# Secrecy in the Age of Transparency

## An Investigation into Legitimations, Conceptions and Practices of Non-Disclosure

A dissertation presented by
Marlen Heide

Supervised by
Prof. Jean-Patrick Villeneuve

Submitted to the
Faculty of Communication Sciences
Università della Svizzera italiana

for the degree of
Ph.D. in Communication Sciences

August 2019

**Board**

Prof. Dr. Jean-Patrick Villeneuve, Università della Svizzera italiana (Thesis Supervisor)

Prof. Dr. Daniel Caron, École nationale d'administration publique (External Reviewer)

Prof. Dr. Tomasz Janowski, Gdańsk University of Technology (External Reviewer)

Prof. Dr. Bertil Cottier, Università della Svizzera italiana (Commission President)

Officially submitted to the Ph.D. committee of the Faculty of Communication Sciences, Università della Svizzera italiana, in August 2019. 

**Abstract**

The objective of this research is to illustrate the complexity and fluidity of the relationship between secrecy and transparency by considering the multiple rationales that serve to justify secrecy. The conceptual contribution of this thesis lies at two levels: (1) the reconceptualization of national security secrecy from realism to risk management and (2) the implications of such reconceptualization to the understanding of secrecy and transparency as antipodes.

The thesis takes an interdisciplinary perspective—drawing on conceptual contributions from the field of security studies—which has thus far not been comprehensively considered in research on national security secrecy. Consequently, the thesis explores how understanding of security itself determines secrecy practices and justifications.

The research perspective is decisively interpretive. Instead of accepting "security" as a universally accepted exemption to the norm of transparency, this analysis investigates both the rationales underlying it as well as their applications, thus providing a more nuanced understanding of the way in which secrecy might be legitimized. Hence, this thesis seeks to move beyond the narrow, positivist approach to the question of how boundaries between secrecy and transparency are negotiated in democracies.

Finally, the thesis also provides a comparative perspective on state secrecy. Most empirical evidence on secrecy provisions and practices is structured around the U.S. case. This lack of comparative perspective can be assumed to lead to a weak conceptualization of secrecy. This analysis focusses secrecy in a variety of additional contexts, especially considering classification frameworks that were subject to reform. Thus, the analysis provides a perspective on both temporal and spatial variation.

**Keywords:** *Secrecy, Security, Transparency, Legitimacy, Risk*

**Acknowledgement**

Writing this PhD thesis was a unique experience, combining both intellectual excitement and occasional doubts. Throughout the past years, I frequently relied on the support, guidance and patience of friends, family and colleagues. Their role in making this project a reality should not be unmentioned:

First and foremost, I would like to thank my thesis supervisor, Jean-Patrick Villeneuve for giving me the opportunity to do this research project. His support and open-mindedness provided the basis on which my ideas could thrive. Under his supervision, I was able to develop a project according to my interest, skills and career objectives. Moreover, he fostered the notion of a PhD as an opportunity for intellectual growth and made, thus, the journey of the past years an even richer experience.

Further, I would like to thank USI's equal opportunity service for welcoming me to their mentorship program and funding for my research stay in London in November 2017. My gratitude also goes to Ben Worthy, who has served as my academic mentor in this context and hosted me during my research stay at Birkbeck College (University of London). Our collaboration in an article project was one of the most valuable learning experiences during my PhD.

With Sofia Wickberg and Maarten Hillebrandt I shared research interests, the delight in open-ended discussions and multiple conference travels. Both lent their critical eyes to the early outline of my thesis project as well as the final papers included in this thesis. Their constructive comments have contributed to quality of my work and have consistently pushed me to think one step further.

My colleagues at the Università della Svizzera italiana have patiently lent their ear to my reflections and concerns throughout the thesis process, but also made my time in Lugano unforgettable: Giulia Mugellini, Nathaly Aya Pastrana, Maria Rikitianskaia, Rebecca Schaer, Rebecca Venema. The student assistants supporting of our team -

Michael Cautillo, Seline Girgis, and Yulia Maslova – were not only great office companions, but their provided invaluable support for my work.

Lastly, but most importantly, I would like to thank my partner Thomas, who supported me every step along the way and had my back on numerous occasions. Without him completing this project would not have been possible.

## Table of Contents

# List of Tables

## Summary

### *1. Foreword*

This thesis developed out of a desire to understand the complex, shifting, and often contradictory relationship between secrecy and transparency in contemporary democracies. The original intent was to determine the boundaries between the need for secrecy in security affairs and the normative imperative of transparency in democratic societies.

After an explorative review of available data sources, it became evident that a study of secrecy practices promised not only empirical insights but also provided the material for a more conceptual review of secrecy, challenging the conventional understanding of secrecy as a "necessary exemption" from the norm of transparency. Notably, recent reforms of classification frameworks in several countries suggest a changing rationalization of official secrecy, which in turn alternates its relation to transparency. These shifts suggest that the fluid relation between secrecy and transparency is subject to a changing understanding and legitimation.

Consequently, in the analytical framework of this study, the researcher opted for an interpretive approach, facilitating the exploration of the rationales provided for rendering secrecy justifiable in the age of transparency. The need for more interpretive research in the field was echoed during a European Science Foundation (ESF) workshop, *Government Transparency: Towards A Shared Understanding of a Fuzzy Concept*, which the researcher attended in June 2014. Here, transparency experts emphasized the need for more analysis of the "political rhetoric, public discourse and genealogical research" (Villeneuve et al., 2014, p. 3). The detailed analytical approach used in this project was then further developed through methodological workshops on interpretive methodologies and concept tracing during the Bamberg Winter Schools in 2015 and 2016, with the support of senior scholars in the field.

The research project positions itself within the body of critical transparency literature published in recent years, which challenges the notion of transparency as a universal good with the concept of secrecy as its opposite. Multiple authors have described transparency as an ambiguous concept that is often politicized and appropriated for strategic purposes by different actors, who themselves have diverging understandings of what is meant by transparency. Moreover, the boundaries between transparency and secrecy are frequently blurred. Transparency can create new forms of opacity or invisibility, while deliberate concealment might draw attention to sensitive information. This thesis seeks to contribute to these ongoing research efforts that aim to move away from an all too simplistic and normatively-charged understanding of what transparency entails and necessitates.

Finally, this study also reflects the professional path of the researcher herself, allowing her to combine a long-standing academic interest in security and defense affairs with professional experiences in transparency research and advocacy. This antecedent is clearly reflected in the interdisciplinary nature of the approach used, seeking to enrich research on secrecy with existing literature from the field of security studies.

### *2. Issues This Thesis Seeks to Address*

This thesis investigates the legitimation of government secrecy in the age of transparency. The current literature treats secrecy primarily as an exemption from the norm of openness and as a "necessary evil." Accordingly, transparency scholars and advocates are concerned with the scope and justification of national security exemptions or the ways in which secrecy can be contained and limited—in short, how an adequate balance between secrecy and transparency can be struck.

The analysis provided here seeks to broaden the debate on the relationship between transparency and secrecy, moving beyond the dominant understanding of them as antipodes. Instead, the boundaries between secrecy and transparency are in flux and subject to justification and reinterpretation.

Therefore, the analysis investigates a specific type of official secrecy, which has been labelled "national security secrecy" and refers to the idea of non-disclosure in support of security, safety, and provision of defense objectives. National security secrecy is one of the most prevalent and contested manifestation of official secrecy. The analysis critically examines the ways in which national security secrecy is legitimized—and how such legitimations change.

This thesis seeks to offer an interdisciplinary perspective on national security secrecy, marrying the academic field of transparency research with that of critical research in security studies. Zegart (cited in Quill, 2014, p. 7) notes that the study of secrecy is made all the more difficult by the fact that approaches to the topic tend to exclude elements from their respective analysis that, if considered together, would offer a more complete picture of secrecy and its effects on democracy. While legitimacy claims for national security secrecy frequently rely on the notion of security itself, the complexity of the concept of security is insufficiently considered in critical research in this field. Yet, the discipline of security studies has much to contribute to the debate on national security secrecy and its legitimacy within democracies. Moreover, both security practice and scholarship have diversified rapidly over the past three decades; the changing understanding of security, however, has been largely disregarded by the national security secrecy scholars. This analysis specifically considers risk security and its impact on secrecy practices and justifications.

Additionally, this thesis aims to contribute to the literature by taking a comparative approach. While official secrecy in general and national security secrecy in particular have been relatively well covered in academic literature, most contributions take the

United States system as a case study. Quill (2014, pp. 60-61) suggests that the emphasis on *balancing* security and liberty can be explained through the continued reference to this specific legal-administrative context. Following this critique, it can be assumed that secrecy would be rationalized, justified, and even contested differently in different countries. While the problem is noted in the literature, the scarce empirical evidence primarily comes from policy papers and practitioner research. Consequently, the analysis takes a comparative approach to provide a richer and more nuanced conceptualization of national security secrecy.

Finally, this thesis seeks to make a methodological contribution by investigating national security secrecy through interpretive methodologies. While multiple authors stress the need to consider the reasoning, justification, and sense-making of government secrecy, little to no empirical evidence has been generated in this regard. An interpretive approach to state secrecy allows for tracing how secrecy is rationalized and discursively legitimized in a practical context.

### *3. Answers This Thesis Offers*

This thesis situates itself within the body of critical transparency literature emerging in recent years (e.g., see Fenster, 2006, 2014, 2015; Flyverbom et al., 2015; Birchall, 2014). Through investigating "national security secrecy" as a prevalent and contested expression of official secrecy, it questions the current conceptualization of secrecy as an antipode to transparency.

The analysis draws extensively on critical security studies in order to obtain a better and more complex understanding of the concept of security itself. Thus, it touches the most sensitive aspects of scholarship on the issue: In what context can security concerns justifiably limit transparency? What forms and scope of secrecy are acceptable? In response, the thesis offers a more complex understanding of the dynamics of national security secrecy beyond the idea of a "necessary exemption." It

outlines the theoretical origins of some secrecy claims, thereby providing both scholars and transparency advocates with better judgement vis-à-vis secrecy legitimation motivated by governments and institutions.

Beyond disentangling the rationales for conventional secrecy provisions, the thesis explores to what extent and in what way the changing nature of security has altered the practices of secrecy in recent years. Notably, the shift toward "risk security" provides a fruitful entry point for the analysis. The selected case countries (United Kingdom, New Zealand, and Australia) have recently reformed classification frameworks. These "revamped" classification frameworks display risk management thermology and techniques to varying degrees. The analysis suggests novel classification practices challenge the conventional understanding of secrecy as separation between insiders and outsiders, protected and non-sensitive information. Instead, they reflect the increasing necessity for effective information management and comprehensive large-scale exploitation of information. This necessity stems, in part, from the expectation of transparency, digitization of bureaucracies, and information-based (security) governance.

### *4. Organization of the Thesis*

This thesis consists of a collection of articles, resulting from research that was conducted between 2015 and 2019 at the Institute for Public Communication at the Università della Svizzera italiana in Lugano, Switzerland. All articles have been presented at international workshops and conferences to an audience of experts in public administration and transparency research. Based on formal and informal peer-to-peer feedback, the research was adapted and reworked. The articles collected in this thesis have been submitted for publication in peer-reviewed journals.

The articles are sequenced in a logical order, starting with a critique of the current understanding of "national security secrecy" (Chapter 1), moving on to a proposal for

alternative conceptualizations of secrecy as risk (Chapter 2), and ending with an empirical comparison between multiple countries that have revised secrecy provisions alongside risk rationales (Chapter 3). While each article pursues a distinct analytical objective, their collection contributes to a common research objective—understanding the legitimation of secrecy in the age of transparency. The conclusion of the thesis draws on its analytical findings to critically question the conception of transparency and secrecy as opposing concepts.

*Summary, Table 1: Organisation of this thesis*

| Papers | Question | Contribution | Presentation[1] |
|---|---|---|---|
| **Chapter 1: Framing National Security Secrecy. A Conceptual Review** | Q1: Which rationales justify the "necessity claim" of official secrecy? | This paper disentangles three rationales embedded in the 'necessity claim' for secrecy: exceptionalism, policy implementation and national interest. Each rationale is related to transparency and accountability. | Presented at the Mancept Workshop, 2016, GCTR, 2017 |
| **Chapter 2: From Threat to Risk: Changing Rationales and Practices of Secrecy** | Q2: How do risk rationales alternate the conventional logic of national security secrecy? | The analysis builds on the recent shift from conventional 'realist' security to risk security. Comparing classification in two distinct security contexts (UK vs. Germany), it explores how risk thinking alternates secrecy practices. | Presented at the IRSPM 2017; GCTR, 2019 |
| **Chapter 3: Changing Patterns of Information Governance: A Comparative Analysis of Classification Frameworks** | Q3: How do classification reforms align in terms of objective, content and structural outcome across case countries? | Comparing three recently reformed classification frameworks (UK, Australia, New Zealand), the analysis investigates to what extent we can expect a newly emerging norm of risk secrecy more broadly. | Presented at the IRSPM 2017; CPSA Annual Conference 2019 |

[1] GCTR: Global Conference on Transparency Research
IRSPM: Annual Conference of the International Research Society for Public Management
CPSA: Canadian Political Science Association Annual Conference
Mancept Workshop: Annual Conference of the Manchester Centre for Political Theory

Prior to the presentation of articles, the document provides a general introduction to the research work, which includes a concise review of relevant literature and an identification of problems emerging from this review (‘Literature Review and Problem Setting’). This is followed by an outline of the analytical approach underlying the individual studies (‘Research Strategy’). The core research – consisting of three discreet research articles – is subsequently presented as Chapter 1-3.

Chapter 1 constitutes a critical literature review, confronting scholarly discourses on government secrecy, notably non-disclosure for national security purposes, with the pertinent literature from security studies. Specifically, the analysis seeks to discuss common assumptions about the necessity for secrecy with their conceptual roots. The analysis suggests that there is not a single rationale for national security secrecy, but different logics apply depending whether the perceived need for secrecy concerns decision-making, policy implementation or crisis response. More broadly, it becomes evident that arguments in favor of national security secrecy are heavily rooted within the realist school of international relations, rendering them both conceptually narrow and in need of revision vis-à-vis the current security discourses.

Chapter 2 builds directly on the criticism emerging from this initial analysis. Here, the analysis seeks to confront conventionally – realist-derived – assumptions about national security secrecy with more recent discourses within the security studies and policy-making itself, specifically the notion of risk-security. A conceptual and empirical comparison illustrates how a different conception of security itself might alternate the understanding and practice of secrecy in its support. The emergence of ‘risk secrecy’ challenges conventional assumptions about national security secrecy as outlined in Chapter 1. The analysis closes with an initial conceptualization of risk secrecy as well as its implications with regard the questions of transparency and accountability.

Chapter 3 builds upon the exploratory work regarding risk secrecy, investigating multiple cases that display patterns of secrecy governance determined by risk rationales. Here, the analysis examines recently reformed classification frameworks to identify common trends and patterns of secrecy governance. Building on the initial insights and conceptions from the previous chapter, this study provides a more in-depth and empirically broader understanding of national security secrecy in the age of risk and uncertainty.

The empirical findings and contributions emerging from the research in each chapter is summarized in the last section of this document (‘Thesis Conclusion’).

## Literature Review and Problem Setting

*This section provides a review of relevant literature in the field of transparency research and security studies, thus setting the stage for the research puzzle of this thesis. The section starts with an outline of the current prevalence of transparency in modern democratic governance, its assumptions and its roots. It then moves on to discussing more critical transparency literature, challenging the normative paradigm. The consequences for the understanding of secrecy as an antipode to transparency are outlined thereafter. The second part of this section takes on a specific case of state secrecy – national security secrecy – its rationales and underlying complexities. The review concludes that secrecy cannot merely be seen as an antipode of transparency and that secrecy on based on security considerations need to pay close attention to the understanding of 'security' itself.*

Throughout the past decades, the notion of openness and visibility increasingly influences the relationship between citizens and the state. By now, transparency is considered to be a "universally advocated public value" (Cooper, 2004, p. 400), challenging the conventionally protected, secretive areas of governance. Faced with citizens' decreasing trust of public institutions, their changing expectations about accountability or disclosure, and the data appetite of the information society, governments have opened up through incremental and, at times, radical reforms. The "transparency wave" that swept across public institutions around the globe can be traced through the implementation of freedom of information legislations, open data platforms, large-scale leaks, or various formats for citizen consultation and participation. It appears as a *sine qua non* that policy-making and implementation are open, inclusive, and accountable.

The rise of transparency as a necessary ingredient for modern governance presumes a specific assumption regarding concealment and opacity in public affairs—secrecy is primarily understood as the normative antipode of transparency, where "some important discussions of transparency and democratic accountability…typically start from the normative position that secrecy is undesirable and problematic" (Costas & Grey, 2014, p. 1425). The secrecy privileges of governments have come to be seen as a latent possibility for the mismanagement or abuse of information. "The link between secrecy and deceit is so strong in the minds of some that they mistakenly take all secrecy (especially when protected by silence) to be deceptive" (Bok, 1989, p. 7). Within the logic of good governance, secrecy is primarily associated with deviant behavior: corruption, mismanagement, and the citizens' declining trust of public institutions. "The use of state secrets appears both more pervasive in practice and more discredited in the public mind than at any point in history" (Pozen, 2010, p. 260).

The dualism between transparency and secrecy is already reflected in various definitions of transparency. Transparency has been described interchangeably as either "lifting the veil of secrecy" (Davis, 1998, p. 121) or the ability to "see through." (Albu & Flyverbom, 2016, p. 7) This definition entails the ambition to turn the black box of government into a glass house, allowing citizens to follow decision-making processes and scrutinize public officials. Transparency is expected to resolve the problems arising from government opacity; it is "thought of as a potent antidote to the mischiefs of power, such as inefficiency, fraud, and corruption" (Flyverbom et al., 2015, p. 386). Hence, Justice Brandeis is frequently cited for the claim that "sunlight is the best disinfectant." (cited in Meijer et al., 2015, p. 5)

### *1. Transparency as "the End of Secrecy"*

Transparency can be understood as a liberal-democratic reform project that sets out to cure the persistent ills of governance—from citizens' distrust in their governments and remote decision-making to inefficiency and corruption (Grimmelikhuijsen, 2012;

Birchall, 2014; Worthy, 2015). Consequently, public sector transparency enables both citizen participation in and control of public institutions. Meijer et al. (2015) have described the control function of transparency as *administrative transparency* "introduced to curb corruption and stimulates more efficient decision-making and public service delivery" (p. 3). Instead, participative logic is labelled as *transparency in the political realm*, which concerns itself with "the right to know, the contribution to a strong democracy, and checks and balances" (Meijer et al., p. 3). In many ways, transparency is perceived as a response to government secrecy and its negative effects.

Transparency, in the administrative realm, addresses the tendency of bureaucracies to hoard information, either out of risk aversion (Rourke, 1957, p. 540) or blame-avoidance (Hood, 2007). "Whether out of convenience or a dim suspicion that disclosure is intrinsically riskier than non-disclosure, government agencies always seem to err on the side of secrecy even when there is no obvious advantage to doing so" (Aftergood, 2009, pp. 402-403). Transparency allows bureaucratic actions, which are unethical or not aligned with public interest, to be detected and deterred. Detection allows the citizens to scrutinize and possibly sanction the behavior of potentially shirking officials. Deterrence is based on the idea that visibility is an effective tool for consciously reviewing the consequences of one's action. Bentham suggests that the possibility of being observed generates discipline amongst the observed:

> For why should we hide ourselves if we do not dread being seen? In proportion as it is desirable for improbity to shroud itself in darkness, in the same proportion is it desirable for innocence to walk in open day, for fear of being mistaken for her adversary. [...] The best project prepared in darkness, would excite more alarm than the worst, undertaken under the auspices of publicity. (cited in Baume & Papadopoulos, 2012, p. 12)

The control function of transparency is anchored in the principal-agent-theorem (Prat, 2005, 2006), which problematizes the asymmetry of power between two contract

parties. In the "social contract," the citizens (principals) entrust the public officials (agents) to govern for the benefit of public interest. However, as a result of the nature of the relationship, the agents have an information advantage over the principals, facilitating hiding and shirking behavior. This is equally true for bureaucracies, which "exist to control information and to exercise control *through* information and are secretive because secrecy is a means to both ends" (Weber, cited in McClean, 2011, pp. 58-59). Transparency reduces the asymmetry of information, allowing principals to monitor agents. Thus, transparency creates the precondition for accountability and for sanctioning non-compliance.

In contrast, transparency in the political realm is primarily associated with deliberative democratic theory, which promotes an active involvement of the public in decision-making processes. While state secrets (*arcana imperii*) were considered a legitimate dimension of political power for a long time (Horn, 2011), transparency challenges closed-door decision-making, smoke-filled rooms, or unaccountable leadership. Openness and access are the preconditions for generating a public sphere, a space in which the citizens can deliberate on socio-political issues. Essentially, "information access and exchange lie at the heart of deliberative democracy" (Jaeger & Burnett, 2005, p. 474). Transparency in the political realm is a distinct rejection of the trustee model of representation that perceives the governing elites as "wiser and more far-seeing than his constituents, and for this reason more fit to rule" (Mansbridge, 2009, p. 386). The trustee model entails a "disdain for the 'typical citizen', whose 'scant attention to matters that do not engage his 'immediate personal and pecuniary' would lead to poor political decision making" (Schumpeter, cited in Mansbridge, 2009, p. 387) In contrast, transparency in the political realm is "the embodiment of public control as an end in itself. Democracy, after all, is not about the people necessarily being right, but about the right of the people to be wrong" (Schauer, 2001, p. 1349). Thus, transparency in the political realm rejects governmental paternalism, favoring a

delegate model of representation instead, where elected officials work in close engagement with and are accountable to their constituency.

### *1.1. Conceptual Challenges*

While a strong normative understanding of transparency continues to dominate government reform projects, recent scholarship on transparency suggests that the promises and assumptions underlying it might be too simplistic. Different studies illustrate the shortcomings of transparency upon implementation as well as the weak conceptualization of the ideal more generally (Grimmelikhuijsen et al., 2013; Meijer & Curtin, 2006; de Fine Licht, 2014).

Multiple authors have pointed to the ambiguous meaning of transparency, allowing for a polyvalence of attributions and applications. "Underneath this universal veneer, transparency can be many things. Indeed, it is in some senses an 'empty signifier' that can be 'filled' by very different interpretations or emphasis" (Worthy, 2015).

Consequently, transparency can be appropriated by a variety of actors for different purposes—from government press departments to leakers. These actors most likely have very different understandings of the scope and acceptable practices of transparency. Meijer (2013) has described the alternating, speaker-dependent meaning of transparency as the cognitive dimension of transparency: "values such as democracy, privacy, and efficiency play key roles in the construction of government transparency, and these values are weighed and conceptualized differently by the various actors" (p. 432).

This ambiguity triggers vivid contestations, renegotiating the boundaries of legitimate transparency. The struggle with the meaning and potential contributions of transparency is politicized and ongoing (Fenster, 2015).

The conceptual ambiguity of transparency is also displayed in transparency practices. While strong and pervasive transparency narratives might function as moral beacons, disclosure dynamics, in reality, are much more complex and the benefits of transparency do not always hold (Meijer, 2016). Transparency provisions, it is argued, cannot prevent secrecy and might even create new, increasingly intangible forms of opacity (Teurlings & Stauff, 2014, p. 5). For instance, the unrestricted disclosure of information can overload audiences with uncontextualized data, "drowning" the recipients in information and, thus, reducing visibility. Likewise, deliberate concealment can enhance the attention that is paid to the very piece of information that is sought to be kept secret. (Heide & Worthy, 2019) Thus, "although it is relatively straightforward to define in general terms, transparency has extremely complex and often contradictory implications when applied to concrete situations, and it is possible for different kinds of transparency to be in conflict with one another" (McClean, 2011, p. 19).

Moreover, transparency is not an isolated concept, it is embedded within a wider framework of information management, i.e. administration's capacity to collect, systematize, store information. Effective information management is a precondition for enabling information provision (Caron & Bernardi, 2019). Thus, successful transparency builds – rather counterintuitively - upon information control.

Some authors even question whether transparency can be achieved at all. If, as many transparency scholars argue, information needs to be audience-sensitive and contextualized (O'Neill, 2006, p. 81; Naurin, 2007, p. 3), then the very process of mediation creates a specific representation of reality. Christensen and Cheney (2015, pp. 77-78) argue that "the call for transparency is essentially a rejection of established representation," assuming that some representations of reality are more intrinsically true than others or that representations of reality can be overcome altogether. Yet, the representative nature of information transfer is inescapable. In this respect, Teurlings and Stauff (2014) observe a disconnect between the transparency imperative to "lift

the veil" and expose the true nature of things—and the necessarily mediated character of transparency.

The conceptual and empirical criticism of transparency questions the conceptual understanding of secrecy as the antipode of transparency. It appears that the relationship between both concepts is much more complex, fluid, and intersubjective than conventionally understood. The boundaries between transparency and secrecy are subject to contestation, justification, and renegotiation. The present analysis draws on the critical transparency scholarship in order to investigate the changing legitimation of government secrecy in the age of transparency.

### *2. Official Secrecy and the Notion of National Security Secrecy*

While the spread of transparency reforms has been heralded as "the end of secrecy" (Florini, 1998), government secrecy persists even in fully developed democratic systems. It takes the form of classification frameworks, information privileges, or closed-door deliberations. There is a near-universal consensus that some secrecy measures are justified and necessary to protect authorized national security activities, permit confidential deliberations, or personal privacy (Aftergood, 2010). Even transparency statues acknowledge the role of secrecy for the conduct of governance: "All Freedom of Information Laws recognize that there are circumstances under which information should not be released because it would harm public or private interests" (Banisar, 2007, p. 223).

How can the persistence of secrecy be reconciled with the normative claim for transparency, which is so pervasive in current democracies? This thesis investigates the legitimation of government secrecy in the age of transparency through the case of "national security secrecy."

### *2.1. National Security Secrecy*

National security secrecy is one of the most prominent and notorious forms of official secrecy. It seeks to prevent the release of sensitive information to enemies and supports swift government action in times of crisis. Consequently, security concerns frequently serve as a driver for secrecy practices and regulations, either as a result of security anxiety or as a pretense to extend the governments' power. Secrecy, in the form of document classification, was introduced, formalized, and augmented in the face of an anticipated confrontation. The U.S. classification regime was initially established in the context of World War I, further developed during the World War II, and the Cold War (Relyea, 2003).

> Prior to the establishment of the National Archives in June 1934 by President Franklin D. Roosevelt, each federal agency was entirely responsible for the management and preservation of their records, and public access was a matter of ad hoc privilege—entirely unregulated and largely nonexistent. (Strickland, 2005, pp. 547-548)

Equally, the British Official Secrets Act of 1911 emerged from a war scare situation, representing "a spur-of-the-moment response to the exigencies of national security, framed on the belief that Britain would soon be at war with Germany" (Moran, 2014, p. 24). Similarly, the discourse on survival and threat imminence during the cold war period culminated in paramount degrees of paranoia and secrecy (Blanton, 2003).

The increasing expectation of transparency is also reflected in the case of national security secrecy, triggering vivid contestations over the scope and content of secrecy exceptions. The past two decades have been shaped by a tug-of-war between increased protection of security secrets and their—frequently unauthorized—disclosures. The aftermath of the 9/11 attacks was seen in the stark levels of secrecy, notably in the United States and their partner countries, reflected in an expansion of document classification and closure of some previously public processes. Several military allies

followed this example, enhancing secrecy provisions and practices (through the adaption of legal frameworks). In a backlash to excessive secrecy, recent years have also been marked by extensive revelation, especially of security-sensitive information, such as the Wikileaks' Afghan War Logs and Collateral Murder Footage in 2010 as well as Snowden's revelations of undue surveillance activities in 2013. The following sections present the rationales for national security secrecy, as discussed in the current literature, as well the contestations that challenge its legitimacy.

### *2.2. Challenging National Security Secrecy: A Question of Boundaries*

National security secrecy is generally perceived to be a legitimate exemption from the rule of openness. Even the precursor of modern transparency, Jeremy Bentham, conceded to secrecy in matters of national security, suggesting that publicity should be restrained if it furthers an enemy's project (Quill, 2014, p. 53). National security secrecy pertains to information that would, upon release, pose an identifiable threat to national security by compromising defense or foreign affairs. This is, according to Aftergood (2009, p. 402), a legitimate form of state secrecy: "Protection of such information is not controversial. These safeguards are the raison d'être of the classification system, and the public interest is served when this type of information remains secure." National security is, thus, "an important concern that may justify firm limits on governmental openness" (Curtin, 2014, p. 689).

While "national security secrecy" is considered a legitimate dimension of governance, there is an ongoing debate about how much secrecy is permissible and what kind of secrecy is acceptable. The challenge of the field lies in the distinction between legitimate and illegitimate secrecy (Pozen, 2010, p. 260). As Aftergood (2009) notes:

> If all government secrecy actions were uniformly bad or abusive, the public policy solution would be simple: to eliminate secrecy. If all government secrecy actions were necessary or prudent, no solution would be required, since there

> would be no problem. But in practice, government secrecy seems to be comprised of a shifting mix of the legitimate and the illegitimate. (p. 399)

Scholarly approaches to the dilemma between "necessary secrets" on the one hand and accountability and participation on the other have primarily suggested that an adequate balance could be achieved between openness and concealment.

The logic of balance is equally—or perhaps especially—applied to the security sector, where the dilemma is framed as one between liberty and security. In the words of Schoenfeld (2010, p. 220), a "central issues for a free society: the balance between freedom and order and, at core, whether or not a free society can protect itself." Nevertheless, when are security interests weighty enough to supersede transparency norms? The response to this and similar questions is ultimately context dependent, reflecting institutional factors, security concerns, and path dependency. Different countries display various oversight arrangements in establishing indirect transparency[2] and Freedom of Information laws differ with respect to the scope of and application to relevant security exemptions.

Moreover, the justifications for and the perceived legitimacy of national security secrecy can be expected to depend on the perspective from which a speaker is arguing. Fenster notes in this regard:

> Transparency proponents view secrecy as an inefficient and harmful bureaucratic practice whose overregulation of information flows demands correction. It is a correctable bug in the system, one that the right mix of legal and institutional reforms can fix by allowing information to flow to the public. (…) Secrecy's proponents view the issue from an opposite, though parallel,

[2] Different systems display accountability mechanisms to address the accountability–participation gap accruing from national security secrecy provisions. These include parliamentary committees with the right to access classified documents, parliamentary veto powers for military intervention decisions, ombudsmen to investigate deviances, etc.

> position. Their concern for national security, foreign relations, and law enforcement—and for allowing an autonomous, unitary executive to protect the flow of information—leads them to view secrecy as a crucial administrative goal. (2014, p. 314)

Thus, the balance between secrecy and transparency might not be subject to objective evaluation but, instead, to attribution, perspective of speakers, and interpretation. The perceived legitimacy of secrecy provisions depends on the justification for and acceptability of institutional arrangements and their practices.

In the case of national security secrecy, such legitimations can be contested based on the understanding of what security entails. Amiri points to the resulting problems:

> The polyvalent meaning of national security ultimately translates into an uncertainty what exactly constitutes information that are too sensitive to be disclosed: As there is no universally accepted definition of national security, there exists no common understanding of which kind of information may endanger national security if released. (2014, p. 20)

Consequently, the Global Principles on National Security and the Right to Information (Tshwane Principles) of 2013 suggest that "it is good practice for national security, where used to limit the right to information, to be defined precisely in a country's legal framework in a manner consistent with a democratic society" (Open Society Foundation, 2013, p. 14). In practice, however, justifications remain vague: "les récentes législations sur la transparence de l'administration…se contentent de formules vagues, sujettes à interprétation extensive" (*own translation:* Recent legislation for administrative transparency ... rely on vague phrasings and are, in consequence, subject to extensive interpretation.) (Cottier & Masson, 2013, p. 234).

The understanding of security constitutes a key aspect for scholars concerned with the question of how to moderate national security secrecy. A thorough engagement with

the concept of security is essential for a comprehensive appreciation of the challenges underlying "national security secrecy." However, it appears that research in the field rarely questions what constitutes security. In some ways, security essentially constitutes the elephant in the room in studies on state secrecy.

### *2.3. Security—The Elephant in the Room of National Security Secrecy*

The following sections introduce the concept of security by drawing on critical scholarship from the field of security studies. Thus, it sets the stage for a more critical reflection on the national security secrecy legitimation arguments, which are prevalent in both scholarly literature and policy practices. The specification of security is essential not only because the term is subject to significant redefinition over time and across contexts but also because it "has been used to justify suspending civil liberties, making war and massively reallocating resources" (Baldwin, 1997, p. 9). Therefore, state secrecy for the purpose of national security is directly related to the way in which security is perceived: "decisions to restrict information seem to depend on prevailing security considerations" (Aftergood, 2010, p. 839). Specifically, the following section outlines the realist rationales embedded in the prevailing justifications for national security secrecy and the questions that arise as a result.

### *2.4. Realism and National Security Secrecy*

In its most conventional understanding, security follows the realist tradition, which provides a state-centric understanding of security, determined by military rationales and the perceived need for survival. Here, the term "security" refers to the security of a nation from outside threats—guarding its political independence and territorial integrity. Guaranteeing security is the *raison d'etre* of governments. Building on Hobbes' claim that life without security would be "solitary, poore, nasty, brutish and short" (cited in Leterre, 2011, p. 442), the escape from conflict to a stable political

order is the genesis of the modern concept of security (Williams, 1998). “In anarchy, security is the highest end. Only if the survival is assured can states seek such other goals as tranquility, profit and power” (Waltz, 1979, p. 126). Hence, the goal of security enjoys primacy over other goals that a state might pursue because security is a prerequisite for the enjoyment of other values, such as prosperity and freedom. Thus, security in its conventional understanding supposes a state of peace that might be threatened and should be defended. Security is achieved when threats are prevented or at least managed (Nye, 1988) and force is the primary instrument used for achieving security. According to Lawrence Freedman (1998, p. 69):

> International security addresses questions of force: how to stop it, resists it, and occasionally threaten and even use it. It considers the conditions that encourage or discourage organised violence in international affairs and the conduct of all types of military activity. It therefore deals with the most fundamental questions of war and peace and so the highest responsibilities of government.

The realist rationale is also reflected in the conventional justifications for national security secrecy—this includes the primacy of security over other policy objectives, including transparency, accountability, and participation. For vital decisions and crisis response, the stakes are considered too high to allow uninformed reasons and tenacious debates to undermine the policy objective of security.

Thus, decision-making on security affairs is frequently shielded from normal democratic processes, reducing the scope available for scrutiny and participation. As a result, the idea of survival is prominent in conventional justifications for national security secrecy. It is argued that secrecy in governmental affairs is:

> an essential prerequisite of self-governance...and when one turns to the most fundamental business of democratic governance, namely, self-preservation – carried out through the conduct of foreign policy and the waging of war – the

> imperative of secrecy becomes critical, often a matter of survival. (Schoenfeld, 2010, p. 21)

National security secrecy also reflects the military rationale and the logic of force. It pertains to the importance of information control during conflict, which is emphasized throughout the history of strategy. Thucydides emphasizes the importance of intelligence in military planning and execution; Sun Tzu stresses foreknowledge and the employment of secret methodologies to undermine one's rival (cited in Quill, 2014, pp. 17-18). In wartime, as argued by Michael Herman (1996, p. 88), secrecy hides from adversaries that their plans have been detected and are being countered. Likewise, disclosure of technical data would promote the military capabilities of an adversary (Sunstein, 1986, p. 895). The work of intelligence services relies on the protection of sources and methods that are most vulnerable to counter-measures or manipulation (Chinen, 2009). "Concealing plans and vulnerabilities from adversaries, acting quickly and decisively against threats, protecting sources and methods of intelligence gathering, and investigating and enforcing the law against violators" (Pozen, 2010, p. 277) The protection of advanced military and technology intelligence, the current military operation plans, the identity of intelligence sources, and the confidential diplomatic initiatives constitutes what Aftergood (2009, p. 843) calls "genuine national security secrecy."

### *2.5. Security as an "Essentially Contested Concept"*

While the understanding of security in realist terms dominates the scholarly debate and political argumentations, the perspectives on security are more diverse and complex than suggested above. In his seminal article, Wolfers (1952) outlines the ambiguous nature of security by stating that:

> it would be an exaggeration to claim that the symbol of national security is nothing but a stimulus to semantic confusion, though closer analysis will show

> that if used without specifications it leaves room for more confusion than sound political counsel or scientific usage can afford. (p. 483)

The realist rationale of security has been widely discussed by security scholars, increasingly so since the 1980s. The majority of the literature refers back to Wolfers' article, which points to a variety of analytical problems underlying the question of security, thus challenging the conventional security rationale. Rival approaches suggest, for instance, an international, intersubjective, or constructivist understanding of security. This conceptual diversification has taken place against the backdrop of a changing security environment after Cold War, as new types of threats and security practices began to emerge. The broadened understanding of security is of immediate relevance to the study of national security secrecy. Some conceptual critiques brought forward against a strictly realist approach to security mirror the contestations around the legitimation of national security secrecy. The following sections discuss specific concerns and their implications for secrecy practices.

### *2.6. The Prescriptive Nature of Security: A Conceptual Critique*

In echoing Wolfers' original concerns, Rasmussen (2001, p. 286) suggests that theories of security are essentially praxeology—theories guiding action. It is not always clear whether statements about the importance of security as a goal are empirical observations or part of the security definition. Presenting security as a "vital interest" or "core value" suggests a normatively charged definition of security that does not allow for benchmarking security against other policy objectives. However, security is only one of many policy objectives, competing for scarce resources and being subject to the law of diminishing returns: "The national security mind-set will…make security trump even if the security gains are at best marginal or speculative, or a political performance designed to reassure us that we are doing something in the face of panic or unease" (Quill, 2014, p. 60).

With regard to secrecy, the primacy of security as a policy objective has frequently served as pretense to tip the balance in favor of secrecy. Quill concludes that:

> the balance metaphor has come to serve as one of those mind forged manacles.…I want to suggest that the question of balance isn't really a question at all, and in that sense, it is quite revealing. The balance metaphor contains in it, then, an implicit commitment to security over liberty. (2014, p. 43)

This is what is known as the "trump card of security" in the transparency literature (Wadham & Modi, 2003, p. 97), which is applied for justifying non-disclosure.

### *2.7. The Constructed Nature of Security: Normative Critique*

Constructivist security scholars have discussed the practical implications of a narrow, realist understanding of security. "Security theory must grasp an elementary but largely ignored proposition: security politics in general is organized by particular definitions of security, which constitute not only the practices that define threats, but also through which security is achieved" (Ciuta, 2009, p. 314). Constructivist scholars argue that the very term "security" is used as a signifier through which certain rules are applied to actions of force (Rasmussen, 2001, p. 287). The usage of security terminology (such as survival, threat, vital interest, or security as a term itself) moves an issue "out of the sphere of normal politics into the realm of emergency politics, where it can be dealt with swiftly and without the normal (democratic) rules and regulations of policy-making" (Taureck, 2006, p. 3). Thus, security does not exist as such but is represented and recognized in a discursive process. Huysman (1998), hence, describes security discourses as "a technique of government which retrieves the ordering force of the fear of violent death by a mythical replay of the variations of the Hobbesian state of nature" (p. 571). Information control and secrecy enhance this dynamic, allowing governments to present a unified, carefully constructed picture of

events so that public opinion follows the leaders' proposed path of action (Olmastroni, 2014; Sagar, 2012).

Moreover, the suspension of normal democratic processes during emergencies and crises, breeds the suspicion of deviances and, in fact, has frequently been abused. Security concerns frequently serve as a pretense for pursuing self-serving goals or concealing mismanagement. Deliberate abuse of information privileges for political advantage is "to advance a self-serving agenda, to evade controversy, or to thwart accountability. In extreme cases, political secrecy conceals violations of law and threatens the integrity of the political process itself" (Aftergood, 2009, p. 403). As shown by Gibbs (1995), through an analysis of several historical cases, bureaucratic politics and elite control of foreign policy-making are key motivators for non-transparency. Here, favoring secrecy over transparency can undermine the very objective of an exemption.

### *2.8. The Contextual Nature of Security: A Comparative Critique*

The realist understanding of "security" is mostly not sensitive to context. However, "what counts as normal or exceptional – not only what counts as a threat – is different in different contexts" (Ciuta, 2009, p. 313). According to Ciuta, the understanding of security reflects a state's history of security—from the genealogy of threats to strategic myths or culture (p. 317). Thus far, the field is dominated by U.S. scholarship, consequently proliferating concerns and discourses that pertain to a specific institutional environment. For instance, the question of balancing liberty and security reflects a country-specific concern of how to "contain" state prerogatives.

Beyond that, security is not only subject to national but also to temporal variations. Security has been differently defined during the pre- and post-Cold War periods; and it changed again in the aftermath of 9/11. The conventional notion of threat has been replaced by an array of determinants, ranging from vulnerabilities to challenges and

risks. Territorial, interstate conflicts were largely replaced by a defense paradigm focusing on hybrid, non-state threat actors and uncertainty. The changing security environment ultimately has implications on the practice of secrecy. It "requires a more open system where information is shared amongst a broader set of actors because potential targets are diffuse" (Chinen, 2009, p. 28). Conventional secrecy routines such as compartmentalization are thus increasingly challenged.

### *3. Research Implications*

Security is a highly ambiguous concept, which is thus subject to contestations, appropriations, and interpretations. "The idea that security can be reduced to objective and countable needs is conceptually enticing and politically problematic.…Thus, political actors can make plausible yet competing claims about security" (Stone 1999, p. 89). For normative and conceptual reasons, the debate on the legitimation of national security secrecy needs to pay attention to the contextuality of security and to the complex, politicized nature of the concept itself. Here, the research takes on board Quill's (2014, p. 58) fundamental critique of the idea that security and liberty can be adequately balanced: "A balance is a machine. And machine metaphors can be misleading because they offer the possibility of an accurate, technical solution to a messy (e.g. political) problem."

This thesis sets out to expand the understanding of national security secrecy beyond its conventional, realist understanding. For that purpose, it draws on critical security scholarship that has proven sensitive to the contextual changes in the notion of security itself. Recognizing the ultimately constructed nature of the necessity claims of security, the analysis applies an interpretive approach. It seeks to trace justifications and rationalizations of national security secrecy that form the basis for its legitimation.

## Research Strategy

### *1. Research Objective*

This thesis investigates the legitimation of government secrecy in the age of transparency. The analysis starts from the persisting contestations regarding the "necessity" and scope of exemptions from the norm of transparency, notably national security secrecy. Such contestations focus on the notion of security itself, raising questions regarding the usefulness of secrecy for a specific security policy or about whether security arguments serve as a pretext for limiting the scope of transparency and accountability. Recent scandals and security failures have further challenged the legitimacy of secrecy provisions.

The analysis traces the changing rationales through which non-disclosure is rendered legitimate. Here, legitimation is understood to provide "explanations and justifications of the salient elements of the institutional tradition. It explains the institutional order by ascribing cognitive validity to its objectivated meanings and justifies the institutional order by giving a normative dignity to its practical imperatives" (Luckmann & Berger, 1967, p. 111). The research approach, therefore, assumes the constructed, intersubjective, and contextual understanding of secrecy. It relies on interpretive methodologies to unwrap meanings and justifications provided for non-disclosure.

The analysis sets out to explore the rationalizations and justifications for national security secrecy provided from a "conventional" realist perspective and beyond. It takes classification frameworks in different countries as its main object of analysis, tracing differences between national contexts and changes over time with regard to the management of official secrecy.

The following section provides a systematic overview of the research approach, including methodological choices, data sources and structure of the work. Table 1, below, summarizes the general research strategy and the analytical approach taken to pursue the research objective.

*Research Strategy, Table 1: Overview of the Research Design*

| | |
|---|---|
| **Research Objective** | Tracing changes in the legitimation of state secrecy |
| **Case Study** | 'National security secrecy' as a case of state secrecy |
| **Level of Analysis** | Legal secrecy provisions at national level |
| **Unit of Analysis** | Classification Frameworks |
| **Analytical Approach** | Interpretive Methods |

## *2. Methodological Approach*

This research project explores the way in which "national security secrecy" is rationalized and, hence, legitimized. Legitimacy requires the state to justify its rights to impose requirements and to enforce them (Copp, 1999). In order to govern a certain field, it has to be "represented" in a way that enables it to enter the sphere of political calculation and deliberation. "A given power relationship is not legitimate because people believe in its legitimacy, but because it can be justified in terms of their beliefs" (Beetham, 1991, p. 11).

Therefore, tracing the rationalization of secrecy requires close attention to be paid to language, sense-making processes, and practices that render non-disclosure legitimate. Here, interpretive analysis serves to explore the rationales that shape actions and institutions. "Interpretivism is…centrally motivated by a concern to understand – and indeed to 'explain' – actions, practices and, if perhaps to a somewhat lesser extent, institutions" (Hay, 2011, p. 613).

Inasmuch as official secrecy represents a bureaucratic artefact, it needs to be constructed as a coherent tool for bureaucratic information management as well as justified vis-à-vis constituencies. Hence, the management of official secrecy is determined by rationales that are consented to and, thus, "naturalized."

It could be argued that the problem of official secrecy—how it can be justified against the norm of transparency—is, at its core, an interpretive problem. Much of the literature emphasizes the need to justify the choice for secrecy over transparency in governance affairs to achieve legitimacy. Thompson (1999), for instance, claims that "Secrecy is justifiable only if it is actually justified in a process that itself is not secret" (p. 185). Pasquier and Villeneuve (2007, pp. 158–159) suggest considering the reasons for non-disclosure provided by administrations. In a similar rationale, Chinen (2009, p. 41) promotes the notion that democratic values or processes can frame and legitimatize questions about secrecy. While these and other authors promote the reasoning, justification, and sense-making of secrecy rationales, little to no empirical evidence has been generated from an interpretive perspective on this question.[3] Instead, transparency research relies on a simplistic justification of national security secrecy that derives its legitimation from realist literature. How and whether government actors draw on realist rationales—or whether additional conceptualizations of security secrecy should be considered—is thus far under-researched. An interpretive approach to state secrecy allows for how secrecy is rationalized and discursively legitimized in a practical context to be traced.

The application of interpretive methods is further useful in a context where data is difficult to obtain. Benchmarking the levels of secrecy proves difficult even from a historical perspective because some secrets remain hidden even when the historic relevance has allegedly expired. Secrecy can also be highly entrenched so that even

[3] For a study on secrecy justifications in Europe, see Rittberger & Goetz, 2018. For a cross-country comparison of how states balance transparency provisions with justifications for secrecy, see Setty, 2009. Birchall (2011) examined secrecy rationales and attitudes in US politics.

most government insiders do not know that it exists. Interpretive research has several unique advantages in this regard. First, it is well suited to exploring hidden reasons behind complex, interrelated, or multifaceted social processes, where quantitative evidence may be biased, inaccurate, or otherwise difficult to obtain. Tracing the rationales displayed in the visible aspects of government secrecy allows secrecy researchers to glimpse into the sense-making of secrecy practices in states and institutions. Indeed, there is much explanatory power in a textual analysis that explores tacit knowledge implicit in policy documents and legal or regulatory frameworks.

> Policy makers customarily work within a framework of ideas and standards that specifies not only the goals of policy and the kind of instruments that can be used to attain them, but also the very nature of the problems they are meant to be addressing…[T]his framework is embedded in the very terminology through which policy makers communicate about their work, and it is influential precisely because so much of it is taken for granted and unamenable to scrutiny as a whole. (Hall, 1993, p. 279)

Finally, the ultimate objective of this study is to broaden conceptual understanding of official secrecy in the age of transparency. Interpretive research, taking an exploratory inductive approach, is uniquely suited to such an endeavor. While positivist research engages in theory and hypothesis testing, interpretive research seeks to contribute to theory building through a more flexible, open-ended approach in its research design. In recent years, interpretive analysis has been increasingly applied in administrative sciences and public policy studies to provide a novel perspective beyond positivist insights. According to Hay, "the last decade has seen a very significant 'interpretivist turn' in the fields of public policy and public administration" (2011, p. 167).

The study applies different analytical techniques to pursue this objective, particularly *frame-analysis* (van Hulst & Yanow, 2016; Rein & Schön, 1996; Goffmann, 1974; Benford & Snow, 2000) to explore the realist justification for "national security

secrecy" (Chapter 1); *analytics of government* (Dean, 1999) as an analysis of how risk rationales manifest in policy practice (Chapters 2), and finally *analysis of policy and institutional change* (Streeck & Thelen, 2005; Berman, 1995; Bennett & Howlett, 1992) both in its structural and ideational dimension (Chapter 3). The analysis draws on documentary analysis, specifically investigating secrecy provisions (classification frameworks) as a legislative justification for non-disclosure. Documentation is an established approach to interpretive research in which external and internal documents, such as memos, electronic mail, annual reports, financial statements, newspaper articles, and websites, may be used to cast further insight into the phenomenon of interest or to corroborate other forms of evidence.

In sum, the motivation for applying interpretive methods is threefold: (1) interpretive research allows for empirical engagement with the link between justification and legitimation of state secrecy; (2) interpretive research provides a way forward in settings in which data gathering is difficult and allows for engagement with available data in a meaningful way; and (3) interpretive research offers benefits specifically for exploratory, theory-building endeavors.

### *3. Data Sources*

The analysis takes classification frameworks as its main data source for understanding how states approach official secrets management. *Classification regimes* are determined by laws and regulation aimed at safeguarding documents, assets, and infrastructure sensitive to security. This includes the identification of vulnerabilities, the assignment of adequate secrecy level, as well as the prescriptions for adequate protection measures. A classification status might be temporal, allowing the release of "historic" data after a prescribed time period. Classification regimes are generally built on a need-to-know principle, limiting access as much as possible. Classification regimes are part of what has been described as *formal secrecy*: the "laws, rules, regulations and constitutions that govern what is to be kept secret and how, who can

be entrusted with secrets and what sanctions apply to secrecy breach" (Costas & Grey, 2014, p. 1431).

The choice of data—classification provisions—promises to provide novel insights, with scarce empirical research on such regulations, because "Until recently, even the rules and criteria for classifying and declassifying secret information were themselves secret" (Thompson, 1999, p. 181). Specifically, there is a lack of systematic comparison between the way in which countries construct official secrecy systems in general or classification regimes in particular.[4]

Moreover, several countries have reformed or overhauled their classification frameworks in the last two decades. Such changes have, at times, been so far-reaching that they have challenged the conventional understanding of state secrecy. Classification frameworks not only display the new structures and selection logics for information protection but also the management processes. The analysis does not only play close attention to the practices of secret keeping but also to the language with which secrecy is constructed and legitimized.

### *4. Dissertation Outline*

The chapters of this thesis mirror the three academic papers developed in its framework. They are sequenced logically, starting with a conceptual critique of current justifications of national security secrecy in the first chapter. The second chapter

[4] A notable exception is the investigation of legislations in several European countries, assembled by the Defense and Security Program of Transparency International (Földes, 2014). Furthermore, a monograph on *Secrecy and Liberty. National Security, Freedom of Expression and Access to Information* (Coliver et al., 1999) compiles single-country case studies that discuss official secrecy from a legal perspective. Finally, Banisar's (2007, pp. 217–235) contribution on oversight and national security discusses the question of official secrecy from a comparative legal perspective.

While these contributions provide useful analysis, they do not consider recent changes in classification regimes, notably reform waves in Anglo-Saxon countries throughout recent years. Further, they provide a comparison not from an academic perspective, but applied policy research, thus lacking a critical-conceptual dimension and more generally serving a different purpose.

introduces the logic of risk, exploring how the changing understanding of security changes secrecy practices. The notion of "risk secrecy" is further conceptualized in chapter three, where recently reformed classification frameworks are compared, and patterns of convergence are identified. Based on the reflections and findings presented in these chapters, the conclusion refers back to critical transparency scholarship, discussing the extent to which the emergence of "risk secrecy" challenges the understanding of secrecy and transparency as antipodes. The following paragraphs provide concise summaries of the chapters of this thesis and the concluding section:

*Chapter 1* investigates current theoretical assumptions regarding national security secrecy. This pertains, first and foremost, to the conceptualization of secrecy as an *exemption* and a *necessity*. Drawing on existing security studies, it traces the roots of conventional justifications for secrecy in security and defense affairs. Specifically, three justifications for national security secrecy are discussed—implementation of policies, exceptional circumstances, and national interest considerations. The chapter illustrates possible frictions, overlaps, and synergies between different rationales for national security secrecy.

*Chapter 2* takes up the conceptual critique provided in the preceding chapter. Based on recent literature from the security studies field, it introduces the logic of risk management by asking how the changing nature of security itself impacts the conceptualization of national security secrecy. Drawing on two cases that qualify as proponents of an either conventional or risk-centered approach to security, the analysis investigates classification frameworks as a prominent handle of national security secrecy.

The conclusion provides an entry point for discussion on how the legitimation of national security secrecy changes in the age of risk management.

*Chapter 3* provides a more comprehensive analysis of risk-based classification frameworks. It compares recent reforms of classification regimes in Anglo-Saxon

countries, tracing the similarities and differences with regard to drivers and outcomes of classification reforms. The analysis suggests an ongoing process of convergence, based on standardization, policy alignment, or lesson-drawing, even if some differences still persist and concrete applications of standards differ. This chapter provides a more comprehensive understanding of the changing rationales and practices of state secrecy.

*The conclusion* summarizes the findings from the conceptual and empirical analyses conducted in Chapters 1–3, reflecting the changing logics of state secrecy, from realism to risk, as identified through the case analysis. This section provides a more complex outlook on the relationship between transparency and secrecy, challenging their conventional understanding as antipodes. The conclusion embeds these findings into existing and ongoing research efforts that provide a more critical understanding of transparency. The thesis concludes with a perspective on the future research agenda for official secrecy that pays attention to the changing role of information in governance.

# Chapter 1: Framing National Security Secrecy: A Conceptual Review

*Authors:*

Marlen Heide, Jean-Patrick Villeneuve

Institute of Public Communication, Università della Svizzera italiana

***Abstract***

*This paper investigates justifications for the "necessity" of official secrecy, by tracing and structuring the rationales underlying it. Justifications will be traced through the case of "national security secrecy"; a prominent example of official secrecy. While the literature generally treats "national security secrecy" as unidimensional, this analysis demarcates multiple distinct rationales and investigates them based on literature from the field of military and security studies. Three justifications for national security secrecy are identified: implementation of policies, exceptional circumstances, national interest considerations.*

*The paper illustrates possible frictions, overlaps and synergies between different rationales for national security secrecy, thus broadening existing conceptualization away from transparency and secrecy as direct opposites. It further contributes to ongoing research on national security secrecy from a frame analysis perspective thus linking theories, justifications and practices of secrecy.*

**Keywords:** *Official Secrecy; National Security; Legitimation; Accountability*

## *1. Introduction*

The current governance literature considers secrecy as a deviance from conventional norms of openness and transparency. Academic discourses regularly start from the presumption that secrecy is undesirable and problematic. (Costas & Grey, 2014, p. 1425). It is considered to be the "flipside" of publicity and inasmuch as openness is heralded as a precondition for democracy, secrecy is assumed to undermine its very foundation. It entails closed-door decision-making, "smoke-filled rooms", unaccountable leadership or public interest defect. In short, secrecy is associated with deviant behaviour: corruption, mismanagement and declining trust of citizens in institutions and representatives (e.g. Birchall, 2014; Stiglitz,1999). As Woodrow Wilson famously declared "secrecy means impropriety" (Bok, 1989, p.8). However, secrecy in government affairs persists, for instance in form of exemption clauses in FOI legislations, classification regimes or information prerogatives.

The persistence of secrecy in the age of transparency is conventionally justified through the argument that some processes or policies require protection or concealment for them to be implemented at all (Thompson, 1999; Curtin, 2014). The question how to reconcile this "necessity" for secrecy with democratic norms of transparency and accountability constitutes a persisting problem in the field. One approach proposes to structure secrecy provisions narrowly and precisely to minimize their abuse (Coliver, 2012). Alternatively, authors suggest providing second order transparency, in other words, laying open the conditions and principles according to which concealment is applied (Thompson, 1999) or the establishment of oversight mechanisms that allow for indirect transparency and provision of accountability (Sagar, 2012). All these mechanisms have different strengths and weaknesses, which are sufficiently outlined in the literature, yet, both academic and policy-makers continue to struggle to establish what constitutes legitimate and illegitimate secrecy. (Pozen, 2010; Aftergood, 2009)

This article aims to trace the rationales underlying the "necessity claim" of official secrecy. Ultimately, the perceived legitimacy of secrecy can be expected to depend on perspective from which a speaker is arguing (Fenster, 2014). Transparency advocates will have a different understanding of what legitimate secrecy entails than most public officials. Within the current transparency norm, legitimizing secrecy certainly requires explaining why the state restricts the flow of information and by what concealment is enforced. Frequently, the "necessity claim" of secrecy is motivated to justify non-disclosure, this claim, however has a variety of reasonings underlying it. If, as Hurrelmann (2017) suggests, legitimation relies on broader political justification processes that occur in a society, it is of value to identify the roots of such justifications. Following Waldron (1993, p. 56), this analysis explores the common beliefs which may be appealed to in the justification of institutional arrangements, in this case official secrecy.

For reasons of feasibility, this analysis will focus on a specific type of government secrecy, which has been labelled "national security secrecy" (Aftergood, 2009), referring for the non-disclosure of information for the safeguard of security and safety and the provision of defence tasks. Safety, security and defence constitute regular exemption provisions within transparency legislations as well as providing the reason why classification regimes exist. While transparency scholars have frequently addressed the question of "national security secrecy", they rarely discuss the essence of security as a justification. The understanding of how security and secrecy relate remains relatively vague, a shortcoming that has been acknowledged by several authors. Amiri notes that polyvalent meaning of security causes an uncertainty which information require protection due to security reasons (2014, p. 20). Moreover, the restriction of information depends frequently on prevailing security considerations. (Aftergood, 2010)

## *2. Analytical Approach*

The analysis explores the rationales underlying the "necessity claim" of official secrecy, specifically national security secrecy, in order to (1) trace the roots of some commonly occurring legitimacy claims for secrecy; (2) map the multiplicity of rationales underlying the "necessity claim"; and (3) examine the ways in which these rationales might stand in contradiction to one-another. This analysis will provide an overview of problems underlying each rationale for secrecy and which solutions for accountability might apply. The discussion section of the paper takes a broader perspective, discussing the implications of the findings of this analysis for the conceptualisation of transparency and secrecy as mutual opposites.

This analysis reviews existing scholarship from the field of international relations, military or security studies. Not only does the literature in this field provide a nuanced approach to the concept of security itself, it also offers various discussions on national security secrecy such as on the role of public opinion in the use of military force, civil-military oversight and the role of information in warfare. The literature on "national security secrecy" have so far only selectively drawn on these insights; a systematic integration of security and secrecy research is so far missing.

Exploring the justifications of secrecy provided in the security studies literature will help understand what motivates policy makers to favour secrecy over transparency in questions of defence and security policy as well as justifications provided to the public. Rationales for national security secrecy identified in the literature review are treated as *frames*, defined as "implicit theories of a situation" (van Hulst & Yanow, 2016, p. 98). Findings are grouped into frames according to prevailing rationales for non-disclosure: emergency response triggering extraordinary measures, secrecy as a requirement for policy implementation and the idea that security is distinct from other policy fields, given that the stakes are higher.

Each rationale has been brought forward by policy-makers justifying non-disclosure, but they are equally reflected in the academic literature, that either critically engages with claims for security measures or finds supporting arguments. While all rationales are closely interrelated, the assumption underlying them are, as we will see in the analysis, quite distinct. Accordingly, the legitimacy claims for secrecy are to be challenges or granted on different grounds. Frame analysis presents a suitable approach for investigating the legitimacy of secrecy inasmuch as it addresses academic controversies that arise in policy analysis as well as the problems that emerge during policy practice. (Rein & Schön, 1996, p. 88). If legitimation entails explaining the institutional order by constituting cognitive validity and normative dignity to practical imperatives (Berger & Luckmann, 1967, p. 111), then framing provides the analytical entry point for understanding the cognitive structure that aim at interpreting the world (Goffmann, 1974, p. 10) as well as the patterns that make such interpretations persuasive to audiences (Benford & Snow, 2000).

### *3. Empirics*

This analysis identifies three possible justifications for the "necessity" national security secrecy. The first rationale justifies secrecy in the case of an immediate and exceptionally grave security threat, requiring extraordinary measures in response, including secrecy. In the following, this rationale will be labelled *exceptionalism frame* drawing primarily on critical security studies for its elaboration. The second justification is the need for secrecy needed to implement security and defence policies (hence, *implementation frame)*. References to this aspect of secrecy can be found in the field of military sociology that is concerned with the question how to bridge the gap between a pre-dominantly illiberal military world and a liberal democratic civilian world.

The third justification of secrecy is based on the idea that foreign and security policy is a complex field best dealt with by officials who have the necessary expertise to

decide what is in a country's interest. This rationale will be referred to as the *national interest frame.*

### *3.1. Exceptionalism Frame*

#### *(i) Theoretical Roots*

Exceptionalism is based on the view that security is a precondition for politics. Realists perceive of the world as an anarchic place (Elman & Jensen, 2014), building on Hobbes' claim that life without security would be "solitary, poore, nasty, brutish and short" (Leterre, 2011, p. 447). The escape from conflict to a stable political order is the genesis of the modern concept of security (Rasmussen, 2001, p. 287). Consequently, in times of crisis, when the survival of a polity is in jeopardy, normal democratic processes might be suspended, to give government a free hand for a decisive emergency response. Locke described the tension between a constitutional governments' need for a strong and extraordinary executive power in times of danger while also aiming to prevent the abuse of such power and bound the executive by the rule of law (Lowery, 2011, p.1341).

In more recent literature, the logic of exceptionalism is reflected by securitization scholars, who describe security as a speech act that motivates notions of survival or imminent threat to evoke an exemption from the normal bargaining processes of the political sphere. (Buzan, Waever & de Wilder, 1998, p. 4) Agamben (2004) famously described to the state of exception as a "no-man's-land between public law and political fact", referring to the difficulty of locating it between the democratic constitutional order and indeed the exception from it; analogous to the principle *necessitas legem non habet* (necessity has no law). The response to threat scenarios is a program of exceptional measures of which secrecy is a key component.

### *(ii) Justification for Secrecy*

Emergencies frequently prompt nations to free their executive authorities from many ordinary constraints (Schulhofer, 2010, p. 4). Crises constitute sudden and unpredictable events that may pose a danger to society and create high levels of uncertainty, confusion and time pressure. (Fleischer, 2013) They trigger emergency responses that suspend normal political processes and move into a narrower and constrained form of politics (Corry, 2012). Secrecy results on the one hand from the suspension of established norms such as openness, scrutiny and participation, due to heightened threat perception. Matters of urgency and survival are thought to justify an unhindered display of executive authority. (Loader & Walker, 2007, p. 206). Security calls for speedy action; thus, consulting, deliberation or judicial reviews are cut short to limit public interference upon executive decisions. (Aradau, 2004) Hence, crisis close down public debate and conflict by limiting the number of authorative actors and legitimate viewpoints. Secrecy here is a power tool, actively sought to allow assertive and speedy government action.

On the other hand, secrecy might emerge as a by-product of security crises, since government constitutes the main communicator on the situation, interpreting events and suggesting plans for action. Olmastroni (2014) suggests that the executive enjoys an information advantage during the early stages of conflicts and thus act not only as the maing source of information for the public, but also shape public opinion vis-à-vis the policy issue at hand. Due to this information advantage governments possess a decisive power for determining threats and putting issues on the security agenda, thus underlining established values such as participation, deliberation and accountability. Security restricts democratic political activity in the name of existential necessity.

### *(iii) Practical Examples*

The exceptionalism rationale is reflected in several legislations such as *state of emergency* provisions, which enable security through defence, policing and control. The age of terrorism is no stranger to the logic of exceptionalism in security affairs. In response to attacks and threats, recent years have seen a various example of democratic states pushing constitutional boundaries, evoking emergency provisions or introducing extraordinary measures in security affairs. Such emergency provisions also entail a limitation of public debates or media freedom.

### *(iv) Ensuing Problems*

The problem underlying the exceptionalism rationale of national security secrecy is that the constitution of security and urgency might be subject to interpretation. The criticism advanced by the Copenhagen School on Securitization referred to this very same problem when pointing out that security and exception can be constituted by a speech act. The problem of secrecy within the context of a national security rationalisation is that security serves as an ambulatory concept – meaning whatever it chooses to mean. (Dandeker, 1994) Security is described by Wadham and Modi (2003, p. 97) as the "trump card of secrecy". Quill (2014, p. 60) adds that the perspective of security professionals will conventionally emphasize security over liberty, even if security gains are at best marginal or speculative, since it is better to be safe than sorry.

### *(v) Solutions*

Some writers claim that accountability does not constitute a major concern in emergency settings, even if normal processes of transparency and control are suspended, since the actions of the executive are more visible during times of crisis,

thus constraining leaders' opportunities for aggrandizement (Posner & Vermeule, 2007, p. 155).

A different approach to the problem of secrecy during times of emergency is the temporal limitation of secrecy, thus providing for the control of decision-making and implementation after the fact (Sagar, 2012). Here, accountability is provided in retrospect. While the implementation of emergency measures is not hampered by the slowness of democratic processes or ex ante check and controls, decision-makers are not incentivized to shirk, since they know that they will be scrutinized later on in the process.

### *3.2. Implementation Frame*

#### *(i) Theoretical Roots*

The implementation frame pertains to the importance of information control in defence and intelligence affairs, which is emphasized throughout the history of strategy. Writers of military strategy, such as Thucydides emphasized the importance of information in military planning and execution (Quill, 2014, p. 17). Sun Tzu stresses foreknowledge and the employment of secret methodologies to undermine one's rival (Quill, 2014, p. 18). Even Jeremy Bentham, a fierce advocate of transparency, conceded to secrecy in matters of national security, suggesting that publicity should be restrained if it furthers the project of an enemy (Bok, 1989, p. 174).

#### *(ii) Justification for Secrecy*

Thompson (1999) has famously argued that some policies in order to be implemented need secrecy, or else they must be abandoned. Defence and security policy-making is probably the most prominent example of Thompson's argument. (Curtin, 2014) While publicity might not necessarily undermine the policy altogether, it can create

detrimental effects for the efficiency or performance in achieving a policy objective. (Mansbridge, 2009) Concretely, publicity might negatively affect defence and security policies in a variety of ways: On the one hand, publicity can compromise advantages vis-à-vis opponents. In wartime, as argued by Michael Herman, secrecy hides from the adversary that its plans have been detected and are being countered (1996, p. 88). In matters of security and defence, secrecy is claimed for concealing plans and vulnerabilities from adversaries. (Pozen, 2010, p. 277) Equally, the disclosure of technical data or tactical information can promote military capabilities of an adversary. (Sunstein, 1986, p. 895). Moreover, the implementation of security policies might be jeopardized by an enhanced vulnerability of security personnel or infrastructure (Sunstein, 1986, p. 895). For the case of intelligence services, this entails the protection of sources and methods – since they are most vulnerable to counter-measures or manipulation (Chinen, 2009). Finally, secrecy in intelligence and defence affairs is supported by the principle of plausible deniability: since national security involves at times questionable practices and even elected leaders should deny knowledge of these (Chinen, 2009, p. 14).

#### *(iii) Practical Examples*

Concrete manifestations of the implementation rationale of national security secrecy can be found in current and past military operations. For instance, the design of weapons of mass destructions as well as advanced military and technology intelligence is protected through secrecy. More recently, targeted killings through drones are conducted as “covert action”, meaning they not be acknowledged and rules of engagement are kept secret (Perkovich & Levite, 2017).

### *(iv) Ensuing Problems*

Information protection defence and security policy is deemed an essential component for policy implementation, but recent years have shown that secrecy can also have adverse effects, undermining its very purpose. The terrorist attacks of 9/11 appear to confirm this reasoning.

The investigation commission following the tragic events concluded that an excess of secrecy obstructed communication within government and thus undermined the effective prevention of the attacks. (Aftergood, 2010, p. 847). Consequently, it has been suggested that security, especially in times of terror, might benefit from information sharing and inclusion of actors rather than restricting access and compartmentalizing intelligence (Aldrich & Moran, 2018; Chinen, 2009)

Moreover, there is a challenge in cases where the implementation of security policies itself undermines existing laws or standards, such as in the case of human rights. Huntington (1957) points to the problem posed to democratic militaries to reconcile liberal standards of democracy with a largely illiberal world of the military.

### *(v) Solutions*

The implementation rationale of secrecy might be addressed through not direct observation but indirect control. This could take the form of oversight mechanisms and bodies. Thus, the appropriateness of the military measures applied might be monitored, without jeopardizing the effectiveness of a security policy. For a more general public participation in matters of security and defence, an open dialogue about policy aims and general tools acceptable can provide accountability and voice. In this regard, Mansbridge (2009) proposes a more communicative approach to transparency that entails giving reasons, explanations and facts, and improving notification.

*Transparency of rationale*, as she names it, allows for a transparency without necessarily undermining a policy's efficient implementation or objective.

### *3.3. National interest frame*

#### *(i) Theoretical Roots*

The justification for secrecy from a national interest perspective is embedded in the realist tradition of international relations scholarship. It assumes on the one hand that there is an objectively identifiable "national interest" and that the concern for that interest should be the paramount guide in the decision-making (Rasmussen, 2001). This interest might not align with common morality or public opinion but represent the best choice for the polity. Machiavelli has described politics as a dark art free from conventional morality and as such 'politicians need to learn how to be bad'.

#### *(ii) Justification for Secrecy*

While secrecy is not explicitly discussed in realist theory, much of the literature on secrecy takes an implicitly realist perspective. (Hill, 2011, p. 1290) In lieu of considering the recent critical discussions of the concept of security itself, those transparency and secrecy scholars, take a distinctively state-centric and aligned with military rationales. From that perspective, secrecy has two justifications within that rationale.

Firstly, secrecy is justified as a protection of governments against ebbs and flows of public opinion. Decision-makers need to be protected from popular pressures so that reason can guide their decision-making. Stakes might be too high to allow uninformed reasons to enter the debate. Ordinary citizens are considered to lack expertise to judge the nature and scope of threats, which is why they are unable to adequately weight their own security interests. (Ward, 2007, p. 38) Domestic public opinion in that sense

is seen as an obstacle to a state's pursuit of the genuine national interest, since it is led by emotionalism and does not exert constant, objective judgement (Knecht & Weatherford, 2006, p. 707) According to Morgenthau (1967, p. 142) it is the task of responsible leadership to form public opinion and not give in to its pressures.

Secondly, foreign and security policy making are considered "high politics", and thus subject to different considerations and processes than ordinary politics. Security is primarily seen as a privilege of the elite (Lippmann, 1955; Mearsheimer, 1990) inasmuch as questions of war and peace at the heart of sovereignty (Sagar, 2012, p. 10). Governments have better information about the dangers peoples face and resources necessary to respond (Ward, 2007, p. 40) The national interest rationale thus follows a trustee model of representation in which the trustee is wiser and more far-seeing than the constituents, and for this reason more fit to rule. (Mansbridge, 2009, p. 386) In identifying and pursuing the national interest, leadership is challenged by smaller, sectional interests. It is the obligation of the state to guard the interests of society, even if this involves disregarding particular domestic interests.

#### *(iii) Practical Examples*

A national interest rationale is underlying many provisions for prerogative powers. The United States state secrets privilege (also *executive privilege*) is the right of the state to refuse to produce evidence on the grounds that its disclosure would gravely harm national security. (Sagar, 2013, p. 41) The Supreme Court has repeatedly held that presidential claims of privilege are grounded in "military or diplomatic" consideration. In the UK decisions on the use of military force are part of the *royal prerogative* (crown privilege). In Germany prerogative powers are granted through the *Kernbereich exekutiver Eigenverantwortung* (core of executive responsibility).

### *(iv) Ensuing Problems*

The realist understanding of secrecy within a national interest framework is conventionally rejected for to its paternalistic approach to policy-making. Rose and Miller (2008, p. 59) suggest that the exercise of *raison d'etat* forces leaders' will upon a national space, thus opposing the fundaments of liberal democracy.

The claim that elite governance furthers better decision for the public at large is countered with the objection that small group decision making furthers group-think and power abuse (Chambers, 2004, p. 405; Janis, 1972)

Further, the power entrusted to government breeds the suspicion of deviances, and, in fact, has frequently been abused. Quill (2014, p. 30) notes that citizens as much – or even more – than external enemies are the primary target of secrecy measures. The protection of information for reasons of national security might be declared to motivate non-disclosure, however, as shown by Gibbs (1995) through an analysis of several cases, bureaucratic politics and elite control of foreign and security policy-making are the underlying reasons for non-transparency. Under the disguise of national security reasonings, citizens were led astray into conflicts that did not serve national interests and wasted national resources in unfruitful campaigns.

The understanding of security and defence policy as "high politics" suggests that some scholars are making the value of security a subject of its very definition. Security as a policy objective, however, needs to be distinguishable, yet comparable to other policy objectives (Baldwin, 1997), which is why the relative importance of security should be left open rather than built into the concept by using terms such as "vital interest" or "core values".

*(v) Solutions*

Recent conflicts faced by Western democracies have been described as "wars of choice" in lieu of past "wars of necessity" (Everts, 2002). They might require a more fundamental public discussion of foreign policy objectives and tools to be reasonably used in external relations. (Everts, 2002). If not integrated in the details of decision making, the public may set at least a "region of acceptability" that sets bounds on politically feasible options. (Knecht & Weatherford 2006, p. 707)

### *4. Frame Comparison*

The specification of frames in the previous section seeks to demonstrate that national security secrecy can be legitimatized not through one, but a variety of rationales in support of non-disclosure. Having disentangled the various secrecy rationales allows mapping the different assumptions underlying and consequences flowing from them. It illustrates that (1) national security secrecy can occur at different levels of the policy cycle; (2) each rationale promotes different types of accountability or participation and (3) national security secrecy can be legitimized in diverse ways, some of which are more contentious than others. This section relates different frames to one-another contrasting and problematizing specific assumptions incorporated in each frame. It should be noted that the secrecy rationales outlined in the empirical section are not mutually exclusive in a strict sense. The analysis identifies divergences as well as overlaps between implementation, national interest and the exceptionalism frame. Besides differences between all rationales, divergences also occur with regard to the commonly known conceptualization of secrecy as an antipode of transparency.

A major difference that emerges between the three secrecy rationales is the occurrence of secrecy. Within the exceptionalism rationale, secrecy is primarily contextual inasmuch as it is motivated by emergency and crisis. In contrast to that, the national interest frame links secrecy to a specific policy field. Finally, the implementations

frame links secrecy to specific policy activities. A further differentiation is the level at which secrecy occurs. The national interest frame primarily discusses secrecy in decision-making, whereby policy implementation is not per se excluded. The exceptionalism frame, justifying secrecy as a means for coercive and speedy action during crisis, implicitly refers to concealment in decision-making as well as implementation. The implementation frame, finally, locates secrecy during the implementation phase of a policy. A final distinction of secrecy is the way in which it is institutionalized.

The exceptionalism frame perceived of it as a temporary measure whereas the national interest frame structures the exemption more permanently. The implementation frame judged the need for secrecy on a case-by-case basis, depending on whether it serves a policy objective.

All three framings if national security secrecy grant different possibilities for public participation and exertion of accountability. Within an exceptionalism logic, secrecy is temporarily limited, allowing for ex-post accountability. Equally, the problems that emerge for participation and accountability are quite different in each rationale. If secrecy is intended to be temporarily limited due to an acute threat, the problem occurs once a security need – and hence a state of exception – is institutionalized. Equally, the implementation frame does not exclude the public from a debate. Rather, it allows for a participation in a general policy choice but does not provide details on the implementation (consent in general or the specificities of a policy). Secrecy within the implementation frame can be problematic when it is abused to cover failures or appears to be detrimental to the overall policy purpose or societal values. Within a national interest rationale, the public is *per se* marginalized as a contributor in questions of international affairs and security.

A final consideration are the differences between the ways in which secrecy is legitimized. The exceptionalism frame, for instance, would find the legitimacy for

secrecy in the social contract logic, which at its essence establishes representation as a means against a social world of violence and threat. Exceptionalism conceives of it as a precondition for a democratic – and hence transparent – order. Here, the idea of legitimacy is embedded within the idea of government itself. From an implementation perspective, secrecy is the consequence of specific policy choices, that require secrecy to be put to practice. The legitimacy of secrecy is derived from its necessity to implement policies legitimized previously. Moreover, certain practices or processes of security governance might be legitimized previously on a more general level.

Proponents of a national interest rationale would justify the need for secrecy as a means for prudence, rationality and stability in a complex and vital area of governance. From a national interest perspective, secrecy is justified by referring to expertise and experience of elected leaders.

What emerges from that is a quite distinct relationship between secrecy and democracy in all three rationales. The exceptionalism frame understands secrecy as a precondition of democracy; the implementation frame sees secrecy as a necessity for implementing democratic choices and finally, the national interest frame conceptualizes security as outside of democracy and secrecy thus as a protection against the downsides of democracy.

Table 1 below summarizes findings from the empirical section and the frame comparison, considering the understanding of secrecy, the role for public participation and accountability, the relationship between transparency and secrecy, the purpose of secrecy and most importantly, the legitimacy claim of secrecy.

Chapter 1, Table 1: *Summary of Results: Comparison of Secrecy Frames*

| **Frame** | **Conception of secrecy** | **Role of the Public** | **Relation of Transparency and Secrecy** | **Purpose of Secrecy** | **Legitimacy of Secrecy** |
|---|---|---|---|---|---|
| ***Exceptionalism Frame*** | Power function | Contextual limitation of the public's role during emergencies | Secrecy as a tool of emergencies is *above* democracy (incl. transparency) | Ensure speedy and concise government response in crisis | Hobbesian social contract: secrecy as a precondition for democracy |
| ***Implementation Frame*** | Instrument | Participation in policy decisions, limitation during policy implementation | Parallel instruments: weighing benefits of secrecy or transparency | Implementation of policy choices, thus pursue public interest | Through legitimation of ex-ante policy choices that necessitate secret action |
| ***National Interest Frame*** | Prerogative | Limitation of participation based on policy field (foreign and security affairs) | Instruments applied in separates spheres of politics | Maintenance of prudence and rationality in "high politics" | Expertise and experience of decision-makers (trustee model of representation) |

## *5. Implications*

The literature on government transparency, including critical publications, treat national security secrecy as a unidimensional phenomenon. From this perspective, tensions emerge between transparency proponents on the one hand and secrecy proponents on the other hand. The former are concerned with the scope of secrecy provisions, advocating the need for the containment and justification of exemptions. Secrecy proponents on the other hand, are concerned with national security or foreign relations, and thus value the executives' ability to control the access to information. (Fenster, 2014, p. 314)

*Theoretical Implications:* This analysis seeks to illustrate that this binary logic might be too simplistic. The perceived necessity for secrecy might be based on very different rationales. While different frames might ultimately support non-disclosure, secrecy frames might contradict one-another in their particular propositions and assumptions, such as the role of the public or objective of secrecy. Further, the tension between transparency and secrecy proponents might be better addressed at the level of such propositions and assumptions rather than the mere dichotomy between provision or non-provision of information.

*Practical Implications:* If national security secrecy constitutes a matter of 'necessity' as the prevalent literature on the topic puts it, one might ask what kind of necessity this claim refers to, i.e. specification at what level the necessity occurs: operational, politics, strategic. When accounting for the necessity of secrecy, such justifications should operate on the adequate level. As such, the present analysis is particularly valuable for transparency advocates, critically examining non-disclosure justifications for their adequacy and challenging secrecy claims on the level where argumentations are located.

From an official side, disentangling secrecy claims might be a valuable baseline for reflecting how secrecy can be minimized and which spaces for accountability and

transparency can be provided, even in times of security emergencies or operational needs.

*Implications for future research:* Finally, the analysis seeks to provide a basis for further investigating legitimation discourses that pertain to national security secrecy. It allows identifying dominant framings of national security secrecy e.g. in a cross-country comparison of secrecy practices, framing conflicts surrounding secrecy practices, and the strategic usage of specific frames by government actors. Moreover, a nuanced understanding of frames provides us with a specific understanding of rules and regulations that provide for government secrecy, such as the presence of absence of emergency or secrecy laws and the ways in which exemption regimes are conceptualized.

### *6. Limitations and next research steps*

The paper constitutes an initial literature review identifying linkages between common assumptions about national security secrecy and their conceptual roots in the security studies literature. The analysis remains thus at a conceptual-exploratory stage. Future research could investigate the workings of secrecy frames in practices and the way they are applied by policy makers. Alternatively, subsequent research could critically discuss the conceptual assumptions about conventional conceptions of national security secrecy vis-à-vis more recent security literature that provides different entry points to questions of legitimacy and legitimation, exploring whether and how these reflect in secrecy instruments.

## *7. Conclusion*

This paper contributes to ongoing research efforts that aim at better understanding the complexities of transparency and secrecy for legitimacy, accountability and democracy of governance (Fenster, 2006,2014,2015; Meijer, 2013; Worthy, 2015; O'Neill, 2006). Specifically, this analysis sought to provide a nuanced understanding of the role of secrecy, previously merely described as a flipside of transparency, inasmuch as transparency is understood as "lifting the veil of secrecy" (Davis, 1998, p. 121). While the literature and public discourse conventionally presents transparency and secrecy as binaries, both concepts are actually ambiguous, politicized and at times parallel, shaped by context and concrete interpretation. Disentangling national security secrecy done in this analysis points to ways in which the complex nature of government secrecy in general can be understood. Through the example of national security secrecy, this analysis illustrates that secrecy does not necessarily undermine accountability and legitimacy, but might, following other rationales, be perceived as a precondition for all benefits conventionally associated with transparency.

Transparency itself is not one dimensional and solely beneficial to democratic governance, but "laden with symbolic value, irrespective of their political significance" (Worthy, 2017, p. 2). This paper argues that future research might investigate secrecy not in relation to transparency, but instead focus on the dynamics, impact and structures of secrecy as a mechanism *per se*, thus by-passing any normative assumptions regarding its desirability. Instead, it might be beneficial to investigate secrecy as a governance instrument that exists in parallel to transparency, not in opposite. Here secrecy, just like transparency might be directed as values such as accountability or legitimacy.

More generally, this analysis might be a useful tool for practitioners and advocates of transparency to critically disentangle governments' claims for national security secrecy, identifying mismatches between rhetoric and concrete action.

Most frequently, diverse secrecy rationales are muddled together as one, for instance using an implementation rationale to justify secrecy at the decision-making level or needlessly transfer exceptionalism rationales to promote a more national interest rationale in the long term.

Another consideration this paper raises is the relevance of embedding questions of transparency, accountability or secrecy within the specific field to which they apply. As the example of national security secrecy shows, legitimations for concealment cannot be discussed in isolation, but might be embedded in the specific rationales of a sector and therefore other academic disciplines. Future research might need to take a more interdisciplinary perspective to fully appreciate the dynamics of good and accountable governance within specific policy fields.

Besides a more nuanced understanding of the relation between transparency and secrecy, this paper also sought to illustrate the central role of rationales and ideas that determine the way in which political legitimacy might be achieved. It includes the presence of prevailing narratives and rationalizations of national security secrecy that might determine the way in which transparency and secrecy operate in practice. Dominant rationales might be understood as tacit institutions in as much as they display system stabilizing functions, such as the idea of a "national interest" as a means to normalize foreign policy choices and generate support for international action.

## Chapter 2: From Threat to Risk: Changing Rationales and Practices of Secrecy

*Author:*

Marlen Heide, Institute of Public Communication, Università della Svizzera italiana

***Abstract***

*This paper explores how risk rationales affect and alter national security secrecy. While the transformation of defence and security policy has been widely discussed by security theorists, transparency scholars have not yet considered the notion of risk in their conceptualisations of national security secrecy. This paper draws on security studies literature to outline the divergences between conventional and risk-based security. The empirical section investigates how the difference between both rationales manifests in secrecy practices by investigating conventional and risk-based classification frameworks (in Germany vs. the United Kingdom).*

*In a risk security setting, information is increasingly seen as an asset and therefore subject to proactive management and exploitation. This requires a shift from a bureaucratic risk aversion in classification practices towards sharing, exploitation, and availability of information. Further, information governance is no longer about the separation between sensitive and non-sensitive information, but a comprehensive evaluation of all government assets for risks. These shifts ultimately change conventional understandings of secrecy as an 'exemption' and a 'necessity', requiring new debates about the legitimacy of secrecy practices.*

**Keywords:** *Risk, Secrecy, Security, Classification*

## *1. Introduction*

Over the past years, security scholars have noted that risk management techniques, such as screening, profiling, or precautionary measures, have increasingly determined security practices. Risk rationales often prevail over conventional 'realist' approaches to security. While the field of security studies has grappled extensively with these transformations (Aradau and Van Munster, 2007; Rasmussen, 2006), academic debates on national security secrecy have widely disregarded these transformations. Secrecy is routinely justified along realist lines as a 'necessity' and 'exception'. However, the emergence of risk rationales in security governance might provide fundamentally different responses to the question concerning what kind of and how much secrecy is legitimate and how to account for non-disclosure.

This paper explores the implications of risk rationales on the conceptualisation and problematisation of national security secrecy. At its outset, the dividing points between conventional security rationales and risk-security will be determined based on existing scholarship from the field of security studies. The empirical section contrasts secrecy practices in a conventional security context (Germany) versus a risk-security context (the UK). Applying an 'analytics of government' approach (Dean, 1999), the analysis investigates classification frameworks of both countries to trace 'regimes of practice', i.e. the way secrecy is conceived, represented, and managed. The paper concludes by discussing the implications of risk-security on the way in which national security secrecy is conceived and practiced.

The analysis finds that a risk-centred approach to security also changes secrecy practices. Classification is no longer only about the protection of sensitive information but also treats information as an asset for security governance. In consequence, information needs to be shared, exploited, and made readily available. This proactive approach to information management implies a departure from bureaucratic risk aversion.

Moreover, the shift from conventional national security secrecy to 'risk secrecy' also questions the conceptualisation of secrecy as an exemption: information governance in a risk setting is no longer about the separation between sensitive and non-sensitive information, but a comprehensive evaluation of all government assets for risks that are less-than-existential.

## *2. Problem Setting and the Objective of the Paper*

Secrecy represents a persistent problem in the scholarship on democratic governance. While openness and accountability are heralded as a *sine qua non*, even fierce transparency advocates concede to some exceptions to the norm of transparency (Coliver, 1998: 2). One of the most important exceptions is non-disclosure, or active concealment, in order to implement protective policies – measures concerning safety, security, and defence (Thompson, 1999; Curtin, 2014). This so-called 'national security secrecy' is embedded in the realist idea that security is an overarching societal value; it is a precondition for governance itself. Thus, security is "an important concern that may justify firm limits on governmental openness" (Curtin, 2014: 689).

While security serves as a constitutive element of exceptionalism, the conceptualisation and understanding of security itself poses a major challenge: "The polyvalent meaning of national security ultimately translates into an uncertainty what exactly constitutes information that are too sensitive to be disclosed: As there is no universally accepted definition of national security, there exists no common understanding of which kind of information may endanger national security if released" (Amiri, 2014: 20). In addressing this persistent question, scholars rarely draw on security studies for an adequate appreciation of security as a concept in itself or critical discourses on the notion of 'necessity' embedded in security claims.

Instead, contributions on the issue of 'national security secrecy' rely primarily on a realist conceptualisation of security, perpetuating the understanding of secrecy as a 'necessary exemption' from the norm of transparency. This paper provides an entry point for a more critical discussion on how the understanding of security relates to claims for secrecy, arguing that the increasing importance of risk rationales in security governance challenges conventional assumptions about secrecy.

The first part of the paper outlines the conceptual differences between conventional and risk-security rationales, drawing on a rich literature by critical security scholars that discusses the shift from exceptionalism towards risk management techniques in security governance (Rasmussen, 2001; Amoore and de Goede, 2008; Corry, 2014; Aradau, 2016). The empirical section of this paper compares secrecy in a country following largely conventional security rationales (Germany) and a country which adopted largely notions of risk-security (United Kingdom). The analysis of both cases determines if and how secrecy practices differ between these systems. The paper concludes with a discussion of the potential implications of risk security on the conceptualisation of national security secrecy. It proposes that, with the shift towards risk security, secrecy can no longer be thought of merely as an exemption from normal democratic rules, since risk-security thinking is not determined by the immediacy of crisis and threat.

### *3. National Security Secrecy and the Logic of Realist Security*[5]

While rarely made explicit, national security secrecy is primarily conceptualised along realist lines. Here, the notion of survival facilitates the idea of a 'necessary exception': during crises, decision-making and policy implementation might need to depart from otherwise established processes in order to safeguard the (democratic) system itself

[5] The insights on threat security draw on the discussion of exceptionalist security in Chpt. 1. As a cumulative thesis – each chapter representing and original paper – cross-references had to be limited.

(e.g. Ward, 2007; Schoenfeld, 2010). Security precedes other considerations of democratic systems, such as transparency and accountability of processes. Secrecy is a hallmark of the politics of exception (Corry, 2014: 248), limiting the number of authoritative speakers and facilitating speedy decision-making (Roe, 2012; Aradau, 2004). It provides strategic and technical advantages vis-à-vis opponents and reduces the vulnerabilities of the defence apparatus (Pozen, 2010; Fenster, 2014; Herman, 1996; Sunstein, 1986). Secrecy is considered legitimate, as it "works to protect information that would pose an identifiable threat to the security of the nation by compromising its defence or the conduct of its foreign relations. […] the public interest is served when this type of information remains secure" (Aftergood, 2009: 399). Thus, national security secrecy falls under the 'necessity rationale' for government secrecy, where information protection is required for policy implementation. (Curtin, 2014: 689). In fact, it could be argued that security governance is at the heart of the necessity rationale.

Critical International Relations scholarship, and securitisation theory in particular, provides a fruitful entry point for understanding how the exceptionalism of national security is constituted. Research from this field disentangles the rationales, practices, and language of realists' conceptualisation of security. Securitisation theory identifies the 'grammar of security', recurring patterns for the construction of threats in the form of adversaries that pose an imminent and existential threat to a valued referent object, classically a state (Buzan et al., 1998). Huysmans (1998: 571) describes securitisation as "a technique of government which retrieves the ordering force of the fear of violent death by a mythical replay of the variations of the Hobbesian state of nature." Key terms are 'existential threat', 'survival', 'urgency', or motivation of friend-enemy logics (Corry, 2014).

While conventional security along realist rationales has perpetuated secrecy practices throughout the past, recent scholarship from the field of security studies suggests that the notion of security itself is undergoing a fundamental transformation. After the Cold War, and especially in the wake of the War on Terror, security policy increasingly drew on risk rationales, thus changing strategic thinking but also the language in which security is considered. Discussions on the interdependencies between secrecy and security remain widely untouched by these changes, yet it would appear that the prevalence of risk security challenges these current conceptualisation of national security secrecy as an exemption to the democratic norm of transparency.

## *4. Risk-Security Rationales*

Recent years have seen a diffusion of risk logics within the field of security policy. Frequently, security scholars perceive risk-security as an extension of conventional security, making security more encompassing and thus extending state power (Bigo, 2012; Aradau, 2016). Others have argued that risk-security is effectively a departure from conventional security understandings (Corry, 2014). Both perspectives are unified in the assumption that risk security is no longer a matter of emergency politics, but routine procedures. In consequence, risk security undermines the way in which national security secrecy has been understood thus far.

### *4.1. Logic of Risk*

The term 'risk' refers to the probability of an adverse event of some magnitude (Hardy and Maguire, 2016: 80). Risk "implies the ex-ante possibility that things can go wrong or not turn out as expected" (Power, 2004: 60). Risk refers to anticipated hazards as opposed to immediate problems, since "the mode of existence of risks does not consist in being real but in becoming real" (Beck, 2009: 67).

Risk is conventionally conceptualised in opposition to the notion of uncertainty. Whereas uncertainty refers to the indeterminacy of the future and thus the limits of knowing, risk is a form of 'measurable uncertainty', inasmuch as it makes the future knowable through statistical and probabilistic reasoning. Risk "amalgamates knowledge with non-knowing within the semantic horizon of probability" (ibid.: 5). Risk has hence been described as 'calculative rationality' (O'Malley, 2010: 467).

Risk-thinking is pervasive, permeating diverse aspects of life, from insurance to business operations, health, and – indeed – security. Beck (1986) famously coined the term 'risk society' to describe the *zeitgeist* of late modernity. The idea of risk societies refers to the increasingly complex hazards that emerge as a by-product of modernisation and progress, from climate change to global financial operations. As such, the risk rationale assumes that the world is *de facto* increasingly unstable and hazardous, but it also affirms that this uncertain future must and can be managed.

Risk management, thus, engages in predicting and pre-empting future hazards by turning latent dangers ascertainable through sophisticated quantified modelling. In risk management, "forecasting, scenario analysis and actuarial science, provide the basis for calculative rational decisions on risk" (Hardy and Maguire, 2016: 86). Risk management techniques are seen as evidence-based and value free, inasmuch as they are guided by scientific methods and institutionalised procedures and techniques.

Besides this objectivist understanding, risk has been further described as a cognitive scheme through which these hazards are perceived. Ewald (1991) holds that nothing is a risk *per se*. Instead, the notion of risk is a form of rationalising and representing events: "risk is a way [...] of ordering reality […)] representing events in a certain form so they might be made governable in particular ways, with particular techniques and for particular goals. […]

What is important about risk is not risk itself. Rather it is: the forms of knowledge that make it thinkable" (Dean, 1999: 206). The experience of events as risks is not a given; instead, risks emerge as a result of mobilisation-specific rationales and institutions framing their authority in risk terms.

### *4.2. Risk Rationales in Security*

Risk security scholars argue that the concept of risk is also becoming an important determinant of security governance (Petersen, 2011: 703). Security discourses and practices are increasingly dominated by potential risks rather than imminent threats, survival, confrontation, and competition (Hammerstad and Boas, 2015: 478). Risk security emerged against the background of a new strategic environment after the Cold War. Territorial, inter-state conflicts were largely replaced by a defence paradigm focussing on "risks of international terrorism, nuclear proliferation, economic stability, organized crime, cyber-attacks, climate change and natural hazards, crisis management and protection of critical infrastructure" (Földes, 2014: 6). Beck (2009: 147f.) notes in this regard, "The 'old' wars of the twentieth century pitted states against states and armies against armies. This form of confrontation is in principle 'symmetrical' also in the sense that the actors – the states (governments, armed forces) – behave in predictable ways as regards the political goals and the threat potential (the military means)." New wars, or 'risk wars' as Beck labels them, "displace the violence exercised by the state and challenge, undermine and replace the state's monopoly of violence" (ibid.). Counter-terrorism campaigns conducted throughout the past years exemplify the increasing focus on hybrid, non-state threat actors in security governance, and thus reflect the changing patterns of security governance.

The core characteristic of a security risk compared to conventional security is the absence of an enemy doing the threatening, which de-personalises danger by describing attributes of a threat actor rather than actual enemies (Aradau et al., 2008: 148), such as the practice of risk profiling that identifies typical characteristics of

terrorists (Corry, 2012: 244). Thus, risk security tends to 'depersonalise danger' (Hammerstad and Boas, 2015: 278). Further, the language of risk highlights 'the conditions of possibility' wherein a risk could transform into actual harm (Hammerstad and Boas, 2015: 478). Conventional security "deals with direct causes of harm, whereas risk-security is oriented towards the conditions of possibility or constitutive causes of harm" (Corry, 2012: 235). While in a conventional understanding of security threats are tangible and instantaneous, risk security is turned towards the uncertain future.

This changing understanding of threats has in turn altered security governance itself, orienting it towards risk detection and prevention. The management of risk security relies on the security practices of precaution ('better safe than sorry') and pre-emption ('strike first'). For Rasmussen (2006: 109), the purpose of security policy is no longer to stop immediate threats but to filter particularly bad risks away. This translates to approaches such as screening, profiling, or proactive interventions being used in order to manage uncertainty and prevent the materialisation of threats (Aradau, 2016; Corry, 2014).

The turn towards detection and prevention changes the provision of security from emergency response towards bureaucratic routines (Hammerstad and Boas, 2015: 479; Aradau, 2016: 292); it has become a matter of long-term governance aimed at controlling uncertainty (Corry, 2012: 245). Krahmann points to the perpetual demands created by risk thinking: "Risks require permanent surveillance, analysis, assessment and mitigation [….] the potential range of imaginable risks is infinite" (2011: 356). The ubiquity and normalisation of security governance has, in turn, marginalised the question of survival, such that many current security practices deal with threats below the level of existential danger and survival (Corry, 2012: 244). Agamben notes that "in all of Western democracies, the declaration of the state of exception has gradually been replaced by an unprecedented generalization of the paradigm of security as the normal technique of the government" (2004: 14).

Against this background, critical security scholars have cautioned against the diffusion of security into the day-to-day business of government.

Finally, in late modernity, the state itself can be seen as originators of security challenges. In response, security governance has become 'reflexive' inasmuch as "the referent-object itself rather than an enemy becomes the primary target of risk programs" (Corry, 2014: 247). As such, risk management engages extensively in self-regulation, controlling and improving governmental mechanisms.

## *5. Analytical Approach*

### *5.1. Case Selection*

The analysis explores whether and how the shift from conventional to risk security has impacted secrecy practices by investigating two distinctive cases, each representing one of the two rationales: Germany and the United Kingdom. The selection was determined by the prevalence of risk and threat management language and techniques in security policy and governance more generally. The analysis of both cases determines if and how secrecy practices differ between the systems.

The adoption of risk governance in the UK was triggered by a number of crises, after which public sector organisations began importing management tools from the private sector (Power, 2004: 60). By now, the term 'risk' and 'at risk' are used in association with just about any routine event. In Germany, risk management techniques are slow to take place and implementation is rudimentary, which is caused by a lack of centralised planning as well as a lack of expertise in this field (Budäus and Hilgers, 2009).

The difference is also reflected in general practices of security governance. Germany generally counts as a late adopter of post-Cold War security environments. Frequently criticised for being slow in technical and strategic transformation, White Papers for

defence planning have only reluctantly taken on board new notions of security, starting as late as 2006. Despite a comprehensive project for the armed forces, their strategic mindset still points towards deterrence and territorial defence (Junk and Daase, 2013: 142). In the UK, the post-Cold War transformation happened faster and more efficiently than in other countries. Transformation efforts aimed at creating versatile forces, ready to be deployed on a global scale within short notice, a transformation that was concluded by 2004. The approach reflects risk rationales by using the "core risk−security terminology such as uncertainty, vulnerability, resilience, flexibility and preparedness" (Hammerstad and Boas, 2015: 482). Different authors also notice an increasing usage of the language of risk in the UK National Security Strategy, referring to the 'age of uncertainty' (2015: 484) and of 'new and unforeseen threats' (Aradau, 2016: 292).

Terminology, though not a perfect analogue, can thus be measured to isolate a country's position along a scale between absolute adoption of risk rationales and complete attachment to conventional rationales for security and governance, where the UK leans more towards the former and Germany to the latter. As other authors have noted, the UK, despite a comprehensive adoption of risk terminology, still shows patterns of conventional defence thinking (Hammerstad and Boas, 2015). Germany displays some adoption of risk rationales, with its 2016 strategic concept having emerged to be more vocal about 'new threats', like cyber security or economic threats, even if the usage of risk language remains scarce.

### *5.2. Data Analysis*

The analysis of secrecy systems in the UK and Germany will be guided by the main analytical question, "How do risk rationales alter the conventional logic of national security secrecy?". The analysis follows an 'analytics of government' approach. (Dean, 1999) Analytics of government investigates specific situations in which the activity of governing is 'problematised' – in this case, state secrecy.

The focus is not on the empirical activity of government, but rather on the organised practices through which a society is governed and governs itself (Lawlor and Nale, 2014). Against this background, this analysis investigates the rationales through which secrecy is rendered governable, tracing the principles that organise the selection and protection of sensitive information.

The analytics of government investigates 'regimes of practice', i.e. coherent, organised, and routine ways of going about governmental activities (Dean, 1999: 31). Regimes of practice include, for instance, how the sphere to be governed is conceived and represented, the forms of knowledge and techniques applied to specific governance problems, as well as the goals, outcomes, and consequences of governmental policies (ibid.: 32). Regimes of practice can thereby focus on specific policy problems or problematise institutional practices themselves (Rose & Miller, 1992), such as in the case of state secrecy. This analysis treats classification provisions – the most prominent technique of state secrecy – as a regime of practice and explores its mechanisms by determining types of information considered for classification, determinants of sensitivity, the objective of information protection, and the relation between classification and openness provisions.

Classification provisions are the main data source for this analysis, constituting the primary provision for state secrecy. Thus, the analysis refers primarily to the UK Government Security Classification (Version May 2018) and the German General Regulation for Material and Organizational Protection of Classified Documents (Verschlussachen-Anweisung). Governmentality analysis focusses on the routines of bureaucracy; theories, programs, knowledge, and expertise that composes a field to be governed and the ways of seeing and representing that field embedded in the practices of government. Thus, the approach takes policy papers, official publications, legal texts, and academic publications as its sources.

Analytics of government assumes that discourses on government are an integral part of the workings of government rather than simply a means of its legitimisation (Dean, 1999: 36). The analysis takes an interpretive approach, paying close attention to the language and problem representation applied in the abovementioned documents, and, specifically, whether and how threat and risk terminology are applied. Indicator terms such as threat, danger, mention of concrete threats, territorial defence, survival, etc. versus probability, risk, uncertainty, etc. are drawn from existing security studies literature, specifically securitisation and risk-security scholarship. Table 1 below summarises the analytical components identified in the previous section, which form the basis for the analysis:

*Chapter 2, Table 1: Analytical Components*

| | **Conventional Security** | **Risk Rationale** |
|---|---|---|
| **Conception of Security** | State-centric; political independence, territorial integrity; military logic; symmetrical threats | Constitutive conditions of harm; depersonalised danger; dispersed hazards; economic stability, organised crime, cyber-attacks, climate change |
| **Grammar of Security** | Threat, survival, enemy, urgency, imminence | Uncertainty, vulnerability, resilience, flexibility and preparedness |
| **Governance Techniques** | Security as a question of force; prevent threats; deter opponents | Bureaucratic routines of monitoring probability calculations, pre-emption, mitigation |

## *6. Empirical Section*

### *6.1. Selective vs. Comprehensive Approach to Secrecy*

The German approach to classification relies on the *ex-ante* specification of types of official information that qualify for protective marking. According to the regulatory framework pertaining to document classification, "protective markings concern

information related to external and internal security, foreign relations and third-party interests entrusted to the government" (BMI, 2006: 27).

Endangerments, damages, and disadvantages must be demonstrated conclusively and refer to concrete scenarios (ibid.). As a consequence of pre-selecting types of information that qualify for classification, non-sensitive information does not feature as part of the classification system. Thus, the majority of official information is left unmarked. The German classification regime reflects how security rationales motivate governments' information privilege, establishing a legitimate space for official action under the veil of secrecy. Further, information protection in the German case relates to a specific *field of governance*, i.e. activities in foreign and security policy, both of which are usually understood as 'high politics', in which the executive and military technocrats are granted a prerogative in decision-making.

A quite different approach to classification regimes is being pursued in the United Kingdom. Here, the official nature of a document might render it part of the classification system, not a specific threat or danger associated with it. The idea that the official nature of information constitutes its membership in a classification system does not presuppose an increase in official secrecy; rather, it points to a shift in understanding the instrumentality of official information altogether. The Government Security Classifications Policy refers to "all information that government collects, stores, processes, generates or shares" (UK Cabinet Office, 2018b: 3). Thus, the lowest level of classification, information marked as 'official', is applicable to "all routine public sector business, operations and services". The underlying understanding is one of risk management, as all government activities attract risks that "need to be assessed by government organisations so that they can make informed, practical and business enabling decisions" (UK Cabinet Office, 2018a: 5).

The difference between the German and UK approaches suggests a fundamental rethinking of national security secrecy. In the conventional approach, sensitive

information needs to be distinguished from non-sensitive information. The separation between secrets and non-secrets reflects the distinction between normal and exceptional politics within a conventional understanding of security.

It is here transferred to information management, inasmuch as *some* information from the bulk of public information is selected as worthy of protection, thus creating an exception to the norm of unprotected information. The risk management approach to information security assumes a liability of information *per se*, reflecting what risk authors have called a pervasiveness and perpetuation of information management outside of less-than-existential threats.

### *6.2. Degree of Sensitivity vs. Type of Sensitivity*

Both classification regimes apply a graded system in which the level of information sensitivity – and therefore secrecy – depends on the severity of harm which its unauthorised release might cause. Different, however, are the determinants of what constitutes harm in each case.

The German regulation considers the extent of damage inflicted upon national security, i.e. institutions, processes, and policies that comprise the system of defence and external relations for the country at large. The unauthorised release of classified information might either "endanger the existence of vital interests", "endanger security or severely damage the interests", "damage interests", or "create disadvantages" for the Federal Republic and the Länder, depending on whether they are classified as 'top secret', 'secret', 'confidential', or 'for official use only'. The logic applied here is one of gradation; the object of harm remains constant, while the gravity of harm magnifies. The German approach thus reflects a conventional logic in several regards, engaging a language of survival and national interest or escalatory language, pointedly described by securitisation theory.

The UK classification regime considers multiple factors in grading the sensitivity of information, such as areas of government activity, type of threat actors, as well as type of damage. For instance, information classified as 'top secret' might be the target of advanced state actors using significant technical, financial, and human resources. The consequence of unauthorised release would be, for instance, a wide-spread loss of life. The release of 'secret' information could damage military capabilities or the investigation of serious organised crime. Threat actors on this level are states or organised crime groups. Even official-level information displays vulnerabilities, being the target of hacktivists, single issue pressure groups, investigative journalists, competent individual hackers, and the majority of criminal individuals and groups (specified as attackers with bounded capabilities and resources). The undue release of such information might infringe upon the day-to-day business of government.

The distinction between both frameworks reflects the initially outlined distinction between conventional and risk security. Germany applies a system of signalling danger and sensitivity, thus pointing towards the escalating dynamics of emergency. Thereby, the threat itself is not specified, but is likely to change according to the prevailing security assessment. The UK approach takes up the language of escalation to some degree but moves beyond a gradation in terms of damage gravity. The classification stages take into consideration descriptive factors, such as types of threats to be expected as well as the concrete nature of the damage. Following Corry, "the key difference between risks and threats lies not so much directly in the perceived gravity of a danger or its imminence or the de-personalised nature of it but rather in *what kind of causality* a danger is constructed in terms of" (Corry, 2014: 246).

### *6.3. Information as a Liability vs. Information as an Asset*

While information protection is a natural aim of putting classification regimes into place, the comparative analysis suggests that the purpose and boundaries of information protection might vary. Broadly speaking, the objective of the German

classification system is the protection of sensitive information. In the UK, information protection is complemented and supported by proactive information management and effective exploitation of information. The difference of approach between both countries suggests a shift from risk aversion to risk management.

The divergence of both approaches is reflected already in the stated objective of the respective classification frameworks. The German guidelines set out to "provide material and organizational protection for classified information" (BMI, 2006: 2) and for "agencies and institutions working with classified documents to provide a protective framework as well as personnel with access to classified documents and thus have to consider protective measures" (ibid.). The UK classification scheme describes the "administrative system for the secure, timely and efficient sharing of information" (UK Cabinet Office, 2018b: 4). Further, the policy specifies how information assets are classified to "ensure they are appropriately protected, support Public Sector business and the effective exploitation of information" (ibid.: 3). The mention of 'national security' is notably avoided – thus departing from the conventional rationale for official secrecy.

The example of German classification systems treats information first and foremost as a liability. The UK classification system suggests that information is not only seen as a vulnerability as suggested by conventional security logics, but as an *asset* for anticipating and managing future risks, enhancing the governance capacity of information itself. In contrast to the German example, UK classification guidelines suggest that vulnerabilities are dispersed and in need of ongoing assessment and management. Further, the focus of information classification shifts from foreign and security policy to a wide array of hazards and vulnerabilities.

The emphasis of the German classification guidelines is placed on various measures to handle and protect sensitive information, thus providing a tool for official process management. The guidelines describe a system for documenting classification

activities, re- and declassification, infrastructure for information protection, and quality control that allows safe handling of sensitive information. Further, the guidelines assign authority not only for the production of classifications but also for the access of sensitive information, thus pointing to the notion of insiders and outsiders.

The classification guidelines in the UK and the German display some similarities, inasmuch as they provide a guide to handle, store, and protect sensitive information, designate authorities and responsibilities, or provide guidance for the identification and marking of sensitive information. However, the UK guidelines also serve as a tool for self-regulation, addressing the problem of over-classification and risk aversion. The guidelines caution that "applying too high a marking can inhibit sharing and lead to unnecessary and expensive protective controls" (UK Cabinet Office, 2018b: 13). Information management needs to be 'business-enabling': that means proactive and responsible, allowing not only for information protection, but also information availability and usage. The guidelines emphasise that "information needs to be trusted and available to the right people at the right time. The failure to share or exploit information can impede effective government business" (UK Cabinet Office, 2018b: 5). In consequence, UK officials are entrusted with the responsibility and accountability of information appropriation thus contributing to the broader task of government security.

Most importantly, the role of information appears to change: in conventional security, information is one component of security governance. In risk-security, information is seen as a means for constituting security. The former perceives of information as a vulnerability, the latter as an asset.

### *6.4. Secrecy Prerogative vs. Complementing Transparency and Secrecy*

The relationship between classification and access to information provisions is an essential component of information security. Both cases display fundamental differences in their perspectives on said relationship. While Germany mostly treats these as different areas of government, the UK approach could be described as 'two sides of the same coin'.

The UK classification places secrecy provisions within the framework of other applicable legislations, including the FOI law of 2000. Provisions for information disclosure and protection thereby exist in parallel:

> Classification markings can assist in assessing whether exemptions to the Freedom of Information Act 2000 (FOIA) may apply. However, it must be noted that each FOI request must be considered on its own merits and the classification in itself is not a justifiable reason for exemption. (UK Cabinet Office, 2018b: 15)

Thus, the classification status of a document does not immediately lead to its non-release.

The German classification framework makes no mention of the *Informationsfreiheitsgesetz* (IFG) that came into force in 2006. The IFG in turn entails a general exclusion of classified information from release in the case of Germany, pointing to an understanding of state prerogative in information protection. State secrecy provisions clearly override information access.

In the UK, the release or concealment of information is subject to continuous evaluation, balancing harm with interest for disclosure. Security exemptions are largely subject to an interest test: "To justify withholding information, the public

interest in maintaining the exemption would have to outweigh the public interest in disclosure" (ICO, 2017). Such assessments are not part of the German IGF law.

The German approach points to a system of legitimate exemption, hence an acknowledged power function of the state in a particular area of government. It provides a curated space for government and bureaucracies to operate in sensitive areas according to their best judgement. On the contrary, the UK classification system emphasises the continuous assessment and management of information for the benefit of performance and security of government operations. Information management here entails the diligent assessment of information through rigid guidelines as well as assessing potential lingering risks to a polity or constituency.

## *7. Summary of Findings*

The analysis set out to compare secrecy practices in a conventional security context versus one dominated by risk rationales. Table 2 below provides a summary of the points of comparison identified in the previous section:

*Chapter 2, Table 2: Summary of Empirical Results: Conceptions of Threat and Risk Secrecy*

| | **Threat Secrecy** | **Risk Secrecy** |
|---|---|---|
| **Conception of security secrecy** | Exception | Routine management |
| **Types of information considered** | High politics, vital interest | Includes also mid-level security |
| **Scope of information considered** | Selecting sensitive information | Comprehensive exploitation of information |
| **Approach to sensitive information** | Information as vulnerability | Information as assets |
| **Bureaucratic strategy** | Risk aversion | Proactive management of risk |
| **Relation to Openness** | Secrecy as prerogative | Complementarity |

As noted at the outset of this paper, risk security relies on monitoring, forecasting, and probability calculations – processes that rely on the availability and quality of data. As Seifert has noted, there are "high expectations for data mining, or factual data analysis, being an effective homeland security tool" (2004: 463). In contemporary security governance, "information is the key to victory" (Strickland et al., 2005: 436). The analysis in this paper suggests that an information-centred approach to security also alters secrecy practices. Data assessment is no longer limited to a few selected pieces of sensitive information, but all information features as part of the classification apparatus ('comprehensive approach'). Further, the classification regime is no longer only about the protection of sensitive information ('information as liability'), but the perception of information as an asset. This, of course, requires another approach to information management, ensuring the quality and availability of information for effective exploitation.

The adoption of risk management strategies for effective information management and exploitation also requires a departure from bureaucratic risk aversion towards a proactive management of risks. Bureaucracies have been described as secretive due to their tendency toward risk aversion, blame avoidance (Hood, 2007), and bureaucratic politics (McClean, 2011: 59). Such dynamics of bureaucratic secrecy can create intelligence failure and thus undermine security itself (Hitz and Weiss, 2004). Reforms to the UK classification system in 2014 were directly driven by this specific concern about risk aversion and blame avoidance. The new classification guidelines lay out that an "emphasis upon personal responsibility and accountability that underpins the new policy is a key feature" (UK Cabinet Office, 2018a: 2). Agencies should aim for "staff who are well trained to exercise good judgement, take responsibility and be accountable for the information they handle". This implies that, for information management to be effective, public sector staff need to be ready to take risks and responsibility. In many ways this demonstrates the reflexivity of risk. As Power (2004)

argues, public institutions are increasingly seen as being vulnerable to their own members and hence become the targets of risk management efforts.

## *8. Conclusion*

Risk secrecy challenges some of the commonly held assumptions about state secrecy as a whole, notably its understanding as the flipside of transparency. In many ways a risk-driven approach to managing sensitive information expands the scope of states' discretionary power with regard to disclosing or withholding information, since all government information feature as part of the classification system. Critical risk security scholars have cautioned that risk security techniques are a means to further expand state power – what Bigo (2012: 277) has called a "permanent state of emergency". For scholars, this raises conceptual questions as to the dichotomous understanding of transparency and secrecy, notably when boundaries between information release and information protection become blurred. For practitioners, this means an even closer focus on the specific justification of information protection and its adequacy within a given context, emphasizing the importance of not only classification rules, but also practice.

While risk secrecy set new challenges for evaluating the legitimacy of non-disclosure, it also opens new opportunities for accountability. The analysis in this paper suggests that in a risk-security setting, secrecy might no longer be understood as a prerogative of the bureaucracy, but itself subject to accountability. The UK classification framework, while still addressing the protection of sensitive information vis-à-vis outsiders, is also a tool for ensuring due process and effective management within the framework. This falls in line with Dean's observation that with the rise of risk management, the state's role to take

> …care of population and individuals is being partially displaced by, re-inscribed and recoded within another trajectory whereby the mechanisms of

> government themselves are subject to problematization, scrutiny and reformation. This turning of the state upon itself can be described as governmentalization of government. The result might be called reflexive government, which has to render governmental institutions and mechanisms, including those of the social itself efficient, accountable, transparency and democratic. (Dean, 1999: 193)

Thus, the concern about every-expanding state power only holds in part: while, for instance, the UK classification scheme is much more pervasive by encompassing all public information, the organisation of national security secrecy is equally subject to constant evaluation and re-evaluation (through harm and public interest tests). The disclosure of such logics of provision is equally creating a transparency of process. In consequence, it appears that the dichotomy between 'normal' democratic workings and exceptional measures (secrecy) does not hold any longer. Security and secrecy itself are subject to 'accountability'.

### *9. Limitations and Next Research Steps*

This exploratory study investigates a limited number of cases only, thus further analysis in needed to better understand potential trends within classification reforms and the applicability of patterns identified here. Such analysis should also move beyond the narrow focus of similar cases (Westminster democracies, Commonwealth countries, members of 5-Eye community), in order to see the wider relevance of observations made in this analysis – or conversely contrast them to other reform approaches. Further, longitudinal research is needed to trace the development of the reforms in present case countries, noting policy adaptations or changes across time. This is especially relevant since the present analysis constitutes a snap shot of reform efforts, but equally suggests that classification adaptations can be ongoing (see the case of Australia). Future analysis should also consider the implementation of new

classification frameworks, including emerging challenges and adaptation by different types of institutions.

Finally, it would be worthwhile to observe the implications and linkages between classification reforms and their consequences both upstream and downstream. Specifically, this entails consequences for document creation and records management (upstream) as well as provision of documents to the public (or not) downstream.

## Chapter 3: Changing Patterns of Information Governance: A Comparative Analysis of Classification Frameworks

*Authors:*

Marlen Heide, Jean-Patrick Villeneuve

Institute of Public Communication, Università della Svizzera italiana

***Abstract***

*This study examined recently reformed classification frameworks in the United Kingdom, Australia, and New Zealand to better understand the changing nature of state secrecy. The analysis investigated and compared drivers and outcomes of the classification reforms. Reforms across the case countries were driven by a variety of factors, such as administrative inefficiencies, new security risks, demands for accountability, and changing international standards. The structural modifications observed in case countries suggested a trend toward simplification and inclusiveness. Classification provisions also emphasize the proactive exploitation and efficient handling of information, implying a turn from bureaucratic risk aversion towards risk management. In conceptual terms, the changes induced by these reforms challenge the conventional understanding of state secrecy as a 'necessary exemption' from transparency and thus re-open debates about the legitimacy and accountability of non-disclosure.*

**Keywords:** *Information Security, Secrecy, Classification*

## *1. Introduction*

In recent years, the legitimacy of state secrecy has been re-discussed with new urgency. Whereas transparency advocates have criticized excessive information hoarding in the face of new security threats, security professionals have become increasingly concerned with the ability to use and control the vast amounts of information at their disposal. Expectations for transparency, large scale leaks, digitalization of bureaucracies, and the sprawling nature of the contemporary state have rendered information control more difficult to sustain and justify. Some scholars have thus referred to a "crisis of secrecy" (Aldrich & Moran, 2019, p. 93), "the end of secrecy" (Florini, 1998, p. 50), or the "implausibility of secrecy" (Fenster, 2014, p. 309).

This study explored the challenges facing state secrecy and their impact on secrecy practices. The analysis considered three countries that recently reformed their national framework for information classification: Australia, New Zealand, and the United Kingdom. It investigated how these countries responded—through structural adaptations and modified handling provisions – to the changing demands on public sector information management. The analysis took a comparative perspective to understand whether the case countries had similar motives for reform and how the outcomes of the reforms compared. In many ways, the structures and practices of information governance introduced through these reforms put into question conventional conceptions of state secrecy.

### *1.1. Problem Setting*

Information is an essential tool and resource of government (Hood, 1983), and a considerable part of government activity is founded on the production, collection, processing, analysis, dissemination, protection, disposal, and long-term retention of information (Caron, 2017). According to Brown and Toze (2017), "The nature of a

government's information holdings—of what it knows—is as complex as government itself, providing its memory, on the one hand, and raw material for its current and future activities on the other" (p. 583). Information control, notably in the form of administrative secrecy, is of particular concern for information governance. It is, for instance, thought to be indispensable for decision-making processes and the implementation of certain policies to a degree that "some policies, if they were made public, could not be carried out as effectively or at all" (Thompson, 1999, p. 182).

Information control is essential for security governance. Throughout recent years, the role of information further has heightened (Caron & Bernardi, 2019), as security governance increasingly engaged in forecasting and monitoring security risks. The anticipation and pre-emption of threats have come to be seen as an important response to a new, more complex security environment, rendering security governance more knowledge- and data-intensive (Amoore, 2011). According to Doty (2015), "We might reasonably say that there is a general belief among policy makers [...] that 'information is the key to victory'" (p. 349).

The need to monitor and exploit information requires states to adapt their internal management of sensitive information. Previously, intelligence agencies relied heavily on compartmentalization of information. However, the dispersion and complexity of risks requires a broader variety of information to be considered for security purposes.

As a result, security governance by now also requires sharing and exchanging of information: "Unlike during the Cold War, secrets relating to security no longer belong to a few specialized government agencies and departments" (Aldrich & Moran, 2019, p. 96). Now, secrets are dispersed among the government and contractors.

However, the scope and distribution of security-relevant information are also perceived as liabilities. Recent years have seen several unauthorized releases of large-scale data by low-level staff with access to sensitive information, such as in the cases of Wikileaks and Edward Snowden: "The state had granted or enabled access to

information to officials; the officials grew disillusioned and took advantage of their access to copy classified documents" (Fenster, 2014, p. 328). These leaks were supported by a technological infrastructure that accelerated the quantity of disclosed information as well as the rapidity of its circulation. According to Roberts (2012), "A generation ago, leaking was limited by the need to physically copy and smuggle actual documents. Now it is a matter of dragging, dropping, and clicking send" (p. 117). Such leakages raise not only questions about technological vulnerabilities and scale of damage but also the "normalization" of circumventing state secrecy.

The challenges facing state secrecy might explain the recent, ongoing, and sometimes far-reaching reforms of classification frameworks. States—especially in the Anglo-Saxon world—have responded by modifying and, at times, overhauling their classification structures and guidelines. Therefore, this analysis used such reforms as its main analytical handle to explore the changing nature of state secrecy.

### *1.2. Research Objective*

This study examined recently reformed classification frameworks in the United Kingdom, Australia, and New Zealand to better understand the changing nature of state secrecy. The analysis investigated the *drivers* and *outcomes* of the classification reforms in each country. Regarding reform outcomes, the analysis considered structural changes induced by reforms, as well as the rationales and guidelines for handling sensitive information. Furthermore, the analysis compared how much the reform approaches displayed similarity across cases. The following research questions guided the analysis:

***RQ1: What factors drove reforms of classification frameworks?***

***RQ2: What structural changes and handling provisions were introduced by the reforms?***

*RQ2.1: Did the reforms introduce major changes or incremental adaptations?*

*RQ2.2: How did the countries compare in terms of objectives and outcomes of reforms?*

The conclusion of this paper discusses how these classification reforms can alter the conception of state secrecy and which questions emerged regarding the legitimacy and accountability of non-disclosure.

## *2. Methodology*

The analysis compared how recent reforms altered the structure, rationales, and practices of information classification, exploring the changing nature of state secrecy. The United Kingdom, Australia, and New Zealand provided suitable case studies for that purpose, and the literature on policy and institutional change provided the analytical backdrop for the study.

### *2.1. Data Sources*

This analysis used classification provisions—regulatory frameworks for the protection of sensitive information—as its primary data source. In essence, classification refers to the marking of official documents to indicate their protected status (Relyea, 2003). Classification provisions formalize what constitutes sensitive information and attribute levels of confidentiality to different types of sensitive information. Furthermore, classification provisions assign responsibilities for the management of sensitive information. Classification provisions are thus part of what has been described as *formal secrecy*: "laws, rules, regulations, and constitutions that govern what is to be kept secret and how, who can be entrusted with secrets, and what sanctions apply to secrecy breach" (Costas & Grey, 2014, p. 1431).

This study analyzed policy and regulatory documents that organize the document classification system at the national level for all three countries. For New Zealand, the analysis was based on the *Government Security Classification System* (NZ DPMC, 2018a, 2018b, 2018c), which was initially introduced in 2000 and the *Protective Security Requirements* (NZ DPMC, 2018d, 2018e) and *Information Security Management Protocol* (NZ DPMC, 2018f), both of which constitute the basis for classification management. Additionally, a 2018 report by the Inspector-General of Intelligence and Security was considered that reviewed the current classification system and provided suggestions for future reforms (Gwyn, 2018). The United Kingdom's *Government Security Classification Scheme* was reformed in 2014; however, this analysis used the slightly updated version of the scheme released in 2018 (UK Cabinet Office, 2018b). For Australia, the analysis considered both waves of reform in recent years, drawing on the respective framework documents: The 2011 *Information Security Management Protocol* (Australian Government, 2011) and, more recently, the *Protective Security Policy Framework* from late 2018 (Australian Government, 2018), which also updated the framework of information classification. Additionally, the analysis considered guidelines that specified the proper implementation of the classification frameworks as well as explanatory notes or commentaries.

### *2.2. Case Selection*

The analysis focusses on the contextual pressures for state secrecy and their implication for classification provisions. Hence, the selection of cases had to consider changes observed in classification frameworks throughout recent years. For that purpose, the first research step entailed a review of classification frameworks in countries that were available for analysis based on language abilities and document

availability.[6] The eventually selected countries – the United Kingdom, Australia, and New Zealand – were considered suitable case studies. Specifically, the classification frameworks of in all three countries have been overhauled in recent years: The New Zealand classification framework was reformed in 2000; Australia experienced two successive reforms in 2011 and 2018, and the United Kingdom adopted a new classification framework in 2014.

Secondly, the three countries that are part of this study display similarities with regard to managing state secrecy. All cases are Westminster democracies with a tradition of Official Secrets Acts[7] that criminalize the release of protected security-sensitive information by public officials. It has been argued that the Westminster system is based on such secrecy, "protect[ing] the deliberations of the cabinet, secrecy to protect the advice proffered by public servants to their ministers, secrecy to hide what happened within the public service" (Australian Government, 2009, p. 42).

Furthermore, all three countries are, next to the US and Canada, associated in the Five Eyes alliance for intelligence cooperation and sharing. The alliance is based on close bonds - both political and strategic - amongst Western Anglophone countries. The long-term cooperation between these countries in security matters have not only consolidated existing relations, but also necessitated harmonization of approaches, including information management and security. Besides the internal need for harmonization, the alliance is also subject to outside pressures for transparency and accountability of the alliance itself, notably after the Snowden disclosures of the global surveillance activities. Lastly, the increasing interest of Western partner countries such

[6] Specifically, the following countries were reviewed: Germany, Switzerland, Austria, Canada, the United States, New Zealand, Australia, the United Kingdom

[7] The United Kingdom's Official Secrets Act of 1989 is still applicable. Australia has Part VII of the Crimes Act of 1914, titled "Official Secrets and Unlawful Soundings." The New Zealand Official Secrets Act was repealed by the Official Information Act of 1982.

as Germany or France to deepen cooperation with the alliance might also facilitate a broader uptake of classification practices observed in the selected case countries.

### *2.3. Analytical Approach*

The analysis was founded on the proposition that the changing context of state secrecy outlined at the outset of this paper might have provoked the reforms of classification systems. Indeed, institutional reform or policy change can improve "the performance of existing systems and of assuring their efficient and equitable response to future changes" (Berman, 1995, p. 27).

According to Streeck and Thelen (2005), multiple drivers for change in institutions and policies exist; traditional arrangements can be discredited or pushed aside in favor of new institutional structures or behavioral rationales. Existing institutions may also fail to respond to their changing environment. Institutions can further be "exhausted" when their traditional workings undermine their *raison d'être*. Therefore, this analysis considered which specific dynamics induced the reforms of classification frameworks.

These drivers of reforms are, to some extent, also reflected in the scope of the reforms and the adaptations implemented. Change can, for instance, be incremental or take the shape of full-fledged reforms (Bennett & Howlett, 1992). This analysis considered the structural changes with the classification framework induced by reforms as well as the changing rationales and practices of classification indicated through information handling instructions. The analysis thus sought to understand whether classification reforms represented a comprehensive revision or a partial adaptation.

Finally, the analysis took a comparative perspective, asking whether the case countries took converging or divergent reform paths. Drawing on Bennett's (1991) framework of policy conversion, the analysis investigated whether the case countries shared common policy problems (drivers for reform) and whether they responded with similar

instruments (policy content and instruments). Furthermore, the reasons for any observed similarities, such as international harmonization, transnational communication, or lesson-drawing, were considered (Holzinger & Knill, 2005).

## *3. Empirics*

### *3.1. Drivers for Reform*[8]

The analysis identified three major drivers for reform: (1) administrative burdens and inefficiencies accruing within the context of the previous classification frameworks, (2) a changing security environment featuring new threats and vulnerabilities, and (3) accountability of secrecy provisions vis-à-vis the public. Table 1 below summarizes which concerns mainly drove reforms in each case country.

*Chapter 3, Table 1: Drivers for Reforms*

| | UK | NZ | AUS |
|---|---|---|---|
| **Administrative Burdens and Inefficiencies** | * | * | |
| **Security Challenges** | * | * | * |
| **Transparency and Accountability** | | | |
| **Convergence** | | * | |

#### *3.1.1. Administrative burdens and inefficiencies*

Over-classification accruing within the context of the previous classification framework was reported as a major source of administrative inefficiencies across the case countries, thus driving reforms. In New Zealand, over-classification created staggering costs for information protection and security clearances, as well as intelligence failure and delays (Gwyn, 2018). Similarly, the previous United Kingdom

[8] Digitization here is not listed as a separate driver for classification reforms, since it is understood as a cross-cutting issue, notably with regard to administrative burdens and security challenges.

classification framework was described as “complex, costly, and burdensome” (Gwyn, 2018, p. 28).

United Kingdom bureaucrats considered the previous classification framework confusing; it displayed a multiplicity of categories that appeared too similar to facilitate adequate marking (Maytech, 2018). Lower classification levels were commonly misapplied (Gwyn, 2018), which led to higher-than-necessary markings. The new, simplified classification structure of the United Kingdom was a direct response to this problem. The new guidelines also caution that “applying too high a marking can inhibit sharing and lead to unnecessary and expensive protective controls” (UK Cabinet Office, 2018b, p. 13)

The Australian guidelines equally pointed to the problem of over-classification, urging that limiting “the quantity, scope, or timeframe of classified information is desirable” (Australian Government, 2018, section 5) to reduce costs, ensure access to information, and avoid devaluing of classification. The New Zealand guidelines equally outline the harmful effects of over-classification and advise against irrelevant classification: “To keep the volume of protectively marked information to a minimum, agencies should limit the duration of the protective marking and set up review procedures” (NZ DPMC, 2018d, section 6).

Outdated routines of information protection that were not aligned with the needs of digitalized bureaucracies were another source of inefficiency. In the United Kingdom, the previous framework was criticized as dating “from a time when civil servants only worked with paper ... [It] led to unnecessary controls, complexity, and misunderstandings” (UK Government, 2014, paragraph 7). Francis Maude, the Cabinet Office Minister who drove the reforms, said that the security restrictions on his office computer made it almost impossible to use (Independent, 2013). “It was very, very clunky, and I nearly threw it out of the window […] Anything secret I now look at on paper” (Maude, cited in Independent, 2013, paragraph 10).

### *3.1.2. Security challenges*

Reforms of the classification frameworks were further prompted by a changing security environment with new types of threats and a wider array of vulnerabilities. Such threats and vulnerabilities not only challenged national security but were also presented across classification guidelines as a challenge to administrations' information holdings.

Launched under the umbrella of the new *Security Policy Framework*, the United Kingdom's classification guidelines were embedded in a broader system of security governance. In the foreword of the overall framework, Cabinet Secretary Heywood warned that "there are longstanding threats and risks to bear in mind, but we must also continue to develop our growing appreciation of global and cyber challenges, critical infrastructure dependencies, together with wider resilience and sustainability issues" (UK Cabinet Office, 2018a, p. 2).

In Australia, the first reform wave in 2011 introduces changes that were directly related to the changing nature of security. The restructured classification framework eliminated the distinction between national security information and information classified due to other sensitivities. Such a distinction was "outdated" (Colley, cited in Whigham, 2013, paragraph 3) at a time when even non-classical security issues might have become a threat to the national interest.

The 2018 *Protective Security Policy Framework* introduced a second revision of the classification framework, with the objective of enhancing security of government agencies as well as addressing new security risks and challenges arising from aggregated data and information technology.

In New Zealand, the new guidelines also responded to a new set of challenges and risks: "We are far more exposed today than ever before. We have increasing quantities

of electronic information, […] technologies, which have increased the ways critical information can be accessed. We face increasing and continually evolving threats that make detection challenging" (NZ DPMC, 2018e, section 2). Importantly, the New Zealand guidelines also referred to the problem of insider threats: "Threats to the security of your information can come from inside and outside your organisation" (NZ DPMC, 2018e, section 2).

The problem of cyber security mentioned across classification guidelines reflects not only the changing security environment but also the way in which the requirements of a digitalized bureaucracy forced the reform of classification frameworks. Digitalization creates an array of new vulnerabilities for organizations and processes, and these vulnerabilities challenge both national security and the security of information holdings of public entities.

### *3.1.3. Transparency and accountability*

Classification frameworks equally reflect the tensions between information security and the increasing expectations for transparency and accountability vis-à-vis the public, and classification guidelines portray information security and accountability as mutually constitutive. For example, the United Kingdom's *Security Policy Framework* illustrates this idea, stating that "the security of information is essential to good government and public confidence" (UK Cabinet Office, 2018a, p. 6). Similarly, the Australian guidelines note that limiting the scope of marked information "promotes the image of an open and transparent democratic government that informs the public to the fullest extent possible" (Australian Government, 2018, section 7). The case of New Zealand challenges the conventional idea that security matters require secrecy. Instead, they establish a potential link between security and transparency, stating that "the environment conducive to good security is not necessarily secret. In fact, the decision-making process must be as transparent as possible. This will ensure accountability to the New Zealand public" (NZ DPMC, 2002, p. 2).

### *3.1.4. Convergence*

Reforms in partner countries or international standardization constitute another driver for reform or, at least, provide lessons and examples from which to draw. In their reform efforts, the case countries oriented themselves, in part, along industry standards for information security or classification practices of partners.

For instance, the reforms of New Zealand's classification framework aimed at harmonization with international partners with whom information was frequently exchanged, notably, Australia (Gwyn, 2018). The manual *Security in the Government Sector*, which constituted the framework for security classifications from 2002 to 2014 stated that "some of the manual content is based on or drawn from similar overseas publications", particularly Australian and UK provisions (NZ DPMC, 2002, p. ii). A recent report by the Office of the Inspector-General of Intelligence and Security (Gwyn, 2018) again drew from practices of partner countries to indicate potential paths for a next wave of structural adaptations. Australia's reform of 2018 seemed to be oriented along the example of the United Kingdom, even if such an orientation was not explicitly stated. The structure and labelling of the new classification framework, however, mirrors the current United Kingdom *Government Security Classification* closely.

Another driver for convergence was the emergence of international standards for effective information security management, specifically the ISO/IEC 27000 series and ISO/TC 223 standards. Classification reforms drew on these standards, referring to the triad of information security that comprises confidentiality, integrity, and availability of information (CIA triad), for instance, or using Business Impact Assessment procedures. In many ways, these standards for information security management not only provided a toolbox for the reforms but also created a specific language for thinking about classification based on risk rationales. The ISO guidelines were

developed as industry standards, thus serving as a tool for private sector operators, which implied convergence between public and private sector entities.

### *3.2. Outcomes of Reforms*

This section reviews the outcomes of classification reforms, analyzing both structural changes and handling provisions. The case countries reorganized not only the structure of classification layers but also the logic of information management *within* each layer. Furthermore, handling provisions in reformed classification guidelines drew from risk management techniques, thus indicating a departure from conventional approaches to information classification.

#### *3.2.1. Restructuring of classification frameworks*

All reforms restructured classification frameworks in response to the challenges outlined above. Structural changes included a reorganization of classification layers, the logic of demarcation between different levels of classification, the types of sensitivities within a classification layer, and the handling of unclassified information. Structural changes, however, were not uniform, but displayed considerable differences.

Table 2 below summarizes the main structural changes of the classification structure and illustrates the similarities between the United Kingdom and Australian cases vis-à-vis distinctive patterns identified in the case of New Zealand.

*Chapter 3, Table 2: Structural comparison of classification frameworks*

| UK, AUS | NZ |
|---|---|
| Reduction of classification layers | Multiplication of classification layers, potential for future reduction of layers |
| All public sector information is part of the classification; unclassified information ceases to exist | Unclassified information persists |
| Unified classification framework | Distinction between security-sensitive and otherwise sensitive information |

Table 3 (see next page) displays the classification structures in the selected case countries before and after their reforms. For Australia, the analysis considered two waves of reform: 2011 and 2018. The classification layers in *italics* indicate categories that cover sensitive information other than security-sensitive information. The classification layers in brackets indicate sub-categories of the main classification layers. Wherever the logic of unclassified information persisted, it is indicated in the last row of the table. The table also indicates the conversion of classification layers from one country to another (table of equivalence). The information was derived from the official classification guidelines as well as from the work done by Gwyn (2018).

*Chapter 3, Table 3: Structure of classification frameworks in the case countries*

| **UK (pre-2014)** | **UK (currently)** | **NZ (pre-2000)** | **NZ (currently)** | **AUS (pre-2011)** | **AUS (2011 to 18)** | **AUS (currently)** |
|---|---|---|---|---|---|---|
| **Top secret** | Top secret | Top secret | Top secret | Top secret | Top secret | Top secret |
| **Secret** | Secret | Secret | Secret | Secret | Secret | Secret |
| **Confidential** | | Confidential | Confidential | Confidential | Confidential | |
| **Restricted** | (Official sensitive) | | Restricted | Restricted | Protected | Protected |
| **Protected** | | | *Sensitive* | *Highly protected* | Sensitive (DLM) | (Official sensitive) |
| | Official | | *In confidence* | *Protected* | For official use only | Official |
| | | | | *X-in-confidence* | | |
| **Unclassified** | | | Unclassified | Unclassified | Unclassified | |

#### *3.2.1.1. Structure of the classification framework*

The United Kingdom's *Government Security Classification* of 2014 represented a dramatic simplification of the classification structure. It sought to make handling provisions more intuitive, thus facilitating compliance. The reform reduced the grading of information sensitivity from five to three layers, and these three layers encompass "all information that government collects, stores, processes, generates, or shares" (UK Cabinet Office, 2018b, p. 3). The lowest level of classification, "official" information, incorporates "all routine public sector business, operations, and services" (ibid, p. 7). This "official" layer also has a sub-category labeled "official-sensitive," which provided personnel or handling instructions for some information. Some commentators have concluded that the sub-category 'official-sensitive' makes the three-stage framework, *de facto*, four staged (Robins, 2014).

Similar to the United Kingdom, New Zealand sought to make information classification more accurate and consistent to ensure the appropriate protection of information. Its reform, however, took the opposite approach, diversifying classification layers to allow public officials to define information sensitivities more neatly (Gwyn, 2018). Therefore, the classification framework was extended from three layers to six layers. An additional layer, "restricted," was introduced for security-relevant information, and a new policy and privacy classification, "sensitive" and "in confidence," was added (Gwyn, 2018).[9] The cabinet paper proposing these changes argued "that the new classifications would remedy deficiencies in the three-level system" (Gwyn, 2018, p. 24)—notably, over-classification. Previously, over-classification had occurred "merely because there was no lower classification category available" (Gwyn, 2018, p. 25). However, current discussions in New Zealand have considered a simplification like the United Kingdom's (Gwyn, 2018) in order to make

[9] The "restricted" layer was also introduced to harmonize the classification framework with the Australian guidelines. The introduction of "sensitive" and "in confidence" allowed for a separation between security-sensitive and other types of protection-worthy information.

classification decisions more intuitive for public officials and to reduce administrative complexities associated with each classification layer.

In Australia, recent reforms brought the classification structure closer to the one introduced in the United Kingdom. The 2011 revisions simplified reduced classification layers from seven to six layers during the first wave of reform. The second wave of reform further reduced the classification structure to four layers, including—just as in the United Kingdom—all public sector information. The restructuring was justified by the continuing misapplication of markings at the lower levels of classification.[10] Moreover, the distinction between security-sensitive information and other protection-worthy assets was abandoned as no longer suitable.

The structural reforms of the case countries were primarily concerned with the lowest levels of classification, which appeared to be more prone to incorrect categorization and markings (Gwyn, 2018). Conversely, "secret" and "top secret" classifications remained mostly constant, both in terms of classification within case countries and with regard to conversion between countries.

#### *3.2.1.2. "Unclassified" assets*

While classifications conventionally single out sensitive information for increased protection, the cases of Australia and the United Kingdom indicated that classification no longer only concerned the management of sensitive information. In both countries, all public sector information featured as part of the classification framework.

[10] For instance, reviews of the classification framework in place between 2010/11 to 2018 found that lower protective markings and dissemination limiting markers (Unclassified, FOUO, Sensitive) were frequently misunderstood and consequently misapplied (Gwyn, 2018).

In the United Kingdom, the 2014 reform abolished the subset of "unclassified" information.[11] "The removal of UNCLASSIFIED means all UK government information is OFFICIAL as a minimum" (Gwyn, 2018, p. 30); this might have been indicated on a document but was not required. "Official" information includes all routine public sector business, operations, and services (UK Cabinet Office, 2018b, p. 7). Thus, most information previously unclassified fell into the "official" category after the reform. This approach is not about relabeling information categories but changes the perspective on public sector information in general: "official" information, like all other classification layers, has vulnerabilities and is not automatically available for circulation.

The changes introduced in the United Kingdom did not come without challenges. In a recent evaluation report, the Audit Office found that "this confusion resulted in significantly different handling of OFFICIAL information by departments. Some treated it as they formerly would have handled 'unclassified' information, moving it freely across the internet and using personal email accounts" (Gwyn, 2018, p. 31). Some departments considered "official-sensitive" markings as "an indicator only of enhanced handling requirements for 'official' information; others as a higher classification" (Gwyn, 2018, p. 31).

With the reform of 2018, Australia became more similar to the United Kingdom's provision, with "unclassified" information ceasing to exist. The lowest level of classification, "official," is applied to non-sensitive public information, covering "the majority of routine information created or processed by the public sector" (Australian Government, 2018, section 3).

[11] Prior to 2014, "unclassified" information existed but was not protectively marked; the assessment could be indicated on a document for reasons of clarity.

Marking information as “official” is not mandatory but could be used to indicate that the information forms part of the government record. Unlike the United Kingdom, however, such “official” information did not have a threat profile.

New Zealand was the only country among the selected cases in which “unclassified” information persisted. Unclassified information could be marked as such to distinguish it clearly from classified information and show “that the impact from unauthorized disclosure or misuse has been assessed” (NZ DPMC, 2018a, section 4). In keeping the distinction between classified and unclassified information, New Zealand also considered the vulnerability of unclassified assets, requiring agencies to establish policy “information that needs increased protection but doesn’t qualify for a security classification” (NZ DPMC, 2018a, section 4).

In summary, the trend toward an inclusive approach to information governance reconfirmed governments’ heightened concern about information management at the lower end of the sensitivity spectrum. This may have been due both to a perception of new vulnerabilities of such types of information and/or to the increased value of a broader spectrum of information for security governance.

#### *3.2.1.3. Demarcation of classification layers*

Demarcation of classification categories concerns the way in which the sensitivity of information is assessed. Conventionally, classification levels consider the *gravity of the harm* caused by the unauthorized release of sensitive information (Földes, 2014). Australia and New Zealand largely maintained such a conventional model of demarcating classification layers throughout their reforms. In contrast, the reform in the United Kingdom enacted a more complex set of criteria, demarcating sensitivity levels as *areas of government activity, type of threat actors,* and *type of damage*.

The contrast between both approaches is illustrated in Table 4, which compares "top secret" and "secret" information in Australia and the United Kingdom.

*Chapter 3, Table 4: Comparison of demarcation logic (Australia versus the United Kingdom)*

| | **Australia** | **United Kingdom** |
|---|---|---|
| **Top secret** | Exceptionally grave damage to the national interest | Compromise through advanced state actors using significant technical, financial, and human resources, causing a widespread loss of life. |
| **Secret** | Serious damage to the national interest | Damage military capabilities or investigation of serious organized crime. Threat actors on this level are states or organized crime groups. |

The Australian case follows a conventional gradation logic, demarcating sensitive information by the scope of damage expected for the national interest, as follows: on a "protected" level, information compromise was expected to cause "damage"; at a "secret" level, "serious damage"; and on a "top secret" level, "exceptionally grave damage" (Australian Government, 2018, section 3). At the "official-sensitive" level, information compromise was expected to cause "limited damage" to an individual, organization, or government. The object of harm—national interest—remains constant; the impact of damage increases.

In contrast, the United Kingdom's framework considered a more complex approach to assessing the sensitivity of information, in which the object of damage changes and threat actors feature as part of classification determinants. This assessment most likely paid tribute to the changing security environment, which featured both conventional and novel threats. Identifying vulnerabilities and potential harms beyond the national interest required re-thinking the classical (state-centric, military-related) understanding of security. As such, even "official" information displayed vulnerabilities and might have inflicted damage upon the day-to-day business of government.

This information is considered the target of attackers with bounded capabilities and resources, such as hacktivists, single-issue pressure groups, investigative journalists, competent individual hackers, and the majority of criminal individuals and groups. The framework clarified that *all* government information "has intrinsic value and requires an appropriate degree of protection" (UK Cabinet Office, 2018b, p. 4).

In contrast to the United Kingdom's model, New Zealand remained with a more conventional understanding of security, restricted to the notion of security as "national security." The classification framework distinguishes between information that is protected based on public interest and personal privacy considerations and information concerning national security matters, notably defense and foreign policy (NZ DPMC, 2018b). The former refers primarily to the disruption of day-to-day processes of governance, such as the maintenance of the law or public safety (NZ DPMC, 2018c). Australia ceased such a "dualist" approach to classification in 2011, calling it "outdated" (Colley, cited in Whigham, 2013, para. 3). Treating vulnerabilities in *one* framework reflects the dispersed risks and complex interdependencies of contemporary security.

### *3.2.2. Information handling: Toward risk management*

Besides structural changes, the classification frameworks featured several handling provisions that indicated a new way of thinking about security. Specifically, this analysis noted a change from bureaucratic risk aversion toward the encouragement of risk management. This includes responsabilisation of staff, information sharing, and the focus on proactive information management.

#### *3.2.2.1. Responsabilisation*

The importance of proactive information management is primarily reflected in the distribution of classification authority. All three case countries make agencies responsible for ensuring their own compliance with classification policies through self-inspection and internal audit (Gwyn, 2018). In New Zealand, classification authority—and thus responsibility—is dispersed: "When information is created, the originator must do a risk assessment" (NZ DPMC, 2018s, section 2). The example of Australia makes an even stronger case for responsabilisation. The provisions do not limit authority for original classification, since "agencies created thousands of documents each day, it would be 'very inefficient' to mandate that only senior and experienced officers could classify information" (Australian Government, 2004, p. 99).

The Australian reforms also aimed at decentralizing responsibility; each agency was required to develop its own guidelines based on assessment of organizational needs (Coyne & Meurant-Tompkinson, 2018). Through the second wave of reforms in October 2018, the government's *Protective Security Policy Framework* introduced a shift from a compliance model to a principles-based approach providing general guidelines (Summersby, Hemming, & Wright, 2018). This shift was decided upon based on a previous review that found that the framework did not strike an appropriate balance between risk management and administrative burden (ibid.).

The United Kingdom's guidelines place staff behavior at the center of appropriate information management: "The emphasis upon personal responsibility and accountability that underpins the new policy is a key feature" (UK Cabinet Office, 2018a, p. 2). According to the guidelines, agencies should aim for "staff who are well trained to exercise good judgement, take responsibility, and be accountable for the information they handle" (ibid.).

The initial guidelines released in 2014 even asserted "that the benefits of the new policy will be eroded if organizations are too risk averse and seek to put more information into 'secret' than is absolutely necessary" (Strutt, 2016, p. 4).

#### *3.2.2.2. From need-to-know to need-to-share?*

A risk management approach to information management might also increasingly require sharing information. The conventional "need-to-know" approach to information security relies on compartmentalized markings or technical barriers that restrict access to sub-groups among those that have general access to relevant classification. Recently, security scholars have emphasized the limits of compartmentalization for contemporary security governance (see introduction), limiting the effective usage of information assets. While the need-to-know principle persisted across the case countries even after reforms, Australia and the United Kingdom also considered the role of information sharing, to some extent. Table 5 below outlines the differences between a need to know approach versus a need to share approach.

*Chapter 3, Table 5: Need to Know versus Need to Share*

| | ***Need to Know*** | ***Need to Share*** |
|---|---|---|
| ***Approach*** | *Compartmentalization* | *Responsabilisation to share if needed* |
| ***Objective*** | *Information protection* | *Information availability and exploitation* |

The United Kingdom's *Government Security Classification* policy is an "administrative system for the secure, timely, and efficient sharing of information" (UK Cabinet Office, 2018b, p. 4). While the need-to-know principle also applies in the United Kingdom, the framework took a somewhat different approach, emphasizing

the relationship between information sharing and security: “Information needs to be trusted and available to the right people at the right time. The failure to share and exploit information can impede effective government business and can have severe consequences” (UK Cabinet Office, 2018b, p. 5). The framework displays a tension between protecting information through application of a need-to-know approach and equally enhancing security by sharing relevant information among staff. According to the Cabinet Office, “In extremis, there may be a need to share sensitive material to those without the necessary personnel security control, for example, when immediate action is required to protect life or to stop a serious crime. In such circumstances, a common-sense approach should be adopted” (UK Cabinet Office, 2018b, p. 5).

Australia displayed a somewhat more ambiguous attitude toward the need to share. The country’s guidelines limit the access to information to authorized persons for approved purposes. At the same time, they “facilitate[d] information sharing if needed for business purposes; the originator can (on a case-by-case basis) reconsider application of the AUSTEO caveat to its information and, if warranted, reclassify that information” (Australian Government, 2018, section 7).[12] However, the guidelines caution that “enabling wide use of government information provides substantial benefits, but there are risks involved. […] Where the adverse consequences of increased information access are considered high, the availability and access to the information will benefit from careful management” (Australian Government, 2018, section 6.4).

The co-existence of need-to-know and need-to-share information might create new challenges for secrecy management, presenting public officials with opposing

[12] The Australian Government Security Classification System (AGSCS), active between 2010 and 2018, took a somewhat different approach, being “designed to help implement the Government’s vision for effective information sharing across agencies.” (Burke, cited in Whigham, 2012, paragraph 3)

expectations both to share and to protect information. The co-existence also raises questions about possible criminal liability for mishandling classified information.

#### *3.2.2.3. From information protection to information management*

Guidelines across the case countries further shared the objective that classification should increase public sector efficiency and be business enabling. In other words, information management had to strike a balance between security needs and the organization's ability to exert its mandate.

The New Zealand provisions hold that "robust information security is a business enabler. It helps your organization to maintain the trust and confidence of the public, customers, and partners" (NZ DPMC, 2018f, section 3). The United Kingdom's framework portrays security and efficiency as mutually constitutive, stating that government activities attracted risks that must be "assessed by government organizations so that they can make informed, practical, and effective business enabling decisions" (UK Cabinet Office, 2018a, p. 5). The Australian *Protective Security Policy Framework* (Australian Government, 2018) emphasize that well-managed information supports efficient business.

All guidelines underline the value of government information and the need for appropriate information management. Specifically, the CIA triad (confidentiality, integrity, and availability)[13] of information security systems was a core aspect in all guidelines. By adopting a CIA logic, the case countries oriented themselves around the international standards for information security provided by, for instance, ISO/IEC 27000. For example, Australia placed the CIA objectives prominently by proposing them as the overall purpose for the classification provisions (Australian Government,

[13] *Confidentiality* refers to authorized access only; *integrity* is the accuracy and completeness of information, and *availability* allows authorized users to obtain access to information when required.

2018). Under the section "Why Information Security Matters," New Zealand emphasize that "every organisation relies on the confidentiality, integrity, and availability of the information it processes, stores, and communicates" (NZ DPMC, 2018e, introduction). The United Kingdom's guidelines state that their purpose was primarily "confidentiality" of information and assets; however, "public sector information and services often have significant integrity and/or availability requirements, too" (UK Cabinet Office, 2018b, p. 30)

The idea of efficient management of information suggests a departure from the mere protection of information toward efficient usage and exploitation of data assets. The emphasis on the value of information concerns not only its protection requirements but also its role as an asset for security governance. The effective management of information, supported by responsabilisation of staff and increased sharing, might thwart the conventional risk aversion of bureaucracies when fully realized.

### *4. Summary of Results*

The comparative analysis of classification provisions illustrated that similar objectives drove reforms across the case countries, including administrative inefficiencies, digitalization, security needs, transparency expectations, and international reform efforts. These shared objectives, however, did not consistently lead to identical responses. This summary provides an overview of several cross-cutting developments that were observed in the case countries, as follows: (1) increased emphasis on appropriate management of information, (2) simplification of classification frameworks, (3) responsabilisation of officials in the management of public information and dispersion of information security ownership, (4) adaptation of private sector techniques for information security, and (5) inclusiveness of classification frameworks.

### *4.1. Appropriate information management*

Contextual changes required public sector institutions in the case countries to rethink their approach to information management. Transparency requirements demanded the availability of information and, therefore, required an adequate framework for organizing and evaluating available information. The challenges regarding over-classification and inadequate management of information that sparked reforms in the case countries were directly linked to these requirements for transparency. At the same time, the analysis of classification frameworks also illustrated that having a system in place that allowed for the appropriate management of information was, by itself, understood as a signal for accountable and effective governance vis-à-vis the public. Furthermore, digitalization amplified the production and sharing of information, likewise requiring the administration to improve information management for the benefit of internal efficiency and effectiveness. Finally, with a security sector hungry for information for identifying and preventing threats or risks, appropriate information management became essential for the identification and appropriate exploitation of such information.

### *4.2. Simplification of classification frameworks*

A further trend that was observed in the case countries was the simplification of classification frameworks through reduction of classification layers. In New Zealand, this restructuring remains a reform proposal, for now. The analysis suggested that simplification was seen as a means to reduce over-classification, thus making information more readily available for sharing, both internally and externally. Simplification further allowed for an appropriate assessment of risks embedded in certain information, facilitating appropriate safeguards and usage of information for security purposes.

Changes to the classification framework primarily concerned the lower layers of classification, whereas the highest categories, “secret” and “top secret,” remained widely intact and consistent between countries and over time.
The lower levels of classification appeared to raise the most concerns and confusion among public officials.

### *4.3. Responsabilisation*

Distribution of responsibility was another trend across classification provisions that sought to tackle the problem of over-classification. It concerned the ownership of information security at an individual or agency level (e.g., as expressed through widely distributed classification authority or dispersed responsibility for putting management systems in place to meet the security needs of specific agencies). This distribution represented a departure from previous forms of information management that were centered around the Official Secrets Act and promoted a culture of risk aversion and, in consequence, over-classification. While the effective and responsible management of information was emphasized in all classification provisions and encouraged through various measures, risk aversion remained a persisting problem, as demonstrated by the analysis of the cases.

### *4.4. Private sector techniques*

A further observation was the adoption of private sector techniques for information security management, specifically ISO/IEC 27001. Regarding the selected case countries, where New Public Management (NPM) dominated the reform of bureaucracies for several decades, even core government tasks appeared to feature NPM approaches. The guidelines suggested private sector logic at several points, addressing cost-reduction, efficiency in information management and effective exploitation of information and emphasizing the value of information.

### *4.5. Inclusiveness of classification frameworks*

Two of the cases analyzed—Australia and the United Kingdom—abandoned unclassified information, integrating all public sector information in the classification framework. Such an inclusive approach points to a changing logic of sensitive information management and thus, more broadly, state secrecy. It reflects the understanding that security risks are dispersed and can even be found in public sector activities not primarily associated with security activities. Therefore, for an effective identification of risk and exploitation of relevant data, all information must be assessed regarding its security relevance. Furthermore, the inclusive approach suggests that classification frameworks were no longer merely concerned with the separation between secret and non-secret information, and thus protection of information from external release, but even more concerned with effective management of all information internally. Considering all information within a classification framework emphasized the relevance and value of information for public management in general and for security purposes specifically. It served as a signaling effect, internally and externally, that all public sector information was of value.

The case countries, while facing similar problems and seeking reform, did not embrace change to the same degree. If the conventional approach to classification is described as a system based on compartmentalization, division between secret and non-secret information, and protection of information from conventional threats (espionage, etc.), then New Zealand was closer to such a conventional approach. The United Kingdom, on the other hand, appeared to understand information management differently, considering more diverse threat actors and areas of damage and understanding classification as a means for information management more generally. The Australian approach can be considered a median between the two other cases, displaying a structural convergence with the United Kingdom's framework, yet ideationally being much closer to a conventional model.

## *5. Conclusion*

The shifts in the management of classified information have led to several different types of insights. Some insights are directly related to procedures and practices of administrative secrecy, as well as their managerial impacts. Beyond that, the insights from this study served to reconceptualizing the role and function of secrecy as well as critically reflecting on the normative implications of novel classification practices.

### *5.1. Reforming Procedures*

All three case countries have reformed the way in which classification is thought and practiced, from comprehensive restructuration of the system itself to the attribution of specific administrative responsibilities. These changes represent at the basic level revisions of operational management. It also requires across governmental systems, a greater level of coordination as a direct consequence of moving away from a more centralized, top-down approach.

Given the problem of insider threats through leaks and lack of compliance with existing provisions, one of the primary objectives of information management was not the protection from outside threats but rather the appropriate management of staff behavior, attitudes, and understanding. Classification moved being a formalized documentary standard, to one also involving the human side of the equation. This implies, for example, a greater awareness, within the confines of classification procedures of elements linked to staff attitude and behaviors.

### *5.2. Secrecy Definition and Use*

The analysis suggested that the recent reforms initiated throughout the case countries were not only about the introduction of new information management techniques to

safeguard state secrets but rather about administrative secrecy itself undergoing a re-conceptualization of both its definition and use.

Conventionally, secrecy serves primarily to sensitive areas of government such as defense and foreign affairs. This implied a distinction between secrets and non-secrets; a binary conceptualization that had the benefit of clarity but not that of accuracy. The reformed classification frameworks in case countries moved from a dichotomy to a gradient of differentiation. Such an approach leaves much more discretion and arbitrariness in its evaluation but that also implies a much more precise attempt evaluation and definition.

The need for this gradient approach, rooted in large part in the increasing value and use of information (value as a source for risk evaluation, but also for better policy making and *in fine* monetary returns) has led to a greater openness in its production, collection, analysis and circulation. From a unique type of potential danger information becomes an asset and an opportunity. The consequence is a complete reversal of the role and impact of information protection, moving away from administrative privilege to administrative opportunities.

### *5.3. Implications for Information Management*

The analysis underlines quite clearly a paradigmatic change in information management, opening numerous avenues for the understanding of its function and positioning at the heart of governmental operations.

Whereas secrecy provisions conventionally served as a means for deterring public officials from unauthorized disclosure, the analyzed classification guidelines stressed in contrast the importance of proactive information management and responsabilisation. There is a positive connotation given to providing a more extensive

right to share information, that goes in direct opposition to the previous approach of compartmentalization.

More broadly, revisions to the classification system can be expected to impact information and records management, either in the way it is being created, filed and stored or, on the other side of the spectrum, the circulation, provision and protection of information.

### *5.4. Normative Implications*

The inclusion of all public sector information into the classification framework renders the potential for concealment universal. Every piece of information is subject to classification, since unclassified assets no longer exist. Responsibly using administrative secrecy privilege may come to imply appropriate information management rather than addressing the fundamental normative questions regarding information concealment or disclosure. Citizens might be faced with clearer rules as to what information is not available (what has been termed the 'transparency of transparency'), but not get more *de facto* access to information. (Villeneuve 2014) without the benefit of knowing anything more. The rules will be more open and transparent, but not the underlying information.

### *5.5. Conceptual implications*

In this changing classification environment, the assumed antagonism between transparency and secrecy appeared no longer to exist. The example of the United Kingdom vividly illustrated the ambiguous boundaries between secrecy and non-secrecy in which all government information featured as part of the classification framework. The important of classification, conventionally seen as a tool to identify and protect sensitive information from external view, was equally emphasized as a

means to generate accountability vis-à-vis the public for effective and efficient information governance.

With the use of personal, private data for intelligence operations and the exploitation of publicly available data for intelligence purposes, the boundaries between external and internal data, openness, and secrecy are increasingly blurred; leading to confusion both inside and outside official institution.

### *6. Limitation and Next Research Steps*

The findings in this analysis are so far limited to a limited selection of cases, all of which represent a specific political-administrative system. Thus, the observations made have limited generalizability, even if a broader uptake of described information management practices can be expected in this future due to the leading role of intelligence work conduced within the 5-Eye community. Future research should pay close attention to further reforms of classification regimes and adaptation of practices comparable to those described in this paper.

Further, the practices described in this analysis should be understood as reforms underway. The case of Australia illustrates that classification systems might be subject to ongoing adaptation. Thus, longitudinal research is needed to monitor reform progress and outcomes.

Finally, future research should address the implementation of described practices by different institutions as well as implications for the information management system more generally. The latter includes a close observation on the consequences for information production and records management (upstream consequences, see (Caron, 2017) as well as information availability and provision (downstream consequences).

## *1. Summary*

This dissertation investigates the legitimation of government secrecy in the age of transparency and provides an interdisciplinary perspective on administrative rationales for "national security secrecy." It provides a conceptual exploration of national security secrecy and traces the changing secrecy practices through analyzing classification frameworks. The objective is to broaden the understanding of national security secrecy beyond its conception as a necessary exemption from the norm of transparency, as conventionally suggested in the literature.

The analysis illustrates how secrecy practices have changed in recent years, drawing increasingly on risk management techniques and rationales. These changes do not only reflect challenges facing bureaucratic processes (digitization, transparency) but also highlight the changing, more complex understanding of security. The notion of "risk secrecy" challenges the conventional legitimations for national security secrecy and, in turn, the relationship between secrecy and transparency and accountability.

The following sections provide a summary of the empirical findings and of the contribution this thesis makes to the study field in general.

## *2. Empirical Findings*

The empirical analysis in Chapters 2 and 3 investigates recently reformed classification frameworks to better understand the changing nature of state secrecy. It finds that a variety of factors sparked their reforms—from inefficiencies and dysfunctionalities within existing classification frameworks to new challenges for information handling within digitalized bureaucracies. Furthermore, contextual changes, such as the increasing expectation of government accountability and a new, more complex security environment, require states to adapt their approaches to managing sensitive information. Reformers, therefore, draw on information

management practices used in partner countries or by private sector entities, aiming partially toward harmonization and standardization. Consequently, the reformed classification frameworks show instances of convergence, both in terms of structure and rationales for information handling. The results from the analysis point toward an increasing "riskification" and "reflexivity" of information governance, which are discussed in more detail in the following section.

### *2.1. "Riskification": From Information Protection to Information Management*

Reformed classification provisions center around risk terminology and promote a risk-management approach to information handling. As discussed in Chapter 2, the logic of risk entails predicting and managing of detrimental events in the future. The control of uncertainty, therefore, depends on the effective usage of information assets. Indeed, reformed classification guidelines emphasize the availability and exploitation of information as well as "business-enabling" information governance. The introduction of risk to classification practices suggests a shift from mere protection of sensitive information toward proactive management.

Case countries examined in Chapter 3 also conduct structural revisions of the classification framework for the benefit of effective information management. These are geared toward information inclusion—meaning *all* public sector information is organized through the classification framework—thus taking a wider scope of information into consideration for prediction and forecasting of potential threats. In a risk setting, vulnerable and valuable information can be found even in areas previously not associated with security concerns. Additionally, classification reforms put forward a simplification of the classification structure, making document classification marking more intuitive and, thus, reducing inefficiencies in information governance.

The introduction of risk management rationales into state secrecy governance challenges the bureaucracies' inclination toward risk aversion. While previous approaches to managing sensitive information were based on deterrence, new classification provisions entrust public sector staff not only with the protection but also with the exploitation and—if needed—with the sharing of information. In sum, it appears that secrecy no longer constitutes a prerogative but emerges to become a bureaucratic responsibility.

### *2.2. Reflexive Government: Turning of the State upon Itself*

While protection of information against outside threats is still a fundamental aspect of classification regimes, the reforms also serve as a tool for self-regulation. This dynamic has previously been described as "reflexive government"—the state turning upon itself as a subject for problematization, scrutiny, and reform (Dean, 1999). It entails that institutions are increasingly seen as vulnerable by their own members who, in turn, become the targets of their risk management efforts (Power, 2004). Concretely, reformed classification guidelines seek to address problems of over-classification, excessive secrecy, or insider threats, thus managing both the external demands for accountability and internal requirements for efficiency and control.

The reflexivity of information governance can be traced back to the concern regarding insider threats—mentioned, for instance, in the United Kingdom and New Zealand cases—as well as to the increasing accountability and scrutiny of public sector institutions in the age of transparency. With the rise of transparency and accountability as norms of democratic governance, inappropriate secrecy has emerged as a problem for bureaucracies themselves, reducing the credibility and trustworthiness of public institutions. The reformed classification guidelines advertise effective and appropriate information governance as a reflection of their accountability to the public.

At the same time, information causes an increasing liability not only in terms of security but in terms of exposure. The prevalence of radical, bottom-up transparency in the form of leaks or information hacks, necessitates the rethinking of the bureaucracies' approaches to handling information and staff attitudes or behavior. As such, secrecy management is no longer solely about protecting national security but is also about identifying and preempting information vulnerability.

### *2.3. Toward a New Standard of Information Governance?*

The analysis provides some indications that the approaches to information classification observed in some case countries, notably the UK; might experience a wider take-up. However, the implementation of risk management techniques for secrecy governance is a reform project in progress. Considering that the case countries investigated in Chapter 3 are in midst of their reform projects—subject to continuous assessment and readjustment—the long-term outcomes of these reforms may only be observed in the years to come.

Comparative analysis revealed not only the similarities in the reform approaches but also in the concerns that these reforms seek to addressed, which could be shared by various other advanced democracies. This primarily concerns the adaptations of secrecy management in the information age, responding to (1) the expectation of transparency, considering (2) the increased role of information exploitation for security governance, and (3) the new opportunities and vulnerabilities through digitization. Responsabilisation of bureaucrats and reflexivity of administrations provide comprehensive responses to these challenges.

In their reform efforts, the case countries such as New Zealand also considered, at least partially, the classification practices of their international partners. In the future, other intelligence partners might seek harmonization or draw lessons from these examples when adapting or renewing classification frameworks. Moreover, the reformed

classification frameworks draw on industry standards and private sector techniques, such as Information Security Management Systems or Business Impact Assessments provided by the International Organization for Standardization (ISO), to address the secrecy governance challenges. This permeation of private sector logics in core state activities is most likely to show in other contexts in which New Public Management reforms dominate the public management.

## *3. Contribution to the Field*

The conceptual contribution of this thesis lies in (1) the reconceptualization of national security secrecy, from realism to risk management, and in (2) the implications of such a reconceptualization on the understanding of secrecy and transparency as opposing concepts. Furthermore, the thesis provides (3) an interdisciplinary and (4) comparative perspective on the problem of national security secrecy, thus broadening and deepening the understanding of the way in which it can be legitimized.

### *3.1. Reconceptualizing the Relation Between Secrecy and Transparency*

The thesis challenges the conventional conceptualization of secrecy as an antipode of transparency, thereby contributing to an emerging literature on the ambiguous nature of transparency (see thesis introduction "Conceptual Challenges"). It argues that both concepts are ambiguous, politicized, and, at times, parallel—shaped by contexts and situational interpretations. Through the analysis of national security secrecy, a contribution is made to a growing area of literature that critically examines the claimed benefits and conceptual foundations of transparency.

This thesis argues that the conventional justification for national security secrecy relies on a narrow paradigmatic understanding of security. Chapter 1 unpacks the conventional notion of secrecy as a "necessary exemption" from transparency. The analysis proposes that this claim is based, in fact, on three separate rationales: elite

governance, policy implementation, and crisis response mechanisms. Each rationale provokes different challenges regarding the accountability and legitimation of secrecy.

Chapter 2 identifies the impact of risk rationales in reformed classification frameworks. Here, appropriate information protection is portrayed not in opposition to accountable governance but as a constitutive factor. The notions of "responsabilisation" and "reflexive governance" introduce the idea of bureaucratic self-scrutiny, complementing external monitoring and oversight arrangements with elements of self-regulation. Efficient information management, as seen, facilitates not only information protection but also upstream transparency through increased information integrity and availability.

A critical, context-sensitive approach to secrecy allows scholars to appreciate concealment as a complex social practice, marked by shifting meanings and appropriation. Transparency advocates can benefit from a more fine-tuned judgement vis-à-vis secrecy legitimation that is motivated by governments and institutions.

### *3.2. From Threat to Risk Secrecy*

The thesis examines a new approach to managing secrecy, which has been labelled "risk secrecy" by the author due to its reliance on risk rationales and risk management techniques. The notion of risk secrecy as originally introduced by this work. It refers to a novel way of thinking and administrating state secrecy, challenging various previously-held conceptions of the dynamics and implications of government secrecy. In consequence, this work conceptualizes risk secrecy in contrast to the conventional understanding of bureaucratic secrecy more broadly and national security secrecy in particular. As such, risk secrecy is determined by the following aspects:

- *Information Scope:* risk secrecy entails a shift from conventional separation between sensitive information and non-sensitive information towards an evaluation of all information with regard to their sensitivity. Thus, boundaries between security-sensitive information in the classical sense (e.g. related to defense and foreign policy or intelligence operations) and less sensitive policy sectors are increasingly blurred. This renders the difference between normal and exceptional politics obsolete, while emphasizing the hazards of less-than existential threats. In consequence, secrecy governance evolved from an exception to routine management

- *Information Management:* As a consequence of a broader scope of information considered for enhanced protection, secrecy governance evolves from being an exceptional measure to routine management. Risk secrecy further entails a shift from information protection to information exploitation and proactive, business-enabling information management. In consequence, the perception of information shifts from it being seen as a vulnerability to being perceived as an asset.

- *Information Managers:* Conventionally, secrecy is closely connected to bureaucratic risk avoidance and information hoarding. Risk secrecy in contract recognizes that security hazards might arise not only from outside perpetrators, but also from internal liabilities, such as failure to share information when needed or ineffective exploitation of information. It thus promotes the individual responsibility of information managers.

The concept of risk secrecy describes an emerging practice of defining and handling information sensitivity. As such it provides a theoretical-conceptual framework for an emerging practice as well as an empirical observation of a novel phenomenon.

Risk secrecy is defined by the author as the “proactive management of governments’ information assets for the benefit of information protection and exploitation”. Risk

secrecy can be understood as a novel way of managing state secrecy and, more broadly, as part of a strategy for managing public information.

Risk secrecy reflects the changing security environment in which threats are dispersed and ubiquitous, thus requiring attention to also be paid to non-traditional security fields. Furthermore, it underlines the increasing importance of information in security governance—forecasting and monitoring of future threats—which requires the sharing and in-depth analysis of increasingly larger sets of data. Finally, risk secrecy responds to risks in information security itself, facing increasing vulnerabilities from increased information sharing, digitalization, or insider threats.

The emergence of risk rationales in the governance of state secrecy generates new questions regarding the legitimation of secrecy practices. While governments portray comprehensive information management and accountability as two sides of the same coin, the inclusion of all government data in the framework for information protection potentially expands governmental information control. At the same time, reformed classification provisions suggest an increasingly liberal approach to information management, including sharing, availability, and reduction of over-classification. These trends provoke fresh reflections on whether and when secrecy is constitutive for security.

Finally, the above-identified patterns of ‘risk secrecy’ challenge common conceptions of state secrecy, notably its understanding as the flip-side of transparency and accountability. Scholarly discussions on the conceptions of government openness more broadly. From a practitioner’s perspective, it is essential to understand new challenges states arising from digitization, a wider array of security risks, public-private cooperation, ever-growing information assets held by governments in order to assess legitimacy claims of secrecy.

### *3.3. Providing an Interdisciplinary Perspective*

This thesis "takes security seriously," confronting transparency research with the field of critical security studies. As discussed at the outset of this thesis, security can be considered as the "elephant in the room" in the literature on legitimate exemption: security is widely accepted for its necessity claim, yet poorly understood and subject to contestations. The analytical framework in Chapters 1 and 2 draws extensively on existing scholarship in the field of security studies and provides, as a result, both a nuanced perspective on legitimacy claims as well as a novel perspective on national security secrecy as risk.

How security is defined and perceived matters tremendously for the secrecy is conceptualized and practiced. The interdisciplinary perspective provided by this thesis makes it clear that national security secrecy is neither unidimensional nor constant. It is subject to changing rationalizations and, hence, justifications, depending on the prevailing security considerations and contextual appropriation. Chapter 1 illustrates how national security secrecy can occur at various governance instances, each of which relies on concealment to achieve specific objectives. Chapter 2 illustrates the importance of considering the changing understanding of security itself, notably, in the form of recently emerging risk rationales.

### *3.4. Providing a Comparative Perspective*

National security secrecy has primarily been studied in the context of the U.S. political–constitutional system. While providing a myriad of notable scholarship on the topic, the lack of a comparative perspective limits the conceptualization of national security secrecy. Indeed, the need to balance security and liberty, as it is frequently posed in academic literature, mirrors the narrative that features prominently in U.S. policy debates (Quill, 2014, pp. 60-61). Moving away from an over-studied case that

can be described as atypical,[14] this thesis seeks to broaden the conceptual perspective on national security secrecy by investigating secrecy in other contexts. The analysis investigates secrecy practices not only across Westminster democracies (United Kingdom, Australia, and New Zealand) but also looks at how they compare to secrecy management within federal constitutionalist systems (United Kingdom versus Germany).

The comparison highlights the trends emerging outside of a U.S. context. Furthermore, it illustrates not only convergence dynamics but that, indeed, the countries with general similarities and comparable challenges, such as leaks or over-classification, might develop differing responses either within reforms or through the absence of reforms.

### *4. Limitations and Next Research Steps*

The most obvious challenge facing this thesis project is the assessment of secrecy norms and practices themselves. Since the object of analysis—government secrecy—is by definition subject to concealment, accessing data poses a very real challenge. The thesis seeks to circumnavigate these obstacles by investigating fundamental conceptual questions—instead of reiterating the conventional logics of state secrecy, the analysis focuses on the logics underlying secrecy claims. In addition, the empirical analysis engages with immediately accessible material—secrecy provisions, especially classification frameworks that are an immediately accessible source of data.

[14] Quill has noted that in the case of the United States, public discourse frequently centers around the balancing metaphor (security versus liberty), precluding the possibility that security and liberty might exist in parallel (p. 58-66). Most notably, the administrative argument predominately flips the balance in favor of security. The U.S. favor for security might be explained through its global status as a security actor, what Henry Kissinger has called the "American Exceptionalism." At the same time, the debate around the limitation of individual liberties, such as the right to know, for the benefit of national security are determined by a general suspicion against agents of power, fueled by past scandals of the abuse of secrecy privileges, rendering the role of transparency as a tool against secrecy ever more important.

It has to be noted, however, that these provisions and their implementations might vary: specific actors or institutions can interpret provisions differently and implementations can face challenges.

A further limitation of the study is the exploration of risk secrecy in a limited number of countries, all of which are categorized as Westminster democracies (internal validity). The case countries that featured as part of the analysis in Chapter 3—United Kingdom, Australia, and New Zealand—provide interesting material for understanding the changes in rationalizing government secrecy. They follow specific institutional traditions and, thus, their reforms may also reflect specific systemic problems that they seek to address (external validity). Further research needs to consider classification reforms in other contexts in order to understand whether these were driven by similar concerns and in what way reforms efforts take a similar or diverging approach. Moreover, it is recommended to trace ongoing reforms of classification regimes from a longitudinal perspective to obtain a full understanding of impact and challenges. At the same time, it would be interesting to explore 'deviant' cases, i.e. those countries not undertaking reforms. The case of Germany investigated in Chapter 2 constitutes an interesting starting point. Further analysis on similar cases could help better understanding of their reluctance and policy choices.

Besides adding further contextual and temporal richness to the comparison presented in this study, future research might also trace the implementation of classification provisions at the agency level. Here, it would be worthwhile to investigate the usage and understanding of secrecy provisions by different types of institutions.

Moreover, it should be noted that this study focusses on secrecy provisions which specifically pertain to national security secrecy. While this is a key aspect of state secrecy, it should also be noted that different considerations and dynamics might apply to other dimensions of state secrecy, concerning e.g. deliberations, trade and economic policies.

Finally, implications of classification reforms and risk secrecy on government information management more generally are to be researched. This includes both upstream dynamics, notably consequences for records creation and management, as well as downstream dynamics, such as the availability and provision of information. Such research would, however, entail a broader empirical research, preconditioned by access to relevant interview partners and institutions.

### *5. General Reflection*

The issues addressed within the scope of this research fit into the wider reflections on the blurring boundaries between transparency and secrecy, opacity and concealment, enlightenment and disinformation in the age of fake news and big data. Transparency and secrecy intersect on a larger spectrum of false claims, information overload, information contextualization, narrative versus formal transparency, and scrutiny mechanisms. The work conducted for this thesis underlines the ambiguity of secrecy and transparency as umbrella terms for a number of governance mechanisms. Such ambiguity can easily be applied and abused for political agenda, in addition to public interest considerations.

Can risk security moderate the effects of politicization and normativity? Critical security scholars have cautioned that risk rationales only serve to further expand state power, creating a constant atmosphere of paranoia and legitimizing emergency measures at any time. The concrete impacts of risk management techniques on information governance remain to be seen—current provisions suggest both an expansion of information control (inclusivity of classification regimes) and an increase in process transparency with protective secrecy (responsabilisation, reflexivity, and accountability). What appears certain is that risk secrecy challenges the conventional dichotomy between transparency and secrecy, raising a new question on how the legitimacy of protective secrecy can be ensured and controlled.

**References**


Aftergood, S. (2009). Reducing government secrecy: Finding what works. *Yale Law & Policy Review, 27*(2), 399-416.

Aftergood, S. (2010). National security secrecy: How the limits change. *Social Research: An International Quarterly, 77*(3), 839-852.

Agamben, G. (2004). *State of exception*. Chicago: University of Chicago Press.

Albu, O. B., & Flyverbom, M. (2016). Organizational transparency: Conceptualizations, conditions, and consequences. *Business & Society*, 1-30. doi: 10.1177/0007650316659851

Aldrich, R. J., & Moran, C. R. (2019). "Delayed disclosure:" National security, whistle-blowers and the nature of secrecy. *Political Studies, 67*(2), 291-306. doi: 10.1177/0032321718764990

Amiri, A. P. (2014). *Freedom of information and national security. A study of judicial review under US law*. München, Germany: Utz.

Amoore, L., & de Goede, M. (2008). *Risk and the war on terror*. London: Routledge.

Amoore, L. (2011). Data derivatives: On the emergence of a security risk calculus for our times. *Theory, Culture & Society*, *28*(6), 24-43. doi: 10.1177/0263276411417430

Aradau, C. (2004). Security and the democratic scene. *Journal of International Relations and Development, 7*(4), 388-413. doi: 10.1057/palgrave.jird.1800030

Aradau, C. (2016). Risk, in(security) and international politics. In A. Burgess, A. Alemanno, & J. Zinn (Eds.), *Routledge handbook of risk studies* (pp. 290-298). NY: Routledge.

Aradau, C., & van Munster, R. (2007). Governing terrorism through risk: Taking precautions, (un)knowing the future. *European Journal of International Relations, 13*(1), 89-115. doi: 10.1177/1354066107074290

Aradau, C., Lobo-Guerrero, L., & Van Munster, R. (2008). Security, technologies of risk, and the political: Guest editors' introduction. *Security Dialogue, 39*(2-3), 147-154. doi: 10.1177/0967010608089159

Australian Government, Attorney-General's Department. (2018). *Australia protective security policy framework: Sensitive and classified information.* Retrieved from https://www.protectivesecurity.gov.au/information/sensitive-classified-information/Pages/default.aspx

Australian Government, Australian Law Reform Commission. (2004). *Keeping secrets. The protection of classified and security sensitive information* (Report no. 98). Retrieved from https://www.alrc.gov.au/wp-content/uploads/2019/08/ALRC-98.pdf

Australian Government, Australian Law Reform Commission. (2009). *Secrecy laws and open government in Australia* (Report no. 112). Retrieved from https://fas.org/irp/world/australia/secrecy.pdf

Baldwin, D. (1997). The concept of security. *Review of International Studies*, *23*, 5-26. doi: 10.1017/S0260210597000053

Banisar, D. (2007). Public oversight and national security: Comparative approaches to freedom of information. In H. Born & M. Caparini (Eds.), *Democratic control of intelligence services*: *Containing rough elephants*. UK: Ashgate.

Baume, S. & Papadopoulos, Y. (2012, June). *Bentham revisited: Transparency as a 'magic' concept its justifications and its sceptics*. Paper presented at the Transatlantic Conference on Transparency Research, Utrecht University.

Beck, U. (1986). *Risikogesellschaft. Auf dem Weg in eine andere Moderne*. Frankfurt: Suhrkamp.

Beck, U. (2009). *World at Risk*. Cambridge, UK: Polity Press.

Beetham, D. (1991). *The legitimation of power*. UK: Palgrave Macmillan.

Benford, R. D., & Snow, D. A. (2000). Framing processes and social movements: An overview and assessment. *Annual Review of Sociology, 26*, 611-639.

Bennett, C. J. (1991). What is policy convergence and what causes it? *British Journal of Political Science, 21*(2), 215-233. doi: 10.1017/S0007123400006116

Bennett, C., & Howlett, M. (1992). The lessons of learning: Reconciling theories of policy learning and policy change. *Policy Sciences, 25*, 275-294. doi: 10.1007/BF00138786

Berger, P. L., & Luckmann, T. (1967). *The social construction of reality*: *A treatise in the sociology of knowledge*. Harmondsworth: Penguin Books.

Berman, P. (1995). Health sector reform: Making health development sustainable. *Health Policy, 32*, 13-28.

Bigo, D. (2012). Security, surveillance and democracy. In K. Ball, K. D. Haggerty, & D. Lyon (Eds.), *Routledge handbook on surveillance studies* (pp. 277-284). NY: Routledge.

Birchall, C. (2014). Radical transparency. *Cultural Studies Critical Methodologies, 14*(1), 77-88. doi: 10.1177/1532708613517442

Blanton, T. (2003). National security and open government in the United States: Beyond the balancing test. In Campbell Public Affairs Institute (Ed.), *National security and open government: Striking the right balance*. NY: The Maxwell School of Syracuse University.

BMI - Bundesministerium des Inneren. (2006). *Allgemeine Verwaltungsvorschrift zum materiellen und organisatorischen Schutz von Verschlusssachen*. Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/VSA_pdf.pdf?__blob=publicationFile

Bok, S. (1989). *Secrets: On the ethics of concealment and revelation*. NY: Vintage Books.

Brown, D. C. G., & Toze, S. (2017). Information governance in digitized public administration. *Canadian Public Administration*, *60*(4), 581-604. doi: 10.1111/capa.12227

Budäus, D., & Hilgers, D. (2009). Öffentliches Risikomanagement – Zukünftige Herausforderungen an Staat und Verwaltung. In F. Scholz, A. Schuler, & H. Schwintowski (Eds.), *Risikomanagement der öffentlichen Hand* (pp. 17-77). Heidelberg, Germany: Physica.

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Boulder, CO: Lynne Rienner.

Caron, D. J. (2017). La production documentaire dans les administrations publiques : enjeux et pistes de solution. In N. Michaud (Ed.), *Secrets d'États? Les*

*principes qui guident l'administration publique et ses enjeux* contemporains (pp. 807-839). Québec: Presses de l'Université du Québec.

Caron, D. J., & Bernardi, S. (2019). *La gestion de l'information au sein de l'administration publique : essai de typologie*. Rapport de recherche pour la Chaire de recherche en ressources informationnelles de l'École nationale d'admninistration publique, 1-63.

Chambers, S. (2004). Behind closed doors: Publicity, secrecy and the quality of deliberation. *The Journal of Political Philosophy, 12*(4), 398-410. doi: 10.1111/j.1467-9760.2004.00206.x

Chinen, M. (2009). Secrecy and democratic decisions. *Quinnipac Law Review, 27*(1), 1-53. Retrieved from https://ssrn.com/abstract=1302067

Christensen, L. T., & Cheney, G. (2015). Peering into transparency: Challenging ideals, proxies, and organizational practices. *Communication Theory, 25*(1), 70-90. doi: 10.1111/comt.12052

Ciuta, F. (2009). Security and the problem of context: A hermeneutical critique of securitisation theory. *Review of International Studies, 35*(2), 301-326. doi:10.1017/S0260210509008535

Coliver, S. (1998). Commentary to: The Johannesburg Principles on national security, freedom of expression and access to information. *Human Rights Quarterly, 20,* 12-80. doi: 10.1353/hrq.1998.0005

Coliver, S. (2012, December 11). *National security and the right to information*. Testimony presented to the Legal Affairs and Human Rights Committee of the Parliamentary Assembly of the Council of Europe, Paris.

Coliver, S., Hoffman, P., Fitzpatrick, J., & Bowen, S. (1999). *Secrecy and liberty: National security. Freedom of expression and access to information*. The Hague: Martinus Nijhoff Publishers.

Cooper, T. (2004). Big questions in administrative ethics: A need for focused, collaborative effort. *Public Administration Review*, *64*(4), 395-407. doi: 10.1111/j.1540-6210.2004.00386.x

Copp, D. (1999). The idea of a legitimate state. *Philosophy & Public Affairs*, *28*(1), 3-45. doi: 10.1111/j.1088-4963.1999.00003.x

Corry, O. (2012). Securitisation and "riskification:" Second-order security and the politics of climate change. *Millennium*, *40*(2), 235-258. doi: 10.1177/0305829811419444

Costas, J., & Grey, C. (2014). Bringing secrecy into the open: Towards a theorization of the social processes of organizational secrecy. *Organization Studies*, *35*(10), 1423-1447. doi: 10.1177/0170840613515470

Cottier, B., & Masson, N. (2013). Le domaine de la sécurité ou comment concilier confidentialité légitime et transparence nécessaire. In M. Pasquier (Ed.), *Le principe de transparence en Suisse et dans le monde* (pp. 233-254). Lausanne: La fondation des presses polytechniques et universitaires romandes.

Coyne, J., & Meurant-Tompkinson, A. (2018, February 19). Security is not a dirty word. *The Strategist — The Australian Strategic Policy Institute Blog*. Retrieved from https://www.aspistrategist.org.au/security-not-dirty-word/

Curtin, D. (2014). Overseeing secrets in the EU: A democratic perspective. *Journal of Common Market Studies*, *52*(3), 684-700. doi: 10.1111/jcms.12123

Curtin, D., & Meijer, A. (2006). Does transparency strengthen legitimacy? A critical analysis of European Union policy documents. *Information Polity, 11*(2), 109-122. doi: 10.2139/ssrn.1434862

Dandeker, C. (1994). National security and democracy: The United Kingdom experience. *Armed Forces & Society, 20*(3), 353-374. doi: 10.1177/0095327X9402000303

Davis, J. (1998). Access to and transmission of information: Position of the media. In V. Deckmyn & I. Thomson (Eds.), *Openness and Transparency in the European Union* (pp. 121-126). Maastricht, Netherlands: European Institute of Public Administration.

de Fine Licht, J. (2014). Policy area as a potential moderator of transparency effects: An experiment. *Public Administration Review, 74*(3), 361-371. doi: 10.1111/puar.12194

Dean, M. (1999). *Governmentality: Power and rule in modern society*. London: Sage.

Doty, P. (2015). U.S. homeland security and risk assessment. *Government Information Quarterly, 32*, 342-352. doi: 10.1016/j.giq.2015.04.008

Elman, C., & Jensen, M. (2014). *The realism reader*. London, UK: Routledge.

Everts, P. P. (2002). *Democracy and military force*. London, UK: Palgrave.

Ewald, F. (1991). Insurance and risk. In G. Burchell, C. Gordon, & P. Miller (Eds.), *The Foucault effect: Studies in governmentality* (pp. 197-210). Chicago, IL: University of Chicago Press.

Fenster, M. (2006). The opacity of transparency. *Iowa Law Review*, 91.

Fenster, M. (2014). The implausibility of secrecy. *Hastings Law Journal*, *65*(2), 309-363. doi: 10.2139/ssrn.2220376

Fenster, M. (2015). Transparency in search of a theory. *European Journal of Social Theory*, *18*(2), 150-167. doi: 10.1177/1368431014555257

Fleischer, J. (2013). Time and crisis. *Public Management Review*, *15*(3), 313-329. doi: 10.1080/14719037.2013.769852

Florini, A. (1998). The end of secrecy. *Foreign Policy,* (111), 50-63. doi:10.2307/1149378

Flyverbom, M., Christensen, L. T., & Hansen, H. K. (2015). The transparency–power nexus: Observational and regularizing control. *Management Communication Quarterly*, *29*(3), 385-410. doi: 10.1177/0893318915593116

Földes, A. (2014). Classified information. A review of current legislation across 15 countries. *Transparency International Corruption Risks Series*. Retrieved from http://ti-defence.org/wp-content/uploads/2016/03/140911-Classified-Information.pdf

Freedman, L. (1998). International security. Changing targets. *Foreign Policy, 110*, 48. doi: 10.2307/1149276

Gibbs, D. N. (1995). Secrecy and international relations. *Journal of Peace Research*, *32*(2), 213-228. doi: 10.1177/0022343395032002007

Goffman, E. (1974). *Frame analysis: An essay on the organization of experience*. Cambridge, MA: Harvard University Press.

Grimmelikhuijsen, S., Porumbescu, G., Hong, B., & Im, T. (2013). The effect of transparency on trust in government: A cross-national comparative

experiment. *Public Administration Review, 73*(4), 575-586. doi: 10.1111/puar.12047

Gwyn, C. (2018). A review of the New Zealand Classification System. *The Inspector-General of Intelligence and Security*. Retrieved from http://www.igis.govt.nz/assets/Uploads/Classification-Review-Report.pdf

Hall, P. (1993). Policy paradigms, social learning, and the state: The case of economic policymaking in Britain. *Comparative Politics, 25*(3), 275-296. doi:10.2307/422246

Hammerstad, A., & Boas, I. (2015). National security risks? Uncertainty, austerity and other logics of risk in the UK government's National Security Strategy. *Cooperation and Conflict, 50*(4), 475-491. doi: 10.1177/0010836714558637

Hardy, C., & Maguire, S. (2015). Organizing risk: Discourse, power, and "riskification." *Academy of Management Review, 41*(1), 80-108. doi: 10.5465/amr.2013.0106

Hay, C. (2011). Interpreting interpretivism interpreting interpretations: The new hermeneutics of public administration. *Public Administration, 89*(1), 167-182. doi: 10.1111/j.1467-9299.2011.01907.x

Heide, M., & Worthy, B. (2019). Secrecy and Leadership: The Case of Theresa May's Brexit Negotiations. *Public Integrity, 21*(6), 582-594. doi: https://doi.org/10.1080/10999922.2019.1609273

Herman, M. (1996). *Intelligence power in peace and war*. UK: Cambridge University Press.

Hill, C. (2011). Foreign policy analysis. In B. Badie, D. Berg-Schlosser, & L. Morlino (Eds.), *International encyclopedia of political science*. Thousand Oaks, CA: SAGE Publications, Inc.

Hitz, F. P., & Weiss, B. J. (2004). Helping the CIA and FBI connect the dots in the War on Terror. *International Journal of Intelligence and Counterintelligence, 17*(1), 1-41. doi: 10.1080/08850600490252641

Holzinger, K., & Knill, C. (2005). Causes and conditions of cross-national policy convergence. *Journal of European Public Policy, 12*(5), 775-796. doi: 10.1080/13501760500161357

Hood, C. (2007). What happens when transparency meets blame-avoidance? *Public Management Review, 9*(2), 191-210. doi: 10.1080/14719030701340275

Hood, C. C. (1983). *The tools of government.* London: Palgrave MacMillan.

Horn, E. (2011). Logics of political secrecy. *Theory Culture Society, 28*(7-8), 103-122. doi: 10.1177/0263276411424583

Huntington, S. P. (1957). *The soldier and the state. The theory and politics of civil-military relations*. NY, United States: Vintage Books.

Hurrelmann, A. (2017). Empirical legitimation analysis in international relations: How to learn from the insights – and avoid the mistakes – of research in EU studies. *Contemporary Politics, 23*(1), 63-80. doi: 10.1080/13569775.2016.1213077

Huysmans, J. (1998). A question of the Limit: Desecuritisation and the aesthetics of horror in political realism. *Millennium, 27*(3), 569-589. doi: 10.1177/03058298980270031301

ICO - Information Commissioners Office. (2017). *The guide to freedom of information*. Retrieved from https://ico.org.uk/media/for-organisations/guide-to-freedom-of-information-4-9.pdf

IFG - German Freedom of Information Law. Gesetz zur Regelung des Zugangs zu Informationen des Bundes (IFG). Retrieved from https://www.gesetze-im-internet.de/ifg/BJNR272200005.html

Independent. (2013, October 17). *The secret's out: Whitehall's document classification system devised to thwart German spies in WWII*. Retrieved from https://www.independent.co.uk/incoming/the-secret-s-out-whitehall-s-document-classification-system-devised-to-thwart-german-spies-in-wwii-8884923.html

International Organization for Standardization & International Electrotechnical Commission. (2018). *Information technology—Security techniques—Information security management systems—Overview and vocabulary* (ISO ISO/IEC 27000:2018). Retrieved from https://www.iso.org/standard/73906.html

International Organization for Standardization. (2012). *Societal security—Business continuity management systems—Guidance* (ISO 22313:2012). Retrieved from https://www.iso.org/standard/50050.html

International Organization for Standardization. (2012). *Societal security—Business continuity management systems—Requirements* (ISO 22301:2012). Retrieved from https://www.iso.org/standard/50038.html

Jaeger, P. T., & Burnett, G. (2005). Information access and exchange among small worlds in a democratic society: The role of policy in redefining information behavior in the post-9/11 United States. *The Library Quarterly, 75*(4), 464-495.

Janis, I. L. (1972). *Victims of groupthink: A psychological study of foreign-policy decisions and fiascos*. New York, United States: Houghton Mifflin.

Junk, J., & Daase, C. (2013). Germany. In H. Biehl, B. Giegerich, & A. Jonas (Eds.), *Strategic cultures in Europe: Security and defense policies across the continent* (pp.139-152). Wiesbaden: Springer.

Knecht, T., & Weatherford, M. S. (2006). Public opinion and foreign policy: The stages of presidential decision making. *International Studies Quarterly, 50*(3), 705-727.

Krahmann, E. (2011). Beck and beyond: Selling security in the world risk society. *Review of International Studies, 37*, 349–372. doi: 10.1017/S0260210510000264

Lawlor, L., & Nale, J. (Eds.). (2014). *The Cambridge Foucault lexicon*. Cambridge: Cambridge University Press. doi:10.1017/CBO9781139022309

Leterre, T. (2011). Contract theory. In B. Badie, D. Berg-Schlosser, & L. Morlino (Eds.), *International encyclopedia of political science* (pp. 437-447). Thousand Oaks, CA: SAGE Publications.

Lippmann, W. (1955). *Essays in the public philosophy*. Boston: Little Brown.

Loader, I., & Walker, N. (2007). *Civilizing security*. Cambridge: Cambridge University Press.

Lowery, T. (2011). Prerogative. In G. Kurian & T. George (Eds.), *The encyclopedia of political sciences*. Washington: CQ Press.

Mansbrige, J. (2009). A "selection model" of political representation. *The Journal of Political Philosophy, 17*(4), 369-398. doi: 10.1111/j.1467-9760.2009.00337.x

Maytech. (2018). *What is IL3 accreditation and why are we getting it*. Retrieved from www.maytech.net/blog/what-is-il3-accreditation-and-why-are-we-getting-it/

McClean, T. (2011). *Shackling leviathan. A comparative historical study of institutions and the adoption of freedom of information* (Doctoral dissertation). The London School of Economics and Political Science. Retrieved from http://etheses.lse.ac.uk/3102/

Mearsheimer, J. J. (1990). Back to the future. Instability in Europe after the Cold War. *International Security, 15,* 5-56.

Meijer, A. (2013). Understanding complex dynamics of transparency. *Public Administration Review, 73*(3), 429-439. doi: 10.1111/puar.12032

Meijer, A., ’t Hart, P., & Worthy, B. (2018). Assessing government transparency: An interpretive framework. *Administration & Society, 50*(4), 501-526. doi: 10.1177/0095399715598341

Moran, C. (2013). *Classified: Secrecy and the state in modern Britain*. NY: Cambridge University Press.

Morgenthau, H. J. (1967). *Politics amongst nations*. New York, United States: Knopf.

Naurin, D. (2007). Transparency, publicity, accountability—The missing links. *Swiss Political Science Review, 12*(3), 90-98.

New Zealand Department of the Prime Minister and Cabinet. (NZ DPMC). (2002). *Security in the government sector (SIGS)*. Retrieved from https://www.gcsb.govt.nz/assets/GCSB-Documents/Security-in-the-Government-Sector-2002.pdf

New Zealand Department of Prime Minister and Cabinet (NZ DPMC). (2018a). Government Security Classification System: Overview of security classifications. Retrieved from https://www.protectivesecurity.govt.nz/information-security/classification-system-and-handling-requirements/classification-system/overview/

New Zealand Department of Prime Minister and Cabinet (NZ DPMC). (2018b). Government Security Classification System: Security classifications for national security information. Retrieved from https://www.protectivesecurity.govt.nz/information-security/classification-system-and-handling-requirements/classification-system/national-security-information/

New Zealand Department of Prime Minister and Cabinet (NZ DPMC). (2018c). Government Security Classification System: Security classifications for policy and privacy information. Retrieved from https://www.protectivesecurity.govt.nz/information-security/classification-system-and-handling-requirements/classification-system/policy-and-privacy-information/

New Zealand Department of Prime Minister and Cabinet (NZ DPMC). (2018d). Protective Security Requirements: Guidelines for protective markings. Retrieved from https://www.protectivesecurity.govt.nz/information-security/classification-system-and-handling-requirements/classification-system/guidelines/

New Zealand Department of Prime Minister and Cabinet (NZ DPMC). (2018e). Protective Security Requirements: Why information security matters. Retrieved from https://www.protectivesecurity.govt.nz/information-security/why-information-security-matters/

New Zealand Department of Prime Minister and Cabinet (NZ DPMC). (2018f). Protective Security Requirements: Management protocol for information security. Retrieved from https://www.protectivesecurity.govt.nz/information-security/management-protocol/

O'Malley, P. (2010). Uncertain subjects: Risks, liberalism and contract. *Economy and Society, 29*(4), 460-484. doi: 10.1080/03085140050174741

O'Neill, O. (2006). Transparency and the ethics of communication. In C. Hood & D. Heald (Eds.), *Transparency: The key to better governance?* (pp. 74-90). British Academy.

Olmastroni, F. (2014). *Framing war: Public opinion and decision-making*. New York: Routledge.

Open Society Foundation (OSF). (2013). *The global principles on national security and the right to information*. Retrieved from https://www.justiceinitiative.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles

Pasquier, M., & Villeneuve, J. P. (2007). Organizational barriers to transparency: A typology and analysis of organizational behaviour tending to prevent or restrict access to information. *International Review of Administrative Sciences, 73*(1), 147-162. doi: 10.1177/0020852307075701

Perkovich, G., & Levite, A. E. (2017). *Understanding cyber conflict: Fourteen analogies*. Washington, D.C.: Georgetown University Press.

Petersen, K. L. (2011). Risk analysis – A field within security studies? *European Journal of International Relations, 18*(4), 693-717. doi: 10.1177/1354066111409770

Posner, E. A., & Vermeule, A. (2007). *Terror in the balance: Security, liberty and the courts*. Oxford: Oxford University Press.

Power, M. (2004). *The risk management of everything: Rethinking the politics of uncertainty*. London: Demos.

Pozen, D. (2010). Deep secrecy. *Stanford Law Review, 62*(2), 257-340.

Prat, A. (2005). The wrong kind of transparency. *The American Economic Review, 95*(3), 862-877. doi: 10.1257/0002828054201297

Prat, A. (2006). The more closely we are watched, the better we behave? In C. Hood & D. Heald (Eds.), *Transparency: The Key to Better Governance?* (pp. 91-103). Oxford: Oxford University Press.

Quill, L. (2014). *Secrets and democracy - From Arcana Imperii to WikiLeaks*. UK: Palgrave Macmillan.

Rasmussen, M. V. (2006). *The risk society at war: Terror, technology and strategy in the twenty-first century*. Cambridge: Cambridge University Press.

Rasmussen, M. V. (2001). Reflexive security: NATO and international risk society. *Millennium, 30*(2), 285-309. doi: 10.1177/03058298010300020901

Reddy, S. G. (2006). Claims to expert knowledge and the subversion of democracy: The triumph of risk over uncertainty. *Economy and Society, 25*(2), 222-254. doi: 10.1080/03085149600000011

Relyea, H. C. (2003). Government secrecy: Policy depths and dimensions. *Government Information Quarterly, 20*(4), 395-418. doi: 10.1016/j.giq.2003.09.001

Rittberger, B., & Goetz, K. H. (2018). Secrecy in Europe. *West European Politics, 41*(4), 825-845. doi: 10.1080/01402382.2017.1423456

Roberts, A. (2012). WikiLeaks: The illusion of transparency. *International Review of Administrative Sciences, 78*(1), 116-133. doi: 10.1177/0020852311429428

Robins, C. (2014). UK government security classification scheme. *Cybermatters.* Retrieved from https://cybermatters.info/2014/04/01/uk-government-security-classification-scheme/

Roe, P. (2012). Is securitization a "negative" concept? Revisiting the normative debate over normal versus extraordinary politics. *Security Dialogue, 43*(3), 249-266. doi: 10.1177/0967010612443723

Rose, N., & Miller P. (2008). *Governing the present: Administering economic, social and personal life*. Cambridge: Polity Press.

Rose, N., & Miller, P. (1992). Political power beyond the State: problematics of government. *British Journal of Sociology, 43*(2), 173-205. doi: 10.2307/591464

Rourke, F. (1957). Secrecy in American bureaucracy. *Political Science Quarterly, 72*(4), 540-564. doi: 10.2307/2146193

Sagar, R. (2012). *Should we fear state secrecy?* Retrieved from https://cuptw.files.wordpress.com/2012/10/sagar-secrecy-columbia-oct-18-2012.doc

Sagar, R. (2013). *Secrecy and leaks: The dilemma of state secrecy*. Princeton: Princeton University Press.

Schauer, F. (2001). *Transparency in three dimensions, annotated version of the David C. Baum memorial lecture on civil rights and civil liberties.*

Paper presented at the University of Illinois College of Law on November 11, 2010. Retrieved from https://illinoislawreview.org/wp-content/ilr-content/articles/2011/4/Schauer.pdf

Schoenfeld, G. (2010). *Necessary secrets: National security, the media and the rule of law*. NY: Norton & Co.

Schön, D., & Rein, M. (1996). Frame-critical policy analysis and frame-reflective policy practice. *Knowledge and Policy, 9*(1), 85-104. doi: 10.1007/BF02832235

Schulhofer, S. (2010). Secrecy and democracy: Who controls information in the national security state? *University public law research papers*, no.10-53, Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1661964

Seifert, J. W. (2004). Data mining and the search for security: Challenges for connecting the dots and databases. *Government Information Quarterly, 21*(4), 461-480. doi: 10.1016/j.giq.2004.08.006

Stiglitz, J. (1999). On liberty, the right to know, and public discourse: The role of transparency in public life. *Oxford Amnesty Lecture.* Retrieved from http://www.internationalbudget.org/wp-content/uploads/On-Liberty-the-Right-to-Know-and-Public-Discourse-The-Role-of-Transparency-in-Public-Life.pdf

Stone, D. (1999). *The policy paradox. The art of political decision making*. NY: Norton & Co.

Streeck, W., & Thelen, K. (2005). *Beyond continuity: Institutional change in advanced political economies*. Oxford, United Kingdom: Oxford University Press.

Strickland, L. S. (2005). The information gulag: Rethinking openness in times of national danger. *Government Information Quarterly, 22*(4), 546-572. doi: 10.1016/j.giq.2006.01.005

Strutt, N. (2016). *Whitepaper on the government classification scheme*. Retrieved from http://advisec.co.uk/wp-content/uploads/2016/10/Government-Classification-scheme-draft-2-1.pdf

Summersby, A., Hemming, T., & Wright, M. (2018, October 4). Security maturity: A new protective security policy framework. *Ashurst*. Retrieved from https://www.ashurst.com/en/news-and-insights/legal-updates/security-maturity-a-new-protective-security-policy-framework/

Sunstein, C. R. (1986). Government control of information. *California Law Review, 74*(3), 889-921. doi: 10.15779/Z389160

Taureck, R. (2006). Securitization theory and securitization studies. *Journal of International Relations and Development,* (9), 53-61.

Teurlings, J., & Stauff, M. (2014). Introduction: The transparency issue. *Cultural Studies - Critical Methodologies, 14*(1), 3-10. doi: 10.1177/1532708613519184

Thompson, D. F. (1999). Democratic secrecy. *Political Science Quarterly, 114*(2), 181-193. doi: 10.2307/2657736

UK Cabinet Office. (2018a). *HMG security policy framework*. Retrieved from https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework

UK Cabinet Office. (2018b). *Government security classifications*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/

attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf

UK Government. (2014). *Whitehall starts using simpler security classifications*. Retrieved from https://www.gov.uk/government/news/whitehall-starts-using-simpler-security-classifications

van Hulst, M. J., & Yanow, D. (2016). From policy "frames" to "framing:" Theorizing a more dynamic, political approach. *The American Review of Public Administration, 46*(1), 92-112. doi: 10.1177/0275074014533142

Villeneuve, J. P. (2014). Transparency of Transparency: the pro-active disclosure of the rules governing. Access to Information as a gauge of organisational cultural transformation. *Government Information Quarterly, 31*(4), 556-562. doi: https://doi.org/10.1016/j.giq.2013.10.010

Villeneuve, J. P., Meier, A., & Pasquier M. (2014, June). *European Science Foundation*. Final report, Lausanne, presented at the Exploratory Workshop on Government Transparency.

Wadham, J., & Modi, K. (2003). National security and open government in the United Kingdom. In Campbell Public Affairs Institute (Ed.), *National security and open government: Striking the right balance*. New York: The Maxwell School of Syracuse University.

Waldron, J. (1993). *Liberal rights: Collected papers 1981–1991*. Cambridge: Cambridge University Press.

Waltz, K. N. (1979). *Theory of international politics*. Reading, Mass.: Addison-Wesley.

Ward, K. (2007). The fog of war: Checks and balances and national security policy. *Maryland Law Review, 67*(1). Retrieved from https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1058&context=schmooze_papers

Whigham, J. (2013). Classification system updates. *Defence*. Retrieved from https://www.defence.gov.au/defencemagazine/issue/9/articles/17.html

Whigham, J. (2012). New security classifications. *Defence*. Retrieved from https://www.defence.gov.au/defencemagazine/working/issue/4/articles/10.html

Williams, M. (1998). Identity and the politics of security. *European Journal of International Relations*, *4*(2), 204-225. doi: 10.1177/1354066198004002003

Wolfers, A. (1952). "National security" as an ambiguous symbol. *Political Science Quarterly*, *67*(4), 481-502. doi: 10.2307/2145138

Worthy, B. (2015). What is transparency? Retrieved from http://www.freedominfo.org/2015/09/what-is-transparency/

Worthy, B. (2017). *On the politics of freedom of information*. Manchester: Manchester University Press.

***Note:*** *Access for all online resources has been verified in July 2019.*