) (Defendant's Memorandum of Points and Authorities in Support of Its Motion for Summary Judgment).

Franz Boening v. Central Intelligence Agency, Case 1:07-cv-00430-EGS (D DC July 20, 2007) (Memorandum of Points and Authorities in Support of Defendant's Motion to Dismiss Under Rule 12 and Motion for Summary Judgment Under Rule 56).

Gosling v. Secretary Of State For The Home Department, [2003] UKIT NSA4.

Her Majesty's Attorney General v. Guardian Newspapers Limited & Ors, [1987] UKHL 13, 14, [1987] 1 WLR 1248 (Lord Templeman).

Hitchens v. Secretary Of State For The Home Department, [2003] UKIT NSA5.

In Re Motion for Release of Court Records, Docket Number: MISC. 07-01 (Foreign Intelligence Surveillance Court [FISC] August 31, 2007) (Opposition to the American Civil Liberties Union's Motion for Release of Court Records).

Jefferson Morley v. Central Intelligence Agency, USCA Case #10-5161 (DC Cir 28 February 2012) (Brief for Appellee).

Larry Klayman v. Central Intelligence Agency, Civil Action No. 14-00472 RDM (D DC, June 3, 2015) (Declaration of Martha M. Lutz, Information Review Officer, Central Intelligence Agency).

Larson v Department of State, 565 F (3d) 857 (DC Cir 2009).

Laura Poitras v. United States Department of Justice, et. al., Case 1:15-cv-01091-KBJ (Declaration of David M Hardy).

Liberty (The National Council of Civil Liberties) v. The Government Communications Headquarters & Ors, [2014] UKIPTrib 13_77-H.

Mattathias Schwartz v. Department of Defense et al, Case 1:15-cv-07077-ARR-RLM (September 30, 2016) (Defendant's Memorandum of Law in Support of their Motion for Summary Judgment).

Ministry of Defence v. Information Commissioner and Evans [2007] UKIT EA_2006_0027 (20 July 2007).

Miranda v. Secretary of State for the Home Department & Ors [2014] EWHC 255 (Admin) (Affidavit of Mr Robbins, Deputy National Security Adviser for Intelligence, Security and Resilience).

National Security Archive v. Central Intelligence Agency, Case 1:11-cv-00724-GK (26 September 2011) (Defendant's Motion for Summary Judgment).

Secretary of State for the Home Department v. HM Senior Coroner for Surrey & Ors, [2016] EWHC 3001 (Admin).

Steven Aftergood v. Central Intelligence Agency, Civil Action No. 01-2524 (RMU) (DC) (Defendant's Cross-Motion for Summary Judgment, 15 September 2004).

United States v. Ishmael Jones, Civil Action No 1:10cv765-GBL-TRJ, (ED Va 2011) (Second Declaration of Mary Ellen Cole, Information Review Officer, National Clandestine Service, Central Intelligence Agency).

United States v. Ishmael Jones, Civil Action No 1:10cv765-GBL-TRJ (ED Va 2010) (Declaration of Ralph S DiMaio, Information Review Officer, National Clandestine Service, Central Intelligence Agency).

Wilner v. NSA, 592 (F3d) 60 (2d Cir 2009) (Affidavit from the National Security Agency).

Wilson v. CIA, 586 F(3d) 171 (2nd Cir 2009).