An Examination of the Discursive Construction of Bulk Surveillance as a Societal Issue in the UK (2013 – 2021)

Silviu Cristian Paicu

A thesis submitted in partial fulfilment of the requirements for the Doctor of Philosophy in Information Policy and Governance at the Faculty of Media and Knowledge Sciences

University of Malta

2023

FACULTY/INSTITUTE/CENTRE/SCHOOL: Faculty of Media & Knowledge Sciences

DECLARATION OF AUTHENTICITY FOR DOCTORAL STUDENTS

(a) Authenticity of Thesis/Dissertation

I hereby declare that I am the legitimate author of this Thesis/Dissertation and that it is my original work.

No portion of this work has been submitted in support of an application for another degree or qualification of this or any other university or institution of higher education.

I hold the University of Malta harmless against any third party claims with regard to copyright violation, breach of confidentiality, defamation and any other third party right infringement.

(b) Research Code of Practice and Ethics Review Procedure

I declare that I have abided by the University's Research Ethics Review Procedures.
Research Ethics & Data Protection form code Not applicable - ethically reviewed by MVNIA.

☑ As a Ph.D. student, as per Regulation 66 of the Doctor of Philosophy Regulations, I accept that my thesis be made publicly available on the University of Malta Institutional Repository.

□ As a Doctor of Sacred Theology student, as per Regulation 17 (3) of the Doctor of Sacred Theology Regulations, I accept that my thesis be made publicly available on the University of Malta Institutional Repository.

□ As a Doctor of Music student, as per Regulation 26 (2) of the Doctor of Music Regulations, I accept that my dissertation be made publicly available on the University of Malta Institutional Repository.

□ As a Professional Doctorate student, as per Regulation 55 of the Professional Doctorate Regulations, I accept that my dissertation be made publicly available on the University of Malta Institutional Repository.

02.2023

Abstract

The aim of this thesis is to investigate the discursive construction of the issue of bulk surveillance as a societal topic in the UK after 2013, by focusing on the stakeholders involved in this process. Analysing and bringing to light the existent discourses on bulk surveillance is a way to understand how the relationship between democracy and security in the UK is being reconfigured in the context of new and emerging technologies of surveillance. The debate on bulk surveillance at society level in the UK, provides a ground-breaking framework for researching the dynamics between intelligence and its democratic oversight in an advanced democracy.

The study employs the tool of critical discourse analysis in order to map the discursive landscape of the public debate on bulk surveillance and approaches the topic from the normative angle of democratic intelligence governance. As explained in Chapter 1, the thesis operates within a critical theory framework, aiming to make a theoretical contribution to an emerging corpus of research known as critical intelligence studies. Chapter 2 investigates the proliferation of bulk surveillance regimes in the post-Snowden age by focusing on their historical, conceptual, operational and regulatory aspects. Chapter 3 explores how an intelligence agency, i.e. GCHQ, has mobilized a discourse on bulk surveillance, assembled around the ideas of uniqueness of expertise and knowledge authority. Chapter 4 argues that intelligence oversight expert bodies, i.e. IPCO, could play a pivotal role in democracies, by shaping the public understanding of intelligence practices. Chapter 5 represents the empirical section of the thesis, involving a process of discourse mapping with the help of a qualitative text-processing software.

The debate on bulk surveillance had a transformative impact on the way intelligence community in the UK construe themselves in the public space, as part of the democratic framework. In the case of the intelligence discourse, we found that bulk surveillance is framed as a legitimate solution to security threats. By employing a discourse featuring references to oversight and human rights, the intelligence actors manage to defuse the critique from civil society. Another finding is that in the intelligence discourse, democracy and human rights are now taking precedence over more traditional references to national security. The empirical analysis revealed significant discursive compatibility between civil society organisations, academia and intelligence oversight. We also found that references to human rights and democratic principles, are a common discursive ground for all the stakeholders taking part in this debate. The overall results of the research indicate that the debate on bulk surveillance in the UK has been the driving force behind some important transformations of intelligence and its oversight, with significant implications for the democratic norms and mechanisms.

Acknowledgements

I would like to express my deepest gratitude to my supervisors: Prof. Joseph Cannataci, Prof. Irena Chiru and Dr Aitana Radu, for their guidance and patience and for the great deal of assistance and support I received during my research journey.

In addition, special thanks go to Dr Cristina Ivan, Dr Valentin Stoian, Dr Mihail Chiru and Prof. Noellie Brockdorff, for their assistance and feedback along the way.

Many thanks to all my wonderful colleagues and friends from the ESSENTIAL Project.

Table of Contents

LIST OF ABBREVIATIONS

BBW	Big Brother Watch
BPD	Bulk Personal Datasets
CJEU	Court of Justice of the European Union
CSP	Communications Service Providers
ECtHR	European Court of Human Rights
EI	Equipment Interference
FISA	The Foreign Intelligence Surveillance Act of 1978
FLAG	Fiber-Optic Link Around the Globe
FRA	European Union Agency for Fundamental Rights
GCHQ	Government Communications Headquarters
IIOF	International Intelligence Oversight Forum
IPA	Investigatory Powers Act 2016
IPCO	Investigatory Powers Commissioner's Office
IPT	Investigatory Powers Tribunal
IRTL	Independent Reviewer of Terrorism Legislation
ISA	Intelligence Services Act 1994
ISC	Intelligence and Security Committee
LEA	Law Enforcement Agency
MVR	Massive Volume Reduction
NAS	National Academy of Sciences
NGO/CSO	Non-Government Organizations / Civil Society Organizations

NSA	National Security Agency
PET	Privacy-Enhancing Technologies
PI	Privacy International
RUSI	Royal United Services Institute
SIGINT	Signals Intelligence
SIS	Security and Intelligence Services
VPN	Virtual Private Network

LIST OF FIGURES

INTRODUCTION

As security and intelligence services' bulk data collection practices have become an increasingly present and pressing issue in contemporary democracies, the debate surrounding their use has engaged a variety of societal actors. This has created a dynamic of competing narratives, whose impact on the societal debate and public policy governing the use of these technologies remains largely unexplored.

To explore the impact of these different narratives, this dissertation starts by giving a brief historical overview of intelligence technologies of bulk collection. This is followed by an investigation of the proliferation of bulk collection regimes in the post-Snowden age, focusing on the conceptual, operational and regulatory aspects of these surveillance techniques and their impact on citizens' fundamental rights.

Next, we examine the importance of epistemic diversity for democratic intelligence governance by highlighting the role of academia. Specifically, we explore how the expertise of critically engaged scholars can play a leading role in challenging the expert discourse of intelligence agencies in the age of Big Data and AI proliferation. The chapter examines how the intelligence expert discourse is constructed in the post-Snowden landscape in the UK by investigating the public communication strategies of GCHQ. Driven by a normative rhetoric centred on transparency, the agency's unprecedented steps towards public engagement are traced through an analysis of key policy documents, official statements, and a museum exhibition. In the ensuing and novel context of openness and widespread discursivity around controversial technologies and practices employed by intelligence agencies, critically engaged academia can bring a much-needed diversity of perspective to an increasingly complex and vital policy area in contemporary democratic societies.

The Snowden revelations concerning the use of bulk data collection have uncovered shortcomings in the existing intelligence accountability structures in several leading

democracies and confronted them with a variety of new challenges generated by rapid technological advances. The impact of the disclosures has also been reflected in scholarship, namely in the way intelligence oversight is being reconceptualized as a broader form of governance beyond legal compliance. Chapter 4 examines the case of the UK and investigates instances when the two main oversight institutions, namely IPCO and the ISC, have been shaping the public debate through their published reports and their engagement with civil society actors. The chapter argues that expert oversight institutions are better equipped for shaping the democratic debate on bulk surveillance than any other societal actors due to their configuration of institutional features and statutory power. Empowering existing or creating new independent entities with access to classified information and reliant on technical expertise is the way forward for democratic governance of intelligence services.

A discourse approach: Frames, metaphors, and narratives

The present study adopts discourse analysis as its main research method. As such, it follows the research agenda of critical intelligence studies, which observes intelligence as a "rhetorically conveyed and textually constituted field" in which "ambiguous discourse, not objective truth, is the fluctuating currency" (Der Derian, 1993, pp.36-37).

The narrative struggle unfolds at different levels and involving different dynamics between the societal stakeholders identified as being part of the expert debate on bulk data collection. For the purpose of this study, these actors are academia, civil society organizations, judicial courts, intelligence oversight bodies, and the intelligence community. Given the conceptualisation of the present research in terms of discourse theory, these actors occupy the positions of speakers. Focusing on their discursive engagements with the controversial issue of bulk surveillance in various forms (reports, speeches, key passages, written submissions) also involves looking at what interests, resources and strategies they mobilize.

The narrative analysis starts by tackling the terminological confusion between "bulk collection" and "mass surveillance". We argue that these terms are loaded with normative meaning and represent two opposing discourses. Intelligence actors and other institutions from the governmental sphere have formalized a preference for the terms 'bulk collection' and 'bulk powers', while critical voices from civil society and academia primarily use the term 'mass surveillance' or other terms with similarly negative undertones, such as 'dragnet

surveillance'. In Chapter 2 we investigate how these narratives are reflected in an etymological debate. According to a prominent critical scholar, the term 'collection' is preferred by intelligence agencies for its ambiguity, being used for shunning the criticism associated with mass surveillance but also as an umbrella term for a range of practices including data analytics (Aradau, 2017). The same ambiguity applies to the term 'bulk', a word generally associated more with commodities and less with people, which is then used to obscure any suggestion of surveillance undertaken by humans (Aradau, 2017, p. 337). As our research will show, the choice of the words is important because it evokes certain meanings in support of different narratives.

Another pair of competing narratives, this time at the conceptual level, refers to what constitutes "surveillance". The narrative preferred by intelligence actors is that surveillance happens only when a human analyst is involved in the examination process of the collected data. According to this framing, surveillance is always targeted because human agency occurs only after the initial algorithmic filtering. The justificatory discourse is thus grounded on a fundamental distinction between humans and machines (Aradau & Blanke, 2015). Not only does such a distinction in this context trigger ethical and philosophical questions, but it also evokes tropes reminiscent of science-fiction's classic scenarios of machines vs. humans. Civil liberties activists and critical scholars reject this discourse by stating that surveillance occurs in the initial phase when the data is first collected. As one scholar wrote, "to reclaim human rights in a world governed by technology, we must understand how power is delegated to technological system" (Jassanof, 2016, p. 12).

In chapter 3, we aim to understand how an intelligence agency, i.e. GCHQ, mobilizes a post-Snowden discourse assembled around the ideas of uniqueness of expertise and knowledge authority in dealing with Big Data and bulk collection technologies. Using the tools of narrative analysis, we analyse a museum exhibition organised by the GCHQ in 2019 to mark its centenary. We argue that the exhibition is a good example of a narrative practice used to present, for the first time in its existence, the story of the agency's work to the public. Shared among the exhibitions' sections was a common focus on how GCHQ's work has always been closely related to science, at the forefront of technological innovation from the breaking of the Enigma code to contemporary practices of data-driven security. We then show how the justificatory discourses of intelligence actors and their expert credibility are being challenged by an epistemic community of critically engaged academics working at the confluence of social sciences and information sciences. A

contestation on epistemological grounds of the hegemony of intelligence expert discourse enriches the ongoing societal debate on bulk collection technologies and is a key part in the process of attaining democratic intelligence governance.

Methodology

The post-Snowden landscape in the UK in the regulatory field of intelligence and security has been characterised by a state of competing discourses attempting to constitute the phenomenon of bulk surveillance with important effects on the future of democracy. The present study follows the research agenda of critical intelligence studies and it belongs to the field of qualitative empirical social research. As such, methodologically we adopt a discourse analysis approach applied to the empirical case-study of governmental bulk surveillance in the UK post 2013.

Discursive field

A discursive field refers to "the arena in which different discourses compete for the constitution or definition of a phenomenon" (Keller, 2013, p. 72). In our case, the phenomenon is *the governmental practice of bulk surveillance*. As Snow (2013) observed, discursive fields "encompass cultural materials (e.g., beliefs, values, ideologies, myths) of potential relevance and various sets of actors (e.g., targeted authorities, social control agents, countermovements, media) whose interests are aligned, albeit differently, with the issues or events in question, and who thus have a stake in how those events and issues are framed and/or narrated." (p. 1). In our study, the discursive field is shaped in the form of an expert public debate on the governmental practice of bulk surveillance between a number of relevant societal stakeholders. Snow (2013) proposed an expanded conceptual understanding of discursive fields, presenting a four-fold typology matrix (see Figure 1) based on the system of relations among the actors involved in the debate:

a) the emergent/structured continuum

   Structured fields are characterised through order and stability derived from a legitimated system of relations among actors. Contrariwise, emergent fields are unstable due to the emerging nature of some actors and the system of relations among them or when the existing system is fading due to contestation among the stakeholders.

b) the consensual/contested continuum

The scale of variation of agreement and disagreement between the actors on the societal issue discussed.

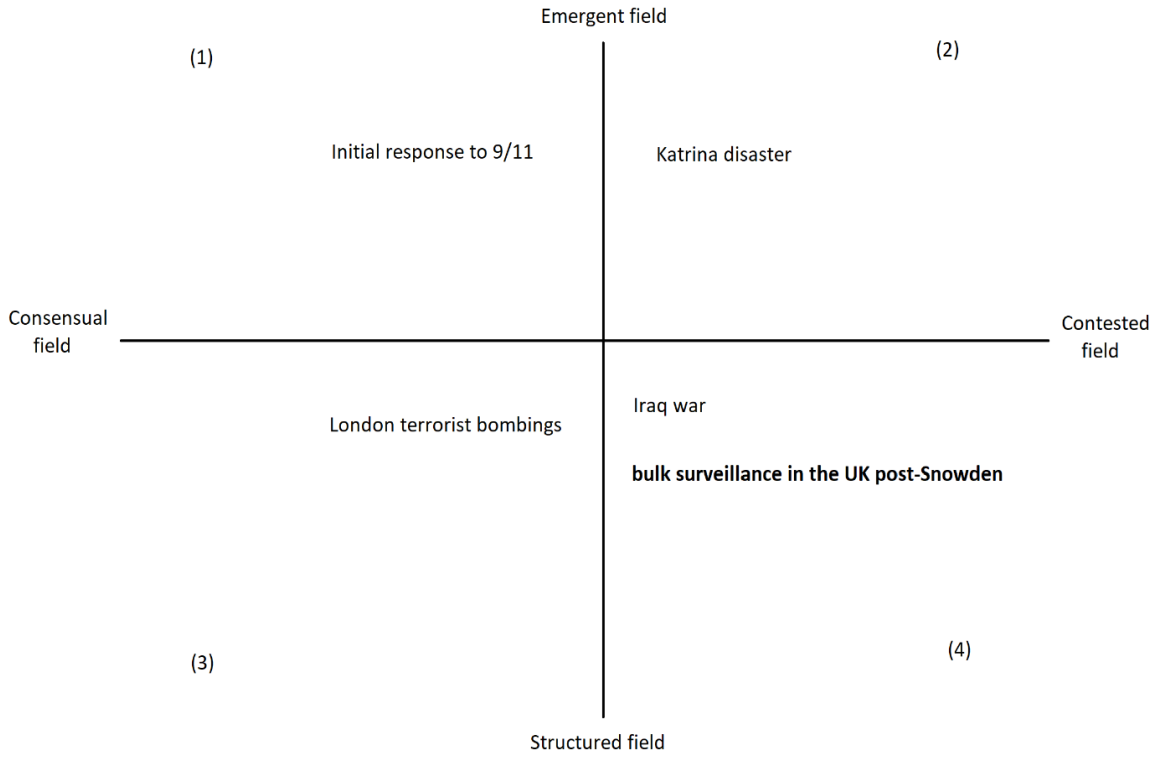

Figure 1: Discursive fields (adapted from Snow, 2013, p. 3).

As we can observe in Figure 1, we chose to place the issue of governmental bulk surveillance in the UK post-Snowden in cell 4. This means that in our case, the discursive field is structured to a certain degree institutionally but there is also a considerable degree of contestation regarding the practice of bulk surveillance. In other words, there is still a lot of disagreement between the actors on *when* to use the bulk powers (e.g. legal/oversight framing) or *whether* to use them at all (e.g. civil society framing). The system of relations among the collective actors in this expert debate has been shifting significantly in light of the 2013 Snowden revelations but also due to contestation among some of the stakeholders, mainly civil society organisations strongly contesting the framing promoted by security and intelligence actors. However, the system of relations between the actors in our case remains structured given its embeddedness in organizational and institutional settings as it is the

case with intelligence oversight and courts. Even civil society organizations like Privacy International have also developed a more patterned way of contesting the governmental framing of bulk surveillance trough litigation and advocacy. Hence, the discursive field that we are focusing on in our research is composed by diverse stakeholders with some divergent views that are involved in this expert debate on bulk surveillance. In this sense, we are operating with a type of discursive field marked by fragmentation into "conflict and alliance systems" (Snow, 2013, p. 3).

Discourse analysis

The use of bulk collection technologies by security and intelligence agencies is a matter of societal relevance in advanced democracies like the UK. Examining through the lenses of discourse analysis fits our research purpose given that discourses "often touch on questions and problems of special societal relevance, notably the existential moral and political questions of larger communities" (Angermuller, 2015, p. 510). The different discourses on the topic of bulk surveillance shape the way this novel phenomenon is understood by the public. Precisely, discourses produce an authoritative language (Ortega Alcazar, 2012) for talking about a specific societal topic and trough establishing certain linguistic parameters they shape how the topic is understood and ultimately how it impacts the reality. As discourses are composed by a multitude of statements, largely in a textual form in our research, the analysis must begin by asking "who produces a statement, how, where and for whom?" (Keller, 2013, p. 111).

The goal of this research is to track and explore the discursive engagements of the British intelligence community, civil society, scientific, judicial and oversight actors in order to account for the policy and regulatory framework surrounding the phenomenon of bulk surveillance for national security in the UK after 2013. We also aim to examine how and to what extent these discourses overlap, compete and produce meaning that will eventually become objective social knowledge and (re)configure the security-democracy relation. Although with the adoption of Investigatory Powers Act in 2016 and other decisions from the ECtHR, bulk surveillance was officially regulated and embedded within a democratic framework, we consider that at the discursive level this societal issue is still an ongoing phenomenon, contested by a significant part of society and not entirely legitimated. For this reason, we consider that analysing and bringing to light the existent discourses on bulk surveillance is also a way to understand how the relationship between

democracy and security is being reconfigured in the context of these new bulk collection techniques.

Research questions

Our main research question is

RQ: How has the controversial issue of bulk surveillance by intelligence and security services been discursively constituted in the UK post-Snowden?

We also formulate secondary research questions:

SRQ1: What are the different discourses that have been competing in the process of meaning making on bulk collection in the UK after 2013?

SRQ2: What societal stakeholders occupy the position of speakers in this debate, using what strategies?

SRQ3: How have the discourses on bulk surveillance been articulated by the societal stakeholders in relation to the democratic norms and mechanisms?

SRQ4: How have the discourses on bulk surveillance evolved since 2013?

A case-study approach

We adopt a case study approach (Gerring, 2004), specifically a focus on the UK societal debate on the use of technologies of bulk data collection by the state security apparatus. It critically examines policy-relevant texts, reports and speeches uttered in the public space by British intelligence officials, civil society organisations, intelligence oversight bodies, and critical academic interventions since the occurrence of the Snowden revelations. As such, this study uses a qualitative content analysis method. For example, the analysis in the case of GCHQ reveals a series of unprecedented steps towards transparency and a normative rhetoric centred on public engagement can be traced at communications level. The focus on discourses that sustain and create legitimate knowledge prerogatives also confers this study a critical character.

There are several reasons for our case study selection. One of these is that the UK has a long history of technological innovation in the field of signals intelligence and are currently wielding one of the most advanced and extensive SIGINT collection infrastructures in the world. Another important justification for this selection is the ongoing public debate around the use of bulk data collection in the UK. A study from 2019 focusing on bulk interception regimes placed the UK alongside a few other democracies (Finland,

Sweden, Norway, and the Netherlands) which have or are having consistent public debates on this issue (Kind, 2019). According to the same study, the United States (US), for example, still lacks such a debate mainly due to the secrecy constraints advocated by the intelligence community on grounds of national security (Kind, 2019). Lastly, an important reason for choosing to focus on the UK was the availability of a considerable number of public documents, legislation, and official expert reviews offering detailed information about the operational and regulatory aspects of the current bulk collection regime, which allowed for the present analysis to be undertaken.

In the UK we identified four major societal actors involved in the debate: the intelligence community (GCHQ), civil society organisations working in the field of human rights, critical academia, and expert oversight entities (IPCO). Given the expert character of the debate we are examining, these actors were selected based on their discursive presence on the subject matter in the public space via specialist texts. We consider that media and MPs[1] as are not directly shaping this expert debate which is taking place on technical, ethical, epistemological, and human rights grounds. Moreover, politicians usually lack specialised knowledge of intelligence related issues. Both media and politicians rather adopt narratives and frames delivered by the actors we identified, and it is through MPs and media that these narratives in the form of metaphors, frames or discourses come to influence public opinion and policy making. As a result, we decided not to include media and politicians in the list of societal actors involved in shaping the debate on bulk data collection.

The case of GCHQ was chosen for several reasons. Firstly, GCHQ was at the epicentre of the Snowden scandal. Secondly, as one of the most powerful SIGINT agencies in the democratic world, the way GCHQ is addressing bulk collection and AI technology, including associated ethical aspects, may have a leading influence on Western intelligence practices. The notable and rapid changes in the agency's approach towards openness and public communication after 2013 is another reason for our case selection. Last but not least is the availability of a considerable number of public documents, legislation, and official expert reviews on operational and regulatory aspects of the current intelligence collection practices in the UK which would allow such an examination.

[1] However, we included in the study the specialised parliamentary committee for intelligence and security (ISC) given that The Committee is supported in its work by the Office of The Intelligence and Security Committee a small group of technical experts

We analyse documents, officials' texts and other communication mediums i.e. a museum exhibition, in order to understand how and why GCHQ post-Snowden has been communicating to the general public on a scale unprecedented in its century-long existence. We examine these communicative strategies as part of a discourse that constructs the intelligence agency's claims to legitimacy of expertise in the fields of security and technology. In other words, the communication attempting to persuade the public about the agency's commitment to transparency also functions as a way to assert publicly GCHQ's knowledge authority. By extension, it is a way for the agency to construct its own public identity as separate from the more famous MI5 and MI6, which have been much more present in the public imaginary. Although institutional cooperation is always presented as the prevailing principle, competition between different branches of the intelligence community is not uncommon. For example, in early 2021, GCHQ proposed an ethical framework for the future use of AI in national security in a released document called "Pioneering a New National Security - The Ethics of Artificial Intelligence". They did so in the name of transparency, but the initiative also served as a way for the agency to assert itself as the main expert authority on this issue vis-à-vis both the public and the other agencies.

CHAPTER 1 - BULK SURVEILLANCE AND THE BURGEONING FIELD OF CRITICAL INTELLIGENCE STUDIES

1.1 From Critical Security Studies (CSS) to Critical Intelligence Studies

This study operates within a critical theory framework and aims to make a contribution to an emerging, yet promising, corpus of research known as critical intelligence studies. A common claim of scholarly publications that approach intelligence from a critical angle is that Critical Security Studies could provide a formative theoretical framework for the under-developed but growing subfield of critical intelligence studies. (e.g. Newbery & Kaunert, 2023; Ivan et al. 2021; Aradau & McCluskey 2022a).

The conceptual apparatus of CSS can provide useful tools for the emerging critical turn in intelligence scholarship. One of these conceptual elements is the centrality of power-knowledge nexus in understanding intelligence, an aspect which is also emphasised by Ivan, Chiru and Arcos (2021) in their critical take on intelligence:

> "[…] in direct correlation to critical security studies (CSS), it is the emerging critical intelligence studies (CIS) subfield that highlights the way interactions created between intelligence, knowledge and power cannot and should not be overlooked if intelligence is to be correctly framed and understood" (p. 2).

Another conceptual feature of CSS that can be emulated in the study of intelligence refers to the shift in vocabulary and language that need to be adopted in order to challenge the established assumptions about intelligence. Terms such as "surveillance" and "secrecy" should become common references when studying intelligence, providing a way out of the constraining technical and neutral language derived from the classic model of the intelligence cycle. In their study on the emerging field of critical intelligence, critical security scholars Aradau & McCluskey (2022a), encouraged the subverting of the narrow vocabulary associated with mainstream intelligence studies:

> "Critical security studies have shifted the innocuous and even desirable language of 'security', with its assumptions of protection, into that of (in)security. A similar shift is yet to be undertaken in studies of intelligence, where the language of clandestine action, surveillance, suspicion and secrecy would need to find crystallisation in a vocabulary that undoes the assumptions that intelligence equals information collection, transmission and dissemination to anticipate threats and support decision-making" (p. 14).

A third conceptual feature derived from CSS, is the rejection of the state-centric ontology in the study of intelligence. A critical turn in intelligence studies would require a multi-focal perspective on intelligence, seen as a domain of multiple societal actors, including civil society and private companies. Mirroring the seminal interrogation from CSS "whose security?", critical intelligence should be driven by similar questions like "who constitutes intelligence?" and "what constitutes intelligence?". In their article *Critical Intelligence Studies: A new framework for analysis*, Newbery & Kaunert (2023) observed that the rejection of the statist model is a crucial point for developing a valid theoretical framework of critical intelligence:

> "Critical Security Studies' recognition of the broadening and widening of the concept of security, and the ensuing recognition that intelligence work is not only done by state intelligence agencies or for states' security, provides an opportunity to push forward the study of intelligence into a position where a well-developed, and theoretically sound, Critical Intelligence Studies can be meaningfully said to exist" (p. 13).

Following into the steps of critical security studies, critical intelligence is a growing corpus of scholarship that, according to Bean (2018), challenges dominant ontologies and epistemologies associated with the traditional study of intelligence. A survey of the critical literature on intelligence uncover some defining features of this burgeoning field of research and different degrees of critique. The defining features are: the acknowledgment of the power-knowledge nexus as inherent in conceptualization of intelligence and a rejection of the functionalist view of intelligence as a field serving policymaking. In its current form, the field of critical intelligence studies includes a diversity of conceptual initiatives, from intelligence understood as a continuation of war (Der Derian, 1993) to intelligence as a social phenomenon (Ben Jaffel et al., 2020) and from intelligence approached as a whole of society (Ivan et al., 2021) to intelligence as mass surveillance (Aradau & McCluskey, 2022a).

1.1.1 The inseparable tie between power and knowledge in the study of intelligence

As already mentioned, a defining feature of critical intelligence studies is the acknowledgment of the inextricable connection between intelligence, knowledge and power in the conceptualisation of intelligence (Ivan et al. 2021). Within a critical approach, a concern with the pervasiveness of power "drives both the research questions asked and the ultimate, political goals of scholarship" (Bean, 2018, p. 532).

One of the first contributions to critical intelligence studies is attributed to international relations scholar James Der Derian and his 1993 article *Anti-diplomacy, Intelligence Theory and Surveillance Practice* published in *Intelligence and National Security*. Written in the aftermath of the Cold War, the article provides a disruptive interpretation of intelligence, opening new avenues for critique and challenging the canonical model of intelligence studies centred on intelligence cycle. Aiming to provide a hermeneutic definition, Der Derian (1993) defined intelligence as "the continuation of war by the clandestine interference of one power into the affairs of another power. […] Intelligence is to make war without war" (pp. 31-32).

Der Derian (1993) identified surveillance as a form of power and as "one mode of intelligence in particular [which] emerged as the most powerful response to the estrangement and accelerated pace of international relations" (p. 32). In the modern age, intelligence has been "sanitized" into a more "neutral" meaning as "information management", specifically referring to gathering, analysing and disseminating information for decisionmakers and national security purposes (Der Derian, 1993, p. 31). Nevertheless, intelligence cannot be decoupled from war and surveillance.

As Aradau & McCluskey (2022a) observed, Der Derian's seminal definition that inaugurated a new path for the study of intelligence has been mostly ignored by intelligence scholars. Capitalizing on Der Derian's original account of intelligence, Aradau & McCluskey (2022a) argued that critical intelligence studies "cannot be focused on 'intelligence' as an aspect of information management, but must situate these practices in relation to security, surveillance and war" (p. 20). The artificial decoupling of power from knowledge in the study of intelligence, impede the manifestation of a more radical critique within the intelligence scholarship. According to Aradau & McCluskey (2022a), most of the academic initiatives grouped in the burgeoning field of critical intelligence studies (e.g.

Bean et al., 2021), are still operating with a separation of power from knowledge, thus making their critique "therapeutic" rather than "transformative" (p. 11). As a consequence, the various criticisms of the intelligence cycle and surveillance that bypass the Foucauldian paradigm of inseparability between power and knowledge, are weak.

1.1.2 Rejecting the primacy of the functionalist outlook that conceives intelligence theorizing as serving policymaking

A second defining feature of critical intelligence studies is a rejection of the state-centric ontology and of the functionalist view of intelligence theorizing as serving decision/policy making. According to Ben Jaffel et al. (2020), intelligence scholarship, including many of the newer critical initiatives (e.g. Bean, 2018; De Werd, 2018), remain prisoner of this lineage which reduces intelligence to state security and "bypasses questions of who and what constitutes intelligence in the world" (p. 326). Only by disrupting this deeply-rooted constraining framework and start looking at intelligence's existence as a social phenomenon, could intelligence scholarship eventually move towards a more radical and transformative critique, shifting from theories "for" intelligence to theories "of" intelligence (Ben Jaffel et al., 2020).

Although less radical, there are other critical initiatives challenging the state-centric ontology of traditional intelligence studies. In one such scholarly piece, Ivan et al. (2021) conceive intelligence not from a statist position, but from a cognitive perspective applied to propaganda and disinformation. Their stated aims, to "reconsider" the dominant ontology and epistemology of intelligence organizations and to "de-reify" intelligence, places their study into a critical framework (Ivan et al., 2021, p. 3). In particular, Ivan et al. (2021) argued for the replacing of the centralized and hierarchic model of interaction between intelligence and policymakers, with a societal model that includes multiple layers of interaction such as dialogue with the public and geared towards empowering citizens. The proposed model described as "whole of society" (Ivan et al., 2021) is less radical in the sense that it still approaches intelligence through a functional lens, namely as an instrument aimed at countering the threat of disinformation and at improving security.

1.2 Surveillance as an inherent dimension in critical conceptualizations of intelligence

The current study capitalizes on a stream of critical scholarship that understands surveillance as a constitutive element of intelligence (e.g. Der Derian, 1993; Ben Jaffel et al., 2020; Aradau & McCluskey, 2022a). As it was emphasized earlier, surveillance cannot be separated from intelligence. Der Derian's (1993) definition of intelligence as "the continuation of war by the clandestine interference [between states]" (p. 31), was supplemented almost three decades later by Aradau & McCluskey (2022a) who described intelligence as the "clandestine interference in the lives of citizens and non-citizens, or [in other words] mass surveillance" (p. 12).

The understanding of intelligence as clandestine interference taking the form of mass surveillance can be accounted by the concept of "surveillant assemblage" (Haggerty & Ericson, 2000). "Surveillance assemblage" is a concept describing a contemporary form of surveillance that operates with delocalized abstractions and standardized data in order to capture information flows of the human body. Such flows from different databases are latter reassembled into new data to construct an identity that can be examined and used as an operational target (Haggerty & Ericson, 2000). As the proponents of this concept observed, the assemblage is "not so much immediately concerned with the direct physical relocation of the human body, […] but with transforming the body into pure information, such that it can be rendered more mobile and comparable" (Haggerty & Ericson, 2000, p. 613).

The "mass" clandestine interference of intelligence in the lives of individuals can be seen as a result of a paradigmatic shift from Foucault's (1980) disciplinary society to Deleuze's (1992) society of control, a shift generated by the technological advancements. Contemporary digital technologies based on algorithmic reasoning and Big Data, made surveillance decentralized, fragmented and dispersed, thus permitting surveillance of mobile populations and not only of individuals confined to restricted spaces as in the panoptic model. According to Lyon (2014), "surveillance practices have been moving steadily from targeted scrutiny of 'populations' and individuals to mass monitoring in search of […] 'actionable intelligence'" (p. 2).

Following this intellectual lineage, the current study adopts a transdisciplinary discursive approach to intelligence through the prism of a socially controversial topic: bulk surveillance. In this sense, by examining intelligence discourse on bulk surveillance, this thesis is also examining how the intelligence actors are being transformed. Because bulk surveillance is constitutive of what intelligence has become, examining intelligence actors'

discourse on bulk surveillance, opens a gateway to understanding how intelligence actors construe themselves at the level of society, in the post-Snowden age.

1.3 Elements of critical theory framework guiding this study and theoretical contribution

As already stated, from a theoretical standpoint this study falls into the emerging field of critical studies on intelligence. The "critical" stance of the current study resides mainly in its concern for power, a specific feature which, according to Bean (2018), "drives both the research questions asked and the ultimate, political goals of scholarship" (p. 532). This study traces the power-knowledge nexus in the discursive struggle between the main intelligence actor (GCHQ) and the other stakeholders identified, such as civil society and academia. The study, hence, acknowledges the pervasiveness of power in society and examines the power struggle between different societal actors at discursive level. Power and knowledge are intimately connected and this study agrees with Der Derian (1993) and Aradau & McCluskey (2022a) in arguing that the field of intelligence cannot be properly studied by separating the power aspects of surveillance and suspicion from a neutral understanding of intelligence understood as information management. Furthermore, the preference for a non-positivist methodology, namely a discursive approach to intelligence through the prism of surveillance, also places this study within a "critical theory" framework.

The study rejects the traditional state-centric and functionalist understanding of intelligence as a cycle with the only role of benefiting the policy and decisionmakers. Instead, our study approaches intelligence as a social phenomenon, meaning that it locates intelligence within "a social space of relationships that expand beyond intelligence services alone and involve other actors embedded in struggles to speak for, perform, and contest intelligence" (Ben Jaffel et al., 2020, p. 328). In other words, it conceives intelligence as a phenomenon involving a diversity of actors, loci and interests. This is translated into empirical research focusing on societal actors that are not traditionally associated with the field of intelligence/national security, like civil society and academia, actors that are contesting intelligence practices of bulk surveillance. The study shows that such actors are becoming more influential on the way intelligence discourse is transforming. In this sense, the empirical section of the thesis demonstrates how discursive elements like "human rights" and "oversight" are now taking precedence over "national security" in the intelligence discourse on bulk surveillance in the UK.

The deployment of the Snowden scandal as a departure point, positions this study on a course characterised by critique and contestation of intelligence, that disrupts "the imaginary of intelligence […] as security and protection" (Aradau & McCluskey, 2022a, p. 16). This is reflected in the manner the thesis approaches the intelligence field, mainly through the normative lenses of democratic intelligence governance, instead of a more traditional perspective centred around national security and protection. For Aradau and McCluskey (2022a),

> "an agenda that sees scandals and affairs as a key feature of critical security and intelligence studies would therefore take seriously the public denunciation of a practice in the name of intelligence, the nature of the apparent transgression and the way in which other actors publicly react to the denunciation" (p. 17).

Similarly, the current study traces how the practice of bulk surveillance that entered into the UK's public space through the Snowden revelations, has generated public reactions from multiple actors like civil society and oversight institutions, eventually taking the shape of an expert public debate.

The present research aims to contribute to the burgeoning field of critical studies on intelligence. It employs a discursive approach to intelligence theorizing through the lenses of surveillance, with surveillance understood as a defining dimension of intelligence. At a theoretical level, the study traces the transformative impact of the debates surrounding bulk surveillance on the role of intelligence in advanced democracies (see Figure 2).

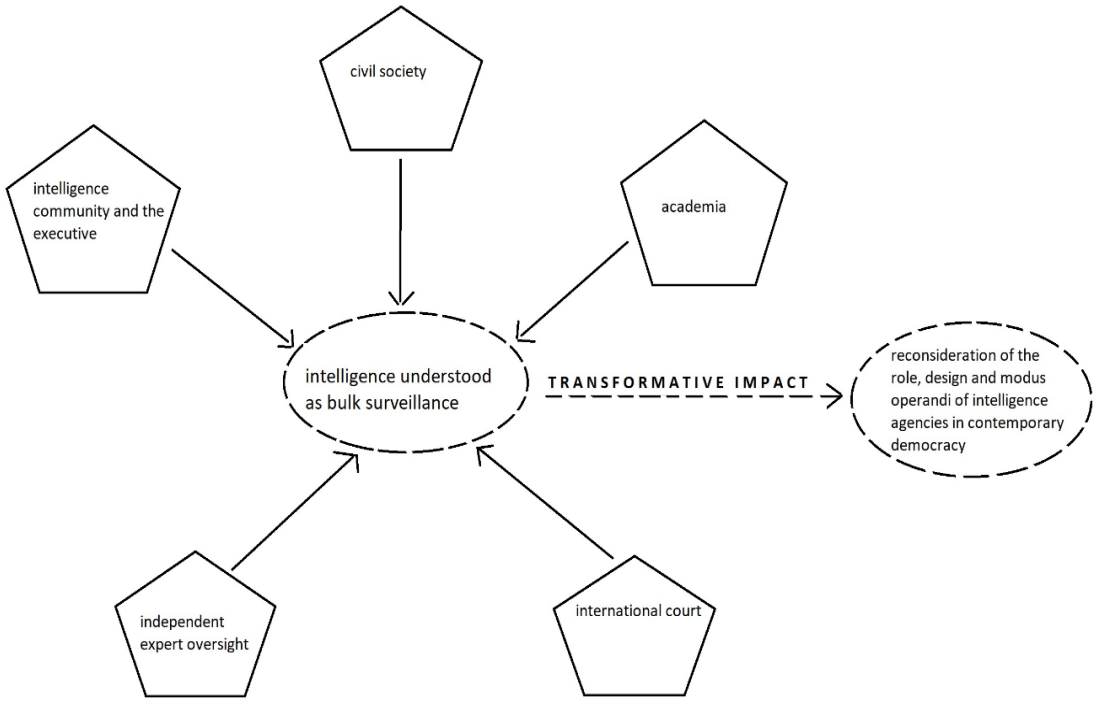

Figure 2: The transformative impact of the debates surrounding bulk surveillance on the role of intelligence in advanced democracies

Bulk surveillance understood as intelligence or constitutive of what intelligence represents today, is at the core of the transformative processes of the intelligence agencies in some advanced democracies like the UK. As the current study will demonstrate in the empirical section, the debates generated by the Snowden revelations around the topic of bulk surveillance had a spill-over effect leading to important transformations at the level of discourse articulated by intelligence agencies and on how intelligence actors discursively construe themselves in the public space. In other words, the debates generated by the bulk surveillance technologies forced intelligence actors, for the first time, into a discursive struggle taking place in the public space.

Before the Snowden scandal and the debates around bulk surveillance, intelligence actors addressing the public sphere through discourses using narratives of democracy and human rights, was something implausible. As Dover et al. (2022) observed,

> "[t]he reaction to the Snowden leaks starkly highlighted that intelligence was always something that was known to the public, but perhaps in a peripheral way, akin to a void or collection of suspicions, but now it had become real or more real" (p. 3).

The manner in which the societal debates on bulk surveillance have been unfolding, signals a new era for intelligence actors in advanced democracies, entailing a

reconsideration of their role, design and modus operandi. In this regard, the formative experience of taking part in a democratic societal debate can become a blueprint for intelligence actors in the upcoming societal debates. There are signs - such as the GCHQ's release of their ethical framework on the future use of AI-, suggesting that the next big debate has already started and revolves around the use of AI for intelligence and security purposes.

1.4 Metaphors as narrative devices

The public debate on surveillance is imbued with metaphors understood here as narrative devices. Metaphors can be seen as "promising analytical objects for reconstructing constellations of practices and narratives" (Smith Ochoa et al., 2021, p. 217). The substantial occurrence of metaphors in the surveillance field can be explained through the complexity of new and emerging technologies of bulk data collection. In this sense, metaphors function as "conceptual frameworks [that] provide a way for the new and complex concepts to be understood and communicated" (Logan, 2017, p. 10).

A study mapping the language employed by journalists to describe surveillance found over 200 metaphors in use (Fleischaker, 2014). Terms used for the data collecting process were, among others, harvest, sweep, and gather; metaphors with literary undertones, such as Orwellian, Big Brother, and dystopian; metaphors evoking historical references, like Stasi and totalitarian; or metaphors with a nautical theme, like dragnet and tentacles. Furthermore, given the gap between the existing regulation and the fast-paced technological developments in the digital field, metaphors of surveillance technologies are also incorporated into legal framework as a way to make sense of new unregulated phenomena. The power of metaphors, thus, resides in the way they shape "the social, political, and legal rules assigned to particular technologies [but also in their potential] to distort, manipulate, or obfuscate reality" (Gill, 2018, p. 464).

The two most important metaphors used in connection to bulk data collection in the UK debate post-Snowden have been 'panopticon' and 'finding the needle in a haystack'. As Aradau (2015) observed,

> "[t]he analogy between the practices of the NSA and GCHQ and 'finding the needle in a haystack' has structured the problematization of mass surveillance in terms of how big the haystack should be, how long it should be kept for, whether collecting the haystack constitutes privacy intrusion or mass surveillance, and how much oversight bigger haystacks require" (p. 21).

While the "haystack" metaphor led to an exclusive focus on regulation and oversight as solutions for governing these intelligence practices, it has also obscured other dimensions, such as the unaccounted production of knowledge by intelligence agencies through the fact that "collecting a haystack of data can reveal the unknown needles" (Aradau, 2015, p. 21). The "haystack" analogy has been adopted and integrated in the intelligence discourse. For example, during a parliamentary inquiry of the intelligence services following the Snowden disclosures, the head of GCHQ at the time made use of this metaphor as follows:

> "If you think of the internet as an enormous hay field, what we are trying to do is to collect hay from those parts of the field that we can get access to and which might be lucrative in terms of containing the needles or the fragments of the needles that we might be interested in, that might help our mission. When we gather that haystack, and remember it is not a haystack from the whole field, it is a haystack from a tiny proportion of that field, we are very, very well aware that within that haystack there is going to be plenty of hay which is innocent communications from innocent people […]. And so, we design our queries against that data, to draw out the needles and we do not intrude upon, if you like, the surrounding hay" (Lobban, 2013, from *Uncorrected transcript of public evidence before the UK's Intelligence and Security Committee*).

The GCHQ director's speech and use of the "haystack" analogy is an example of how one of the main stakeholders we are studying i.e. representatives of the intelligence community, was trying to frame the emerging, at that moment, societal debate on bulk surveillance in the aftermath of the Snowden scandal. Metaphors used to represent bulk collection practices in public and political discourse have the potential of shaping policy measures.

The other popular metaphor, "panopticon", is based on the famous prison model designed by the English utilitarian philosopher Jeremy Bentham, architecturally based on the principle of instilling a perception of permanent surveillance for the prisoners. The model was later reinterpreted by the critical thinker Michel Foucault within his broader power/knowledge theory as representing the power and omniscience of the modern state with its mechanisms of social control. Since then, the panopticon has become the leading scholarly metaphor for analysing surveillance (Haggerty, 2006). The panopticon has therefore been an essential metaphor for surveillance studies and scholars.

1.5 'Bulk collection' versus 'mass surveillance' – two competing narratives

An existing ambiguity related to our research topic in the literature on surveillance is the utilisation of 'bulk collection' and 'mass surveillance'. How different are these two concepts and why is terminology important in this case? The expression 'mass surveillance' is nowhere to be found in official texts such as the new surveillance legislation in the UK. Instead, they refer to bulk interception, bulk equipment interference or bulk acquisition. So, the question that should be asked here is: do these practices differ in any way from the past mass surveillance practices of the East Germany's Stasi, for example? This is basically what we are trying to answer to in this section.

There are two interconnected arguments raised by those favouring a clear ontological separation between 'bulk collection/access' and 'mass surveillance'. The first argument covers institutional and ethical aspects and refers to the extent and reason of surveillance. It juxtaposes a democratic framework against a totalitarian one, corresponding to each of the two concepts. Hence, the difference between *bulk collection* and *mass surveillance* is the difference between a domestic intelligence collection within a liberal democratic state versus collection within a totalitarian state.

The former GCHQ director David Omand argued that what differentiates the two types of collection is the extent of it and the motives for it. Thus, in a democratic framework, the authorities follow the logic of discovery of specific information through bulk access, having no interest in the activities of law-abiding citizens. Conversely, in a totalitarian state, authorities' interest of monitoring the everyday life of their citizens is very high as this can unveil threats for the regime itself (Omand & Phythian, 2018, p. 36). However, Omand's differentiation and use of analogies should be understood as a discursive strategy mobilized as part of the justificatory discourse coming from the intelligence community. The metaphor used when referring to bulk surveillance is *pulling the wanted needle out of the haystack*, which illustrates a logic of finding specific information. By contrast, mass surveillance involves "persistent observation of the population or a significant section of it" (Omand & Phythian, 2018, p. 150). Following this thinking, the institutional architecture at the basis of a liberal democracy would serve as a bulwark against the dangers of an arbitrary practice such as mass surveillance. In other words, the distinction between *bulk collection* and *mass surveillance* could reside in the existence of legal safeguards and proper oversight mechanisms which a society based on the principles of the *rule of law* should have. In this sense,

> "the liberal state has accepted a responsibility for providing a reasonable level of protection of the public through the rule of law, which subjects, for example, intrusive surveillance to strict necessity and proportionality tests that limit the extent that it can be used" (Omand & Phythian, 2018, p. 36).

Bulk collection is understood within this legal framework and being in accordance with the principles of necessity and proportionality while *mass surveillance* is something unregulated and arbitrary, associated to an *Orwellian* type of state. According to the principle of necessity, all intrusion needs to be justified as necessary in relation to clear tasks and missions assigned to SIS and LEAs in accordance with their properly democratic processes, and there should be no other feasible means of achieving the objective (RUSI Report, 2015, p. 13). The principle of proportionality refers to the fact that intrusion must be evaluated as proportionate to the benefits gained and "not just in cost or resource terms but also through a judgement that the degree of intrusion is matched by the seriousness of the harm to be prevented" (RUSI Report, 2015, p. 13). An ethically acceptable bulk collection regime should contain clear procedures and suitable arrangements for a "strict necessity test for the retention of material" (Omand & Phythian, 2018, p. 165). In the end, the data selected for examination and considered relevant to a case will have to be retained. Nevertheless, the retained material should represent only "a very small fraction of what is accessed" (Omand & Phythian, 2018, p. 165). Moreover, the period of retention is another key aspect of bulk collection which has to be subjected to the principle of proportionality. Because retention duration involves the likelihood of human analysts accessing the data collected in bulk, it is important to include duration in the proportionality judgment.

Removal of unwanted material and the application of filtering and selection processes should also be carefully regulated and evaluated. Unwanted material represents that accessed data which is of no intelligence interest. In this sense the efficiency and the discrimination potency of the algorithms used for filtering and discarding this unnecessary volume of data which remains unseen by human analysts, is of crucial importance for the compliance with the liberal democratic standards and privacy rights (Omand & Phythian, 2018).

A *discriminant* is defined in the NAS Report as "detailed instructions for searching a database of collected data used in conjunction with filtering applied as part of collection" [and] "simple enough to be applied in real time as SIGINT data is extracted and filtered" (NAS Report, 2015, p. 36). Likewise, the *selectors* which are applied in order to extract information of intelligence interest should be judiciously considered. However, as the

Report shows, some types of collection are focused on topics rather than people and the discriminants used will inevitably collect information of no intelligence interest. The example offered is about a discriminant which may be less specific:

> "a discriminant that collects all queries to Internet search engines that ask about "sarin" or "poison gas" will collect information about many people of no intelligence interest because only a handful of those making such searches will be of actual interest" (NAS Report, 2015, p. 52).

Thus, if the techniques of selection of relevant material are not discriminating efficiently and if the potential gains of the examination are not proportionate with the degree of intrusion, "then the result would be open to the accusation of having conducted mass surveillance, which is a characteristic practice of totalitarian regimes" (Omand & Phythian, 2018, p. 234).

The *modus operandi* of a liberal democratic regime based on the *rule of law* will, by definition, reject 'mass surveillance' as an unlawful practice. This framework of thought is proposed by David Anderson Q.C., the expert who reviewed the operational case for bulk powers in the UK (2016) after he was given full access to the classified work of the GCHQ and the Security Service. In his review, Anderson (2016) wrote that:

> "[…] it should be plain that the collection and retention of data in bulk does not equate to so-called 'mass surveillance'. Any legal system worth the name will incorporate limitations and safeguards designed precisely to ensure that access to stores of sensitive data (whether held by the Government or by communications service providers [CSPs]) is not given on an indiscriminate or unjustified basis" (p. 4).

It should be mentioned that Anderson was criticized by a part of civil society in what regards the manner in which he carried out his review. According to Liberty, "the review was conducted to a rushed time-frame and thus procedurally compromised" and that it "failed to establish a proven case for the necessity of the powers" (Liberty's briefing on "Report of the Bulk Powers Review", 2016).

1.5.1. Bulk surveillance and democracy

The framework of thought which acknowledges a range of appropriate standards that democracies should meet in actual oversight practices and legislation regarding bulk surveillance, was also advanced by Wetzling and Vieth (2018) in their empirically rich

international compendium of legal safeguards and oversight innovations, *Upping the Ante on Bulk Surveillance*. The two researchers referenced the "many processes and constitutional obligations" associated with the implementation of bulk powers in practice which they identified by studying different national models. (Wetzling & Vieth, 2018, p. 17). Moreover, their study introduces a "bulk surveillance governance analysis scheme" (Wetzling & Vieth, 2018, p. 18), designed as a multi-stage model based on the classic intelligence cycle (see Figure 3). The proposed model clearly displays the different stages of the democratic governance of bulk powers.

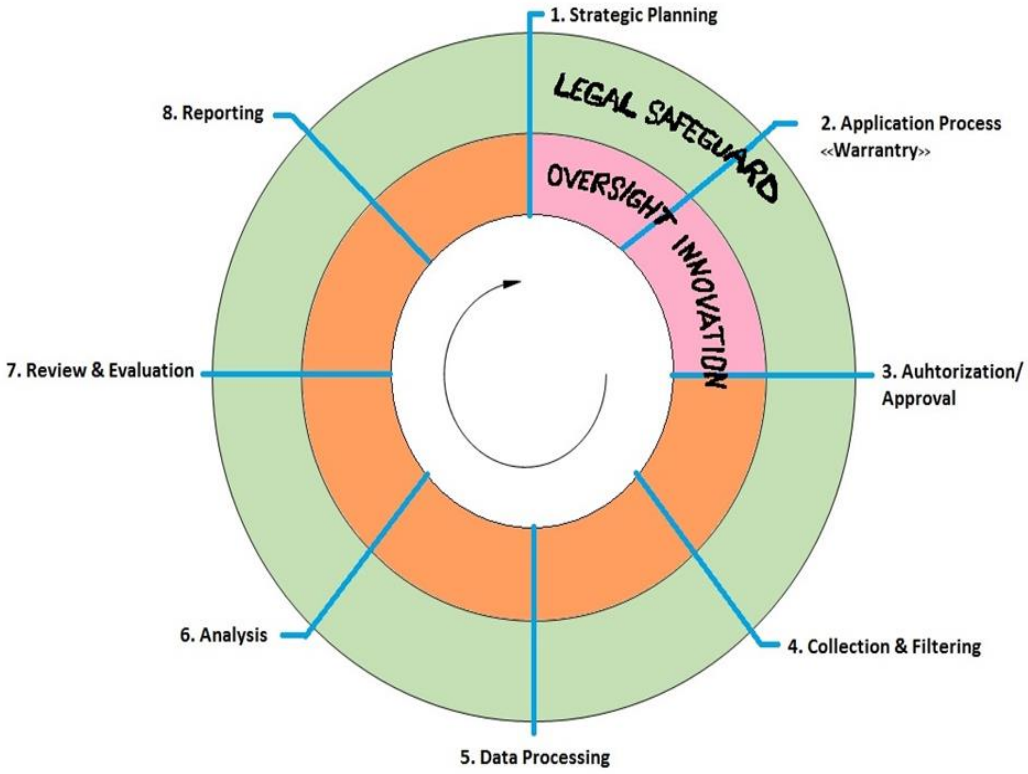

Figure 3: Bulk powers governance analysis scheme (as designed by Wetzling and Vieth, 2018)

One of the key assertions of the compendium is that "comprehensive intelligence legislation is a necessary but not sufficient condition for the effective democratic control of bulk surveillance [*and that*] what matters here are the actual dynamics of judicial oversight as well as its resources, legal mandate, and technological tools" (Wetzling & Vieth, 2018, p. 18). Put it differently, regulating the use of bulk powers is an essential first step in this process of democratic control. After 2015 new intelligence laws incorporating this 'bulk' dimension have been adopted in several European countries like France,

Germany, the UK and the Netherlands while others such as Finland are in the process of reforming their legislation in order to include this category of SIGINT (FRA report, 2017, p. 40). Nonetheless, legal safeguards must be complemented by oversight practices as they are each particularly important and 'mutually constitutive' (Wetzling & Vieth 2018, p. 18).

As this study will show in a later chapter, oversight practices together with oversight innovation represent the dynamic core of democratic governance of bulk powers. Specifically, in the context of rapidly evolving bulk collection techniques deployed by SIS, oversight practices can come up with solutions for a more effective containment of these surveillance regimes through the innovative use of technology. According to Wetzling and Vieth (2018),

> "a court will not design new rules or prescribe specific accountability mechanisms. This is the difficult and necessary work of democratic governance, and it needs to be done by the principled members of the different oversight bodies that understand the critical importance of their work" (p. 10).

1.5.2. Bulk collection as distinct from mass surveillance

Another line of argumentation advanced by those who favor a clear distinction between *bulk collection* and *mass surveillance* is more procedural and derives from their understanding of what constitutes surveillance. To be more precise, the supporters of this approach argue that surveillance happens only when a human analyst is involved in the examination process of the collected data after the algorithmic filtering took place. Accordingly, the initial stages of data gathering and algorithmic analysis do not qualify as surveillance. An advocate of this perspective is the former director of GCHQ, David Omand, who argues that there are two different types of logics at work behind 'bulk access' and 'mass surveillance'. Omand states that the degree of actual harming a person's fundamental rights such as privacy is contingent on "whether a computer only scanned and discarded the relevant material or whether a human analyst saw and logged it for future action" (Omand & Phythian, 2018, p. 150). Thus, while a "bulk access" intelligence operation is geared towards finding specific needed information, the logic underpinning mass surveillance is systematic observation of the population in its routine activity as a way to prevent any potential threats for the political establishment itself (Omand & Phythian, 2018, p. 150). This view was first articulated by David Omand in 2014 during a forum dedicated to the Snowden revelations. According to him, only GCHQ's machines have

"bulk access" while "mass surveillance implies observers, human beings who are monitoring the population" (Omand quoted in Jeffreys-Jones, 2017, p. 248). His approach was adopted by the Intelligence and Security Committee, the parliamentary body in the UK dealing with intelligence oversight, which stated that "surveillance" is exclusively related to a human involvement in the collection process (Jeffreys-Jones, 2017, p. 248).

For Bernal (2016) the difference lies in how we interpret the occurrence of surveillance, specifically at what stage of the collection process surveillance happens. Data surveillance broadly involves three stages (see Figure 4): "the gathering or collecting of data, the automated analysis of data (including algorithmic filtering), and then the human examination of the results of that analysis of filtering" (Bernal, 2016, p. 249). Unlike human rights activists who would categorically claim that the surveillance occurs at the very first stage -when data are collected-, actors belonging or associated to the intelligence community or the governmental area would endorse the idea that we can only talk about surveillance happening at the third stage - when human analysts are involved. For example, in her evidence to the Parliament on the *Draft Investigatory Powers Bill*, the Home Secretary at the time Theresa May, firmly asserted that the UK has nothing to do with "mass surveillance" (Bernal, 2016).

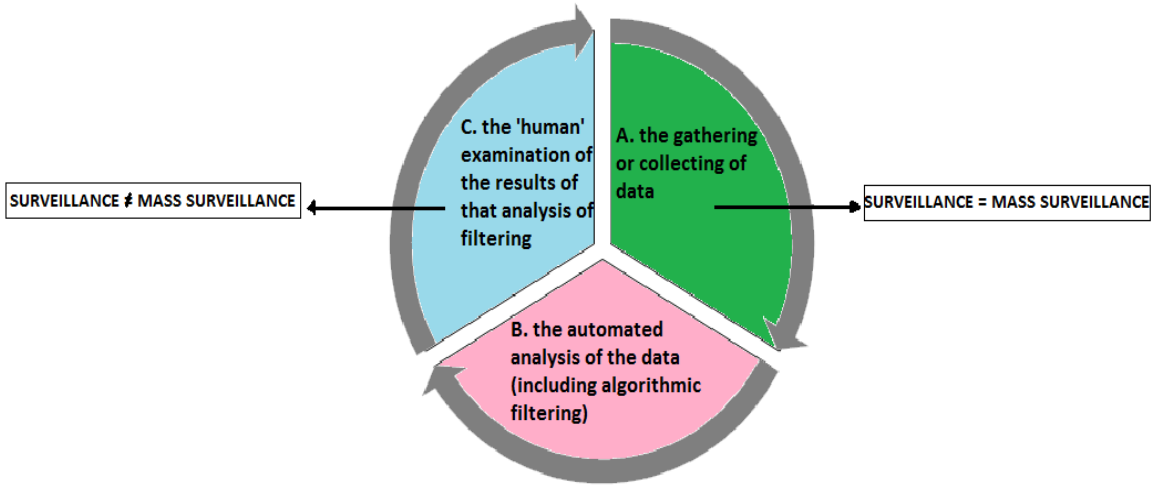

Figure 4: When does surveillance occur in the collection process?

If the surveillance occurs in the *phase A*, there is a clear case of mass surveillance and this would definitely include the *bulk powers* as established by the IPA in the UK for example. On the other hand, if we interpret the surveillance occurring in the *phase C* only,

when a human operator is involved in the process, then we are not dealing with mass surveillance. As Bernal (2016) pointed out in trying to explain the reasoning behind the latter interpretation, "the amount of information looked at by humans may well not be *massive* or *indiscriminate* regardless of how much data are gathered" (p. 249). A supporter of this view, former intelligence practitioner, David Omand, talked about the opportunity of introducing an "ethical test" which should be applied to the design of the intelligence operation, "just as weapons design must conform with international humanitarian law" (Omand & Phythian, 2018, p. 102). The design refers mainly to the *phase B* of the above scheme and should facilitate as far as possible a correct filtering and selection of the relevant information which eventually is seen by human analysts. Following this framework of thought, we can assert that *phase B* is critical in this cycle given that a violation of privacy could happen if the system design itself is flawed and fails to comply with privacy rights standards of discrimination and of proportionality (Omand & Phythian, 2018, p. 102).

1.5.3. Bulk collection as mass surveillance

For a proper understanding of the arguments in favour of a clear distinction between the two concepts, we also need to consider the opposing stance coming from those who argue that *bulk collection* does indeed constitute *mass surveillance*. In this sense, Bruce Schneier, an internationally renowned security technologist and the author of *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (2015), dismisses the thesis that surveillance occurs only when a human operator examines the already selected data as a "nonsense argument" (Schneier quoted in Quinn, 2015). According to him, surveillance happens once people's actions are recorded, namely in the first phase of collection. To support his assertion, Schneier (2015) offered a helpful analogy in the form of made-up statements which authorities would say to people concerned about their privacy:

> "We're going to install a camera in your bedroom and record everything, but it's not surveillance because we won't look at the footage unless we want to [or] yes, your cell phone will keep a constant record of your location, but it's not surveillance, because we won't access the information unless we think you're doing something wrong.[…] These statements make no sense, because we know that once the data is collected and saved, it could be examined; therefore, we have to act as though it will be examined" (p. 1).

In other words, it is very likely that this condition somewhat evocative of Bentham's panopticon, would trigger a chilling effect on private behaviour. Privacy breach happens when the camera is installed in the first place enabling the possibility of someone watching the footage. In other words, there is a latent risk of privacy invasion once the data are gathered in the initial phase.

A similar argument came from the NGOs working in the field of human rights such as Privacy International (2016) whose representatives consider that "bulk powers, by definition, can never be proportionate, and would create an apparatus for perpetual mass surveillance" (p. 10). This view warns about the perilous path of overrunning the principle of proportionality which ultimately leads to the dismantling of the human rights regime. Precisely, by being fundamentally incompatible with the proportionality principle, the so-called bulk powers are but a form of institutionalized mass surveillance and accordingly a threat to the liberal democratic order based on the rule of law.

Another explanation coming from those who see no difference between the two concepts is related to the importance of terminology as a mode of legitimization. In a collectively authored paper published in *International Political Sociology*, renowned sociologists such as Zygmunt Bauman and David Lyon among others (Bauman et al. 2014), consider that the term *mass surveillance* is avoided by intelligence agencies like GCHQ especially because it is reminiscent of the Stasi in East Germany and such a resemblance would prove at least controversial within a liberal democratic society. According to Bauman et al. (2014), "politically, language comes to be the terrain upon which, and through which, modes of legitimization and delegitimization take place" (p. 140).

Dependent on the position of the actor within the societal-institutional framework and/or on the actor's personal beliefs, there exists a variety of expressions used to describe this type of collection: 'strategic surveillance', 'general surveillance of communications', 'indiscriminate bulk data collection', 'bulk powers', 'bulk access', 'bulk collection', 'blanket surveillance', 'dragnet surveillance' and finally 'mass surveillance'. Amongst all these expressions, *mass surveillance* is the one with the strongest resonance, invoking tropes of a not-so-far totalitarian past when everyone in countries like East Germany was under constant observation.

Alternatively, *bulk collection* alludes more to operations that seek the discovery of the *needle in the haystack* which can be the terrorist or the cell of terrorists planning an imminent attack at an unknown time and place. In other words, in the case of *bulk collection* surveillance is considered a sieving operation, "one where the 'mass' runs through the sieve

unobserved and unobstructed, while the one singular aberrant communication is caught […]" (Bauman et al., 2014, p. 140). This way of thinking is sanctioned by remarks such as the one delivered by the former British Foreign Secretary, William Hague: "If you are a law-abiding citizen of this country going about your business and your personal life you have nothing to fear about the British state or the intelligence services listening to your phone calls or anything like that" (*The Telegraph*, 9 June 2013). In their close examination of the expression "mass surveillance", Bauman et al. (2014) argued that "mass" can be understood to mean more than biopolitical landscape of population, namely "the 'multitude' of singular and networked communications subject to surveillance" (p. 140). Their verdict is that "the space of intimacy is, we now know, absolutely penetrated by these agencies, so that a profile is constructed from the digital trace left by the communicating, interactive subject" (Bauman et al., 2014, p. 140).

CHAPTER 2 - TECHNOLOGIES OF BULK SURVEILLANCE

2.1 Introduction

This chapter investigates the proliferation of bulk collection regimes in the post-Snowden age by focusing on the conceptual, operational and regulatory aspects of these surveillance techniques and their impact on citizens' fundamental rights. The starting point for our study is the observable fact that in the post-Snowden landscape, most liberal democracies have expanded rather than reduced state surveillance powers via recent intelligence reforms (Wetzling & Vieth, 2018). Thus, intelligence and surveillance legislation of prominent democracies such as France, the Netherlands and the UK was adjusted in order to incorporate a bulk collection component.

The first part of the chapter discusses bulk method of intelligence collection through a brief historical overview followed by a thorough conceptual examination covering definitions, terminological ambiguities and ethical aspects of a central concept for my current research. It does so by primarily acknowledging the under-theorized status of the concept across the relevant disciplines and the growing gap between practice and conceptualization. Therefore, one of the stated goals of this chapter is also to fill a gap in the research literature on surveillance by achieving some essential clarifications about what constitutes *bulk collection* and how it differs from *mass surveillance*.

Firstly, we will attempt to outline a functional definition of bulk collection by analysing the distinction between *bulk* and *targeted* collection. In order to have a clearer idea of what *bulk* represents, one needs to understand what *targeted* collection is. Next, we tackle the problem of terminological blurriness by focusing on the distinction between *bulk collection* and *mass surveillance*. By doing this, the chapter also addresses the normative premises underpinning these two concepts representing two competing narratives. It is argued that while *bulk collection* corresponds to a liberal democratic order based on the

rule of law, *mass surveillance* is a practice which could rather be found in a non-democratic, illiberal regime. An ongoing topic of confusion and controversy for researchers working in the field of surveillance has been the fact that various societal actors – media, NGOs or governmental actors- use different terminologies and hence different narratives when they refer to the collection and retention of data in bulk. In this sense, examining what is the difference between bulk collection and mass surveillance is crucially important. Given the relative lack of academic literature on this topic, the first section mainly draws on primary sources such as legal texts and governmental reports. Among these, the UK Government's *Operational Case for Bulk Powers* (2016) [Operational case] and the US National Academy of Sciences' *Bulk collection of signals intelligence: technical options* (2015) [NAS Report] are essential texts on which this chapter relies in order to scrutinize the working methods of bulk collection.

The second part of the chapter provides an overview of bulk collection technologies and focuses on their operational and technical aspects. Also, we look at how these bulk collection regimes are implemented in different countries including India, Australia, France, the Netherlands and especially in the UK which is the main focus of my research. In this regard, the recently adopted Investigatory Powers Act 2016 provides a suitable basis for analyzing the issues under discussion including oversight mechanisms and safeguards applicable to bulk powers.

Finally, the analysis of the regulatory aspects is complemented by a section which looks at the European case law on bulk collection. A concluding observation of the chapter is that, increasing the public acceptance of these bulk collection practices should be the next step for the democratic governance of intelligence in the post-Snowden age.

2.2 A brief historical account of bulk method of intelligence collection

In the context of the new technological advancements, governmental surveillance has become ubiquitous, rendering the state security apparatus more powerful than ever before in relation to its citizens. From the very inception of organized communication, the state had an interest in spying its subjects as a form of social control. One of the most quoted examples in this sense is the Post Office in England which has been used since the seventeenth century as a tool for spying on correspondence (Corera 2016). Organized as a single centralized body with a monopoly over mail, the Post Office as envisaged by Oliver Cromwell and his Parliament was going to provide the state with access to communications.

According to the preamble of the Act of 1657, this newly created Post Office "will be the best means to discover and prevent many dangerous and wicked designs against the Commonwealth" (*Tait's Edinburgh Magazine*, 1838, p. 39). As technologies changed, the interception methods deployed by the state to spy on citizens have improved considerably. The 20th century saw the advent of enormous technological changes such as computers and satellites and different surveillance regimes.

2.2.1 Intercepting telegrams

In the US the beginning of the Cold War era witnessed the launch of operation SHAMROCK, a cryptonym referring to a secret domestic surveillance program through which the NSA was monitoring all telegrams sent abroad or received by American citizens. This was done by requesting the big telegraph companies such as RCA, Global, ITT World Communications and Western Union International to handle to the NSA their international cables. These companies agreed to supply the agency with copies of the international telegraphic traffic, a practice rooted in the wartime efforts and cooperation between the state and private sector in order to look for intelligence. In the format of magnetic tape or paper tape copies, these messages were sent to the NSA where an intelligence analyst would examine them (Johnson, 2017). *The Washington Post* estimated that under SHAMROCK, NSA analysts logged and screened millions of telegrams belonging to American citizens, with a volume of 150.000 telegrams monthly in the last few years of the program (Dewey, 2013). This massive domestic eavesdropping program was revealed in 1975 by a Senate investigation. American citizens learned that the NSA was collecting data about them on a massive scale and without any judicial oversight or authorization.

Most historical accounts place the halt of SHAMROCK program in 1975, as a result of the investigations into intelligence activities carried by the U.S. Senate through a select committee also known as Church Committee. However, some authors like Corera (2016) believe that, in reality, "it simply evolved with more formal, but still secret, arrangements with companies" (p. 99). SHAMROCK is important for the historical scrutiny of bulk collection also because it is a good example of cooperation between the state and private companies and hence it can be seen as a template for other surveillance programs which followed. Started as a common war effort and mutual support, this special relation between the intelligence agencies and the companies that provided cable traffic and

the communication infrastructure, has been a constant feature of state surveillance in the U.S. in the 20th century.

2.2.2 ECHELON or the true beginnings of the bulk-data method of intelligence collection

The modern beginnings of the bulk-data method of intelligence collection though are associated with the emergence of satellite technologies and mainly with the project ECHELON which was implemented starting in the late 1960s (Gill, 2019). ECHELON was a joint transnational program adopted by the SIGINT agencies of the U.S., the UK, Canada, Australia and New Zealand. It was operated mainly by the NSA and the GCHQ and designed to collect microwave satellite communications. In the context of the global Cold War, ECHELON was intended to gather signals intelligence of potential value for national security. It comprised a network of listening stations all over the world with one of its major listening facilities at Menwith Hill in Yorkshire, England. Procedurally, ECHELON relied on the signals traffic analysis techniques and on the innovative work originally developed at Bletchley Park during the Second World War (Jeffreys-Jones, 2017, p. 167). The SIGINT agencies operating this program were making use of the built-in trapdoors to be found in every communications satellite deployed in space. Alternatively, a large ground-based relay station would function as an efficient method for intercepting the satellite signal in a certain area (Andregg, 2007, p. 59). The signal was split by exploiting these trapdoors, and a copy would be sent to a vast network of supercomputers for screening and keyword searches of the communications traffic such as faxes, or to a human analyst for a review.

Referring to ECHELON, the investigation journalist Duncan Campbell was revealing in an article published in 1988 in the *New Statesman* that the NSA and GCHQ collected "billions" of messages. The scale of collection was unparalleled in history with the two SIGINT agencies combined capability achieving "near total interception of international commercial and satellite communications in order to locate the telephone or other messages of target individuals" (Campbell quoted in Jeffreys-Jones, 2017, p. 168). The article was also revealing that "computers automatically analyze every telex message or data signal, and can also identify calls to, say, a target telephone number in London, no matter from which country they originate" (Campbell quoted in Cohen, 2014, p. 11). Nevertheless, the value of ECHELON which was a program built primarily on the

technology of satellite communication was already fading away in the 1980s due to a very important change: the growing importance of fibre optic cable for communications.

2.2.3 From satellites to fibre optic cables

An important technological change with significant implications on bulk collection occurred in the late 1970s when fibre optic cables started to replace copper wiring in telephony networks (Cohen, 2014, p. 12). Two main reasons for fibre optic primacy were its comparatively reduced costs and its superior capacity in carrying more data at the speed of light. The transition from analog telephony which were sending electrical signals, to digital telephony sending light signals meant a total reliance on fibre optic cables. Consequently, computer networks also had to make the transition from copper phone lines to fibre optic cables achieving in this way transmission over longer distances at a much faster rate (Cohen, 2014, p. 12).

At the end of the Cold War, fibre optic undersea cables were already the preferred solution for intercontinental communications, outranking satellite technology. However, this change made the SIGINT agencies' work more challenging given that interception of fibre optic cables was more difficult due to higher encryption standards than radio and microwaves (Cohen, 2014). Therefore, it could be stated that the end of the Cold War was overlapping with a full digital revolution which was taking place in the world of communications, generating during the 1990s an increase in the number of internet users from 4 million to over 360 million (Corera, 2016, p. 308).

With the advent of the Internet, the SIGINT agencies had to adapt to the new technological environment, given that the collection model and dynamics changed substantially. The nature of global communications was becoming more fragmentary than ever and moving at a perplexing pace. Agencies like the NSA were being confronted by the problem of information overload and hence a lack of resources to match this massive increase in the volume of traffic data to be intercepted. This made the House Intelligence Committee to conclude, in 1999, that the agency was "in serious trouble" (Dewey, 2013). All internet-based communication such as emails, text messages, phone calls, were now broken down into small fragments known as packets. Interception became in this context the action of capturing a signal consisting of a stream of packets, from the cable (Privacy International, 2017). Therefore, bulk surveillance or what later was coined as bulk

interception, had to be conducted by resorting again to private companies providing communication services.

The new generation of undersea fibre optic cables proved to be difficult to tap underwater, hence SIGINT agencies started focusing on the landing points of this cables, namely on the routing switches belonging to the telecommunication providers. These spots became "the junctures for connecting up transnational, mass spying equipment" (Cohen, 2014, p. 12). The British coastal region of Cornwall became an important hub of terminus points for submarine transatlantic optical cables and hence a prolific supply for intelligence collection by the GCHQ. Britain's technical capability to intercept these fibre optic cables which sustain the world's communications has made GCHQ an "intelligence superpower" (*The Guardian,* 21 Jun 2013). The history of state large-scale surveillance is, however, not exclusively related to technology and the best example in this sense is East Germany with its notorious security service STASI. It was a very different model of mass state surveillance because it was primarily based on human informers.

2.3 Bulk collection: conceptual aspects

2.3.1 Between *bulk* and *targeted* – searching for an operational definition of bulk collection

Given that there is no statutory definition of "bulk" and "bulk power" we decided to establish a working definition in order to delineate the scope of this research. As terrorism scholar Alex Schmid (2004) remarked, "if successful, a definition differentiates one concept clearly from others" (p. 401). In our case, the defining otherness is *targeted* collection and consequently a definition of *bulk* collection would require a clear functional demarcation. To what extent can we operate a clear distinction between these two concepts? Often, ambiguities arise from the lack of a clear distinction between *bulk* and *targeted* collection. This condition allows different societal actors (state institutions, civil society, international human rights bodies) to apply the two labels interchangeably in order to fit their agendas. This confusion is also acknowledged by a European Parliament research study, *Mass Surveillance of Personal Data by EU Member States and Its Compatibility with EU Law* (2013), which states that "the distinction between *targeted* surveillance for criminal investigation purposes, which can be legitimate if framed according to the rule of

law, and *large-scale* surveillance with unclear objectives is increasingly blurred" (Bigo et al., 2013, p. 5).

The US National Academy of Sciences in its influential report, *Bulk collection of signals intelligence: technical options* (2015) [NAS Report] decided that "there is no precise definition of bulk collection, but rather a continuum, with no bright line separating bulk from targeted" (p. 2). The ambiguity regarding the concept of "bulk" is also present in a 2016 document accompanying the *Investigatory Powers Bill* in the UK named *Operational Case for Bulk Powers*. Bulk powers are described as "a range of techniques" employed by the Security and Intelligence Agencies under existing legislation in order to "acquire information in large volumes" (bulk data) which is subsequently used to "generate intelligence about threats that cannot be acquired by more targeted means" (Operational case, 2016, p. 6). The same document provides the following circular explanation: "it is inevitable that much of the data acquired using any of the bulk capabilities will not be of intelligence interest, because it is impossible to determine at the time of acquisition whether a particular piece of information will have intelligence value" (Operational case, 2016, p. 23).

The *Operational case* (2016) distinguished between four bulk powers: Bulk Interception of Communications, Bulk Equipment Interference, Bulk Acquisition (Communications Data) and Bulk Personal Datasets. The UK Government appointed Reviewer of Terrorism Legislation, David Anderson Q.C. in his review about the operational case for bulk investigatory powers (Anderson, 2016), specified how civil society actors view these powers.

For civil society actors such as *Liberty* and *Privacy International*, the essential feature of a bulk power is the access it offers to public authorities such as intelligence agencies to large quantities of data, of which a significant percentage is not linked to current targets (Anderson, 2016, p. 3). This way of conceiving bulk powers is also the one adopted by the committee appointed by the National Research Council in the US, which was charged with finding alternatives that would allow SIS to conduct more easily targeted information acquisition rather than bulk collection. According to committee's vision, "if a significant portion of the data collected is not associated with current targets, it is bulk collection; otherwise, it is targeted" (NAS Report 2015, p. 2). Also, in the UK's *Investigatory Powers Bill*, although "bulk" is not defined as such, we can detect a similar logic at work in the description of Bulk Personal Datasets as "a set of information that

includes personal information relating to a number of individuals where the nature of the set is such that it is likely that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service" (IP Bill 2016, Clause 182).

Another element which must be taken into account when trying to achieve a working definition of bulk collection is the issue of a government's exclusive involvement. Precisely, the *Investigatory Powers Bill* displays a narrower understanding of bulk powers as those powers of collecting data in bulk by the government itself. On this basis, powers to ask communications service providers (CSPs) to gather and retain their customers' data in bulk, are not considered bulk powers, even if SIS and LEAs have the authority to acquire that data (Anderson, 2016, p. 3). The same framework of thought can be found in the NAS Report (2015) which makes a distinction between bulk collection of SIGINT by the US government and the government's utilization of "bulk data held by other parties", a distinction which seems to suggest that the latter is not a form of bulk collection in itself (NAS Report, 2015, p. 57). Nevertheless, according to Anderson's report (2016),

> "the exercise of a bulk power implies the collection and retention of large quantities of data which can subsequently be accessed by the authorities. On this broad definition, the characterization of a power as a bulk power does not depend on whether data is collected and stored by the Government or by a private company […]" (p. 3).

Building on the elements presented above and also on the technical explanations offered by the NAS report (2015), we argue that a working definition of *bulk collection* could have the following layout: *collection conducted by institutions in the sphere of national security, in which a substantial share of the retained data belongs to identifiers that are not targets at the time of collection.* A functional examination of this definition tells us that size alone is not the leading factor of what we call 'bulk collection'. This means that there are no exact numerical criteria regulating what is or is not 'bulk'. Rather, the key aspect of the definition is the act of harvesting non-target data as part of the collection process, this being the benchmark which distinguishes between 'bulk' and 'targeted' collection. By extrapolation, a clear case of targeted collection is hence when collection is about a person of interest. However, there is a whole spectrum of cases in between. That is why, we consider that a working definition for 'targeted collection' should have a more inclusive outline, like the version proposed by the NAS Report (2015): "collection that stores only the SIGINT data that remains after a filter discriminant removes most non-target data" (p. 37).

Having a clearly regulated distinction between targeted and bulk collection is a pre-requisite of a proper democratic governance of bulk powers and henceforth in accordance with the principles of proportionality and necessity. This standpoint is also expressed, albeit in a slightly different manner, in the Venice Commission's definition of *strategic surveillance*, another term designating bulk collection. The Commission emphasizes the distinctiveness of this type of surveillance when compared to law enforcement surveillance or more traditional internal security operations which are always targeted. In this sense, the logic behind bulk collection is finding a danger rather than investigating a known danger. According to the Venice Commission's (2015) definition:

> "Strategic surveillance thus differs in a number of ways from surveillance in law enforcement or more traditional internal security operations. It does not necessarily start with a suspicion against a particular person or persons. It can instead be proactive: finding a danger rather than investigating a known danger. Herein lay both the value it can have for security operations, and the risk it can pose for individual rights. Prosecution is not the main purpose of gathering intelligence. The intelligence is, however, stored and used in a number of ways which can affect human rights" (*p.* 12).

A distinct but not necessarily opposing view is offered in the *Operational Case for Bulk Powers* report (2016) which argues that in reality it is rarely a matter of opting between targeted or bulk powers and that these capabilities should rather be used together. Thus, in order to be more efficient in their pursuit of identifying, investigating and disrupting threats to national security, SIS must use these powers in conjunction (Operational case, 2016, p. 21).

It is true that differentiating between targeted and bulk collection can be challenging, given that a target can be defined after collecting and filtering certain data. This subsequently raises the problem of when an interference with fundamental rights can be established (FRA report, 2017, p. 32). A telling example in this sense is the *Digital Rights Ireland* decision of the Court of Justice of the European Union (CJEU) (C-293/12 and C-594/12) which annulled Directive 2006/24/EC on data retention by private companies for the purposes of their later use by law enforcement agencies. The data involved were gathered and retained on a massive scale, yet LEAs were only allowed to use them for specific, targeted purposes. Under these circumstances one can rightly argue that in this case we could speak of targeted surveillance given the targeted use on the basis of specific warrants of the massively collected metadata (Hijmans and Hijmans, 2016, p.

105). However, in the justification offered by the CJEU it appears that the obligations under Directive 2006/24 were considered a form of "mass surveillance", since the Court evaluated that large groups of the population could feel under constant surveillance.

2.4 Bulk Collection Technologies

2.4.1 Bulk Interception: how it works

This bulk collection method is conducted by intercepting large volumes of data from fiber optic cables and wireless communications. However, in the context of technological developments, bulk interception of cable-bound traffic or in other words tapping the fiber optic cables that make up the backbone of the world's communication network has surpassed wireless interception. Historically, international communications were intercepted by intelligence agencies using satellites and microwave towers such as the NSA's station at Menwith Hill in the UK (Guardian, 21 Jun 2013). Currently, satellite interception accounts for only a small fraction of the network traffic. In the UK this power is utilized for the interception of communications between persons in the UK and persons overseas. Interception is "the process of collecting communications in the course of transit, such that the content becomes available to someone other than the sender or recipient" (Anderson, 2016, p. 23).

Interception and extraction

We first need to understand the data capture phase, where it occurs and how the physical interception facility functions. Bulk interception usually encompasses the gathering of communications as they transit particular communication links. In other words, SIS conduct bulk interception by tapping high capacity submarine fiber optic cables landing in the UK or other locations to intercept their traffic. Interception of the relevant signals in bulk can also be made by diverting data at an internet exchange point. Two of the biggest exchange points in Europe are the Amsterdam internet exchange AMS-IX and the Frankfurt internet exchange DE-CIX. The geographic location plays an important role, making the UK and the US natural landing hubs for most of these fiber cables.

Britain's technical capability to intercept the fiber optic cables which sustain the world's communications has made GCHQ an "intelligence superpower" (*The Guardian*, 21 Jun 2013). For example, TAT-14 (see Figure 5) is a transatlantic cable system with a transmission capacity of 3.15 terabits per second and with landing points in the US, UK,

France, Germany, Denmark and the Netherlands (Privacy International, 2017). Another transatlantic cable is FLAG Atlantic 1 which connects the east coast of North America to the United Kingdom and France -6.000 kilometers- with its terminus in Cornwall, UK. This cable consists of 6 fiber pairs and has a transmission capacity of 2.4 terabit/s per cable (electrospaces.net, 2014).

All internet-based communication such as emails, text messages, phone calls, social media posts are broken down into small fragments known as packets. Interception must be understood in this context as the action of capturing a signal consisting of a stream of packets, from the cable (Privacy International, 2017). Because of the fragmentary nature of global communications, encompassing the partition of communications into packets, a targeted warrant would not necessarily capture all the information needed by SIS (Anderson, 2016, p. 85).

Filtering

The initial stage of interception is followed by the filtering phase which is applied to the traffic on the communication link with the aim of selecting data of potential intelligence value and removing the unnecessary material. An initial filter is applied, a technique called Massive Volume Reduction (MVR) which is used to discard high volume, low-value traffic, thus reducing the volume of data to be processed by 30%. For example, in the Netherlands where a new collection law was passed in 2017, there is an initial filter that removes non-relevant data streams accounting for up to 98% of the data volume.

Next, strong or soft ‘selectors’ are applied. Examining how selectors are devised and applied is very important although this operation is not open to public scrutiny and no information is offered regarding what kind of selectors intelligence analysts use (Granick, 2017, p. 32). Selectors can be particular words, specific countries, telephone numbers, IP addresses and emails. With the help of these ‘selectors’ frequently used in combination, communications of potential intelligence value are obtained and become available to analysts for examination (Anderson, 2016, p. 24). How selectors are chosen and devised is important not just in terms of potential risks of over-collection but also because there are different laws and regimes for selector-based and selectorless collection. (Granick, 2017, p. 33). A query may have several selectors used in combination for searching a database of

stored collected data: e.g. “Internet search requests using the term *sarin* or emails containing *poison gas* or “calls made from identifier x000325 after July 2, 2013” (NAS Report, 2015, p. 36).

Similar to a ‘query’ but applied in real time with filtering process as part of collection is a ‘discriminant’. The use of a ‘discriminant’ is associated with targeted collection and sometimes a ‘discriminant’ can be a specific ‘identifier’ such as a telephone number, an Internet Protocol (IP) address or an email address. The Committee on Responding to Section 5(d) of Presidential Policy Directive 28 in the US regarding the exploration of alternatives to bulk SIGINT collection provides in the NAS Report (2015) a resourceful example of how metadata collected in bulk are used in contact chaining. As illustrated in the drawing (see Figure 6), A and B are targets and a targeted approach will use a discriminant like “collect all calls to or from A or B”. The outcome will be the multitude of contacts displayed in the figure. Yet, within a targeted only collection the discovery of C as an identifier of interest would not be guaranteed if all calls between A or B and C occurred before either A or B was identified as a target. Instead, bulk collection is more useful in this case and guarantees the identifying of C because it offers the possibility to look at older data or ‘history’ and is not limited to only the targets known at the time of collection (NAS Report, 2015, p. 43).

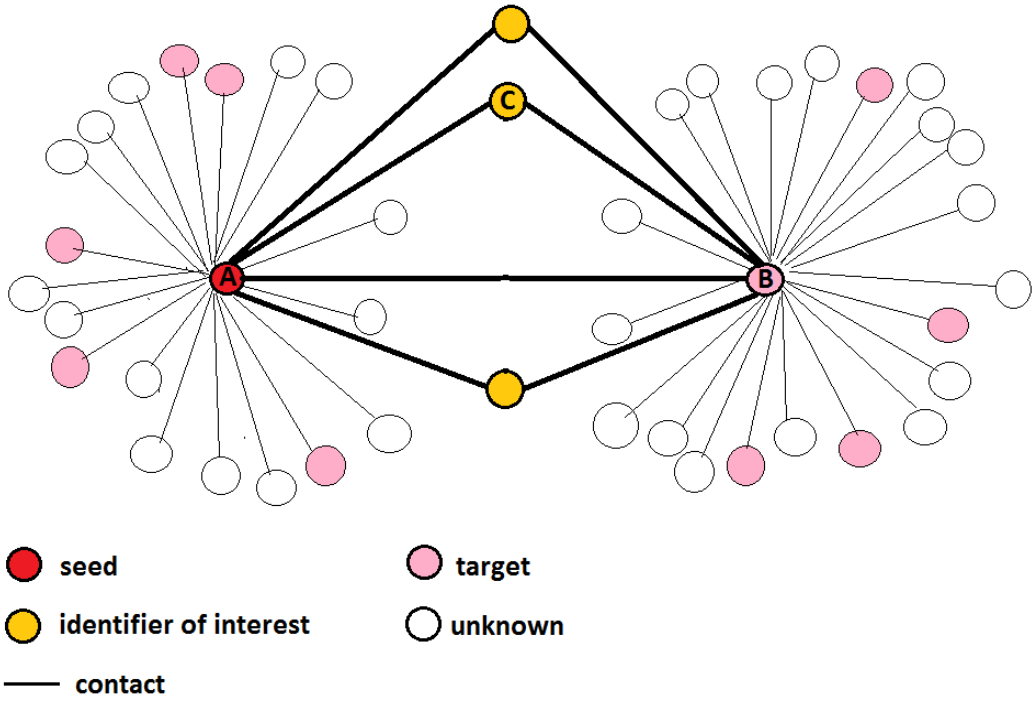

Figure 5 : A network of contacts among identifiers (source: NAS Report, 2015).

Storage and Analysis

The next stages in the bulk interception collection process are storage and analysis. The retained intercepted information has to be stored in large data repositories. NSA for example completed in 2014 the construction of a massive data repository in Utah officially known as Utah Data Center to store the information achieved through bulk interception (Johnson, 2017, p. 190). Privacy International reported that GCHQ has a program called *Black Hole* which is a metadata repository, storing email histories, information about search engine queries, social media activity, records related to hacking operations, and data on individuals' use of tools to browse the internet anonymously (Privacy International, 2016). The analysis of the large databases collected is conducted through data-mining and querying operations. For example, in counterterrorism investigations, the human analyst starts with a "seed" understood as "an identifier of a communications endpoint that has been obtained in the course of intelligence gathering and is deemed relevant to a possible threat" (NAS Report, 2015, p. 31). Based on this "seed", one or more queries of the data stores are formulated in order to find more information such as other parties communicating

with the “seed”. This can be done by querying for collected metadata or even for communications content when is available. By examining the possible multiple connections of the “seed”, the analyst can then find a pattern in these connections leading in the end to a more complete picture of that “seed” involvement within a larger network such as a terrorist organization (NAS Report, 2015, p.31).

Working with the collected SIGINT data involves the utilization of specific software tools. Such a tool developed and deployed by NSA was XKeyscore, a formerly secret computer system with a global reach, used for data-mining and querying. According to *The Intercept*, XKeyscore allowed for ‘incredibly broad surveillance of people based on perceived patterns of suspicious behavior’ (Marquis-Boire et al., 2015, p. 1). Precisely, using specific queries based on location, nationality and browsing history such as “germansinpakistn” as was revealed by one of the leaked slides, would show all individuals in Pakistan accessing certain German language forums (Marquis-Boire et al., 2015). XKeyscore also offered the analyst the ability to look for the usage of encryption or anonymization technologies such as VPN or TOR network and other considerations that could lead to a target or to new strong selectors (electrospaces.net, 2014). Another software tool reportedly utilized for analysis by NSA was NarusInsight, a computer system which could monitor and filter in real-time huge volumes of internet traffic (up to 10 Gigabit/second a single NarusInsight machine) coming from submarine cables such as FLAG Atlantic 1 (electrospaces.net, 2014).

Dissemination

The last stage in the bulk interception process is dissemination. The results of analysis are distributed to other people and organizations both inside and outside the intelligence community. Sometimes these results are directly offered to policy makers. Also, other foreign partners (e.g. countries in The Five Eyes alliance) may also be granted access to these results. However, like the other stages of SIGINT process, dissemination should be properly regulated and overseen by specialized bodies in order to ensure that privacy and other human rights are not endangered. Although in the British case bulk interception is a surveillance power with a compulsory overseas orientation, it will unavoidably collect communications between individuals in the UK (Anderson, 2016, p. 28). This could happen because of the random contents of an international cable or via an intercepted server outside the UK. That is why, intelligence dissemination and sharing must be one of the focal points for the intelligence oversight bodies. With dissemination being

the last stage in the whole process of SIGINT collection through interception (bulk or targeted), we can now have a schematic representation of the whole sequence, as illustrated in the diagram (see Figure 7).

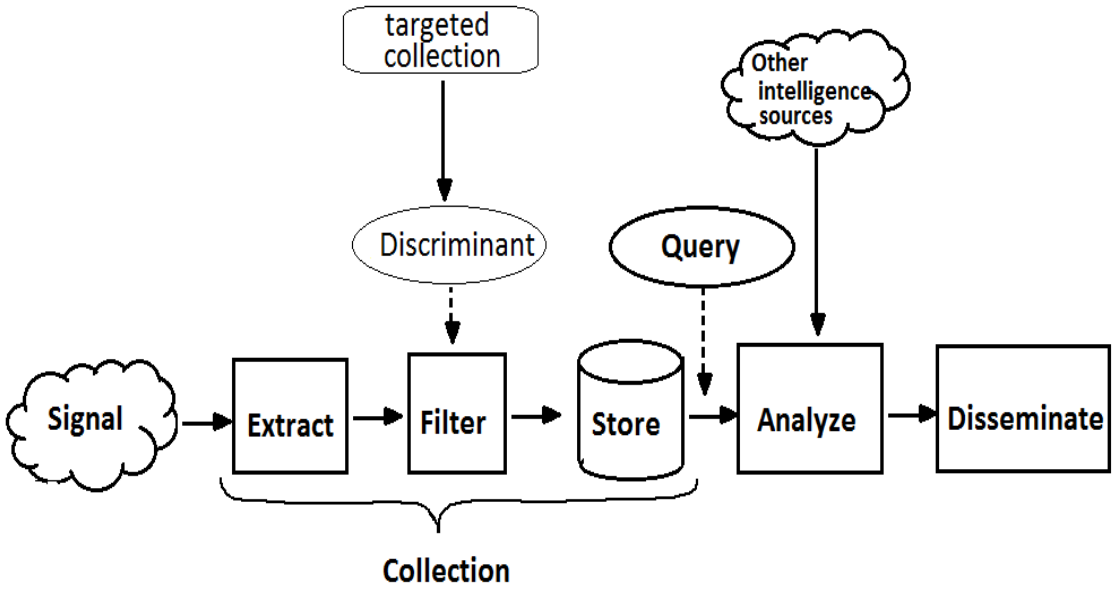

Figure 6 : A conceptual model of signals intelligence interception (adapted after NAS Report, 2015).

2.4.2 Bulk Interception - still very important because of metadata it can collect

In a report from 2015 named *Privacy and Security: A modern and transparent legal framework* examining bulk powers, the UK Intelligence and Security Committee of Parliament [ISC] concluded that the main value to GCHQ of bulk interception resides not in the actual content of communications per se but rather in the associated information with those communications. (ISC Report, 2015, p. 32). Specifically, this associated information that does not disclose the meaning of the communication encompasses "communications data" commonly known as metadata or "secondary data" (IPA 2016) and content-derived information. To put it differently, the basic who, when and where are sometimes more valuable for intelligence purposes than the actual content of intercepted communications (see Fig.5). Still, on the long term the endurance of bulk interception as an intelligence asset is challenged by the growing trends towards universal encryption and the anonymization of devices (Anderson, 2016, p. 91).

In the post-Snowden landscape, more online users are employing tools that can enhance or improve their online privacy also known as Privacy-Enhancing Technologies (PETs). Addressing the principles of data minimization and anonymization, PETs refer to "technologies that allow users to protect their data privacy while using (online) services or applications" (Schuster et al., 2017, p. 77). Examples include tools which can anonymize internet user's activity hiding even the metadata elements (The Onion Router, Tor, VPN) or protect communication through end-to-end encryption standards (E2EE) The foreseen solution to this problem is the deployment of another power, bulk equipment interference also known as hacking (Operational case, 2016, p. 30). Nonetheless, deployment of bulk powers such as bulk interception is sometimes the only way to achieve the quick results that are needed in a crisis scenario such as one involving a hostage situation. For example, the use of bulk interception by the GCHQ has been an essential support of military operations against insurgent and terrorist activity in a remote and unsafe territory like Afghanistan during the UK campaigns. In order to rescue and most probably save the lives of a group of kidnapped British nationals, it was necessary for the UK authorities to make use of bulk interception. Very often in this kind of scenarios, intelligence services have to start their investigation from scratch, with no prior intelligence which can help and under conditions of extreme time pressure (Anderson, 2017, p. 162).

2.4.3 Bulk Equipment Interference

Bulk equipment interference (EI) which is also known as 'bulk hacking' or 'computer network exploitation' is a surveillance power and covers a series of techniques encompassing meddling with electronic equipment. In the words of David Anderson QC, bulk equipment interference methods involve "hacking or the implantation of software into endpoint devices or network infrastructure to retrieve intelligence" (Anderson, 2016, p. 34). Equipment which may provide communications or other information valuable for intelligence purposes, include computers, smartphones and electronic storage gadgets. Copying data directly from a computer of smartphone is also part of this surveillance power. Yet, this power may also involve more complex operations such as exploiting existing vulnerabilities in software for the purpose of remotely extracting information or monitor the owner of the device (EI Draft Code of Practice, 2016). This can be translated as intentionally corrupting software, systems and services and spreading malware with the aim of retrieving intelligence. Under the law IPA 2016, a bulk EI warrant may be used by

the intelligence agencies for overseas collection both the content of communications as well as equipment data which discloses for example the time and date a photo was taken (EI Draft Code of Practice, 2017, para. 2.4).

A key justification for the exploitation of bulk EI power is the fading efficiency of bulk interception owing to technical developments such as end-to-end encryption in dealing with counter-terrorism, counter-proliferation and cyber-defense. Although EI has been used extensively on the basis of targeted thematic warrants by SIS to identify dangerous extremists in Syria for example, it was anticipated at the time of the independent review of the bill that bulk EI warrants are "likely to be only sparingly used" (Anderson, 2016, p. 123). However, only two years into the IPA as active legislation, in a letter from Home Office addressed to the Chair of Intelligence and Security Committee, it was indicated that "GCHQ have revisited the previous position and determined that it will be necessary to conduct a higher proportion of ongoing overseas focused operational activity using the bulk EI regime than was originally envisaged" (Home Office letter signed by the Minister of State for Security and Economic Crime, 3 December 2018). Therefore, one can notice a growing importance of this bulk investigatory power especially in the cases of counter-terrorism.

Bulk hacking along with bulk interception, have been intensely criticized by civil society actors and human rights organizations for their *modus operandi*. They were described as "aggressive forms of surveillance" by the UN Special Rapporteur on the right to Privacy who also criticized the disappointing attitude of "some major powers" regarding state behavior in cyberspace in the context of privacy rights (Cannataci, 2017, p. 20). Privacy International emphasized that hacking by its very nature is dangerous and exploits flaws in software and hardware utilized by millions of users (2016, p. 7).

By intentionally preserving systemic security vulnerabilities in order to exploit them for intelligence purposes, the authorities could open the door to other potential attackers such as foreign intelligence agencies or cyber-criminals. Such a case was the 2017 malware attack known as ''WannaCry'' which affected hospital electronic infrastructures, blocked the computers of businesses, governmental institutions and individual users around the world. According to the US Justice Department which filed criminal charges against, the attack was initiated by a North Korean operative. However, the surprising fact which surfaced in the public space afterwards was that the software used for this attack was based on a hacking tool developed by the NSA itself for surveillance operations (Yadron & Granick, 2018).

The state-sponsored implantation of malware into computer infrastructure systems or networks poses a lot of risks for many innocent people and that is why in some countries like Germany such approaches have been declared unconstitutional (Ni Loideain, 2019, p. 182). The potential for damage is huge and when the state agencies fail to maintain a firm control over these powerful cyber exploits, "hacking looks less like a targeted sniper's bullet and more like a poorly-aimed bomb, with a broad and indiscriminate blast radius" (Pfefferkorn, 2018, p. 10). Thus, bulk hacking can have terrible consequences like offering potential access to cyber-criminals to the devices of large groups of people and access to network infrastructure upon which citizens depend for everyday transactions (Privacy International, 2016, p. 8). As one of the experts who contributed to the Science and Technology Committee Report put it:

> "[t]he right way to get round encryption is targeted equipment interference, and that is hack the laptop, the phone, the car, the Barbie doll or whatever of the gang boss you are going after, so that you get access to the microphones, to the cameras and to the stored data. The wrong way to do it is bulk equipment interference" (Professor Ross Anderson quoted in Ni Loideain, 2019, p. 182).

2.4.4 Bulk Acquisition of Communications Data

Bulk acquisition is the power of SIS to require telecommunications operators to retain and disclose communications data (metadata). Operators could also be asked by SIS to select for examination the acquired communications data by applying certain algorithms. Basically, the communications data obtained via these Communications Service Providers (CSPs) is the *who, where, when, how* and *with whom* of communications and not the intrinsic content. Examples include information extracted from a telephone service subscription, from a detailed bill or from metadata of emails exchanges and phone calls made. In this sense, of intelligence value could be the address to which a message is sent, the time and duration of a communication, the location of the device, the telephone number or email address of the originator and recipient. As it is defined in the Bulk Acquisition Draft Code of Practice (2016), communications data "is limited to data which does not reveal anything of what might reasonably be considered to be the meaning of the communication" (p. 5).

Unlike the previous surveillance powers presented, bulk acquisition can be utilized domestically being described by the GCHQ as "the primary way in which GCHQ discovers

new threats to the UK" (Anderson, 2016, p. 93). According to GCHQ, bulk acquisition is less convenient than bulk interception for foreign operations because it would have to rely on the cooperation of overseas communications service providers (Anderson, 2016, p. 94). The Security Service MI5, highlights on its webpage that "fast, secure access to bulk communications data is essential to MI5 in pursuing our investigations", depicting this power as a "fundamental investigative tool that the agencies use on a daily basis" (MI5 website). Just as importantly, the Intelligence and Security Committee of Parliament referred to this surveillance power as "a critical capability" (ISC Report, 2015, p. 48).

Although bulk acquisition is a surveillance power which only collects metadata and no content related information, in the UK it is acclaimed by the SIS as an essential tool for national security. Given its domestic focus, it is used on a daily basis allowing the SIS to "conduct more sophisticated analysis, by 'joining the dots' between individuals involved in planning attacks, often working from fragments of intelligence obtained about potential attacks" (Operational case, 2016, p. 37). In his Report of the Bulk Powers Review, David Anderson Q.C. endorses the SIS claim that "bulk acquisition offers the advantages over other techniques of speed and the ability to conduct more complex and comprehensive analysis" (Anderson, 2016, p. 101).

Metadata has a standardized format, mostly numerical, and this makes it more suitable to aggregation and to quantitative analysis using data analytics, for example (Bernal, 2016, p. 248). While the actual content of communications is often more difficult to interpret and understand due to different linguistic codes or because of encryption technology, metadata allow a swift examination and may include new types of data such as geolocation. Nevertheless, in terms of privacy interference, metadata is as intrusive as content but "differently intrusive" (Bernal, 2016, p. 248).

2.4.5 Bulk Personal Datasets

Bulk Personal Datasets [BPDs] are sets of information about a considerable number of persons, the majority of whom will not be of any interest to the SIS. These datasets are held electronically by the SIS and analysts will only examine and extract the data relating to the minority who are of intelligence interest (Operational case, 2016, p. 43). Datasets can refer in this context to the passport register for example or the electoral register. In the UK, the main categories of datasets revealed to the Investigatory Powers Tribunal [IPT] were: law enforcement/intelligence datasets, travel datasets, communications datasets,

finance datasets, population datasets and commercial datasets. Personal data is understood here as "data relating to an individual who can be identified from those data, or from those data and other information which is in the possession or, or likely to come into the possession of, the data controller" (Anderson, 2016, p. 43). The BPDs are employed by the SIS for multiple purposes such as identification of potential terrorists and agents, prevention of imminent travel in some cases or to help the SIS to prioritize work.

The utilization of BPDs by SIS in the UK was first exposed in a 2015 report of the Intelligence and Security Committee and subsequently Privacy International initiated a legal challenge in the Investigatory Powers Tribunal about whether the acquisition, utilization, retention, disclosure, storage and deletion of BPDs is in accordance with the law or necessary and proportionate (FRA Report, 2017, p. 69). The IPT found that the SIS were responsible up until March 2015 for infringement of the right to private life by virtue of the lack of foreseeability to the public and the lack of adequate oversight (UKIPTrib 15/110/CH). However, after these techniques encompassing the use of bulk data were publicly acknowledged and followed by improvements regarding the oversight regime, the IPT accepted that BPDs were compatible with the right to private life. In his assessment of bulk powers, David Anderson Q.C. (2016) concluded that BPDs "are of great utility to the SIAs [and that] their principal utility lies in the identification and development of targets, although the use of BPDs may also enable swift action to be taken to counter a threat" (p. 117).

2.5 Bulk collection regimes

2.5.1 Bulk collection regimes around the world

In the edited volume *Bulk collection: systematic government access to private-sector data*, after compiling the results from 12 country reports on the use of bulk collection, Cate & Dempsey (2017) found extensive evidence that governments around the world have been exercising bulk surveillance powers 'in the dark' most often in the name of national security (p. xxix). The authors also acknowledge a change of trends triggered by the Snowden leaks, with countries such as the US and the UK moving towards greater transparency regarding bulk collection. Following this tendency, a number of states around the world have amended their legislation in order to more clearly define the surveillance powers granted to SIS. This move from total secrecy to more transparency, at least in

theory, subjected the bulk powers to the democratic process (Cate & Dempsey, 2017, p. xxix).

In the EU, member states such as France, Germany, Sweden and the Netherlands have reformed their surveillance regulation extensively in the last decade. Beyond the EU and the US, Australia has operated important changes in their surveillance related legislation and India is building a centralized surveillance system. Regarding the issue of large-scale surveillance in countries like China and Russia, we are following Bernal (2016) who stated that "the extent to which more seemingly repressive regimes utilize these kinds of technologies is largely a subject of conjecture; it is a reasonable assumption that it is used extensively" (pp. 247-248).

In Australia the Telecommunications (Interception and Access) Amendment (Data Retention) Act of 2015 introduced a mandatory metadata retention scheme through which the LEAs and the SIS have been granted access to track and retain metadata, a capability which resembles the concept of bulk acquisition of communications data. These institutions which include Australian Security Intelligence Organisation (ASIO) and Australian Federal Police (AFP) can request access to an individual's metadata without a judicial warrant. The Australian data retention legislation represents a disproportionate interference with individual privacy rights being also incompatible with the precedent established by the Digital Rights Ireland decision of the CJEU that annulled the Data Retention Directive in the EU. The country's leading privacy organizations such as The Australian Privacy Foundation (APF) and Digital Rights Watch warned that the executive was planning to introduce new law-enforcement powers that would allow authorities access to encrypted digital data by the exploitation of back-doors. Moreover, Privacy International has drawn attention that the Australian Attorney-General's Department foresees a number of reforms to Australian national security and communication policies, including increased powers to monitor and intercept communications.

In France, the Intelligence Act 2015 dubbed by the media as 'le Big Brother français' was passed in June 2015. The law amends the Interior Security Code which covers the various intelligence techniques available to the French SIS including provisions for mass retention of communication metadata. Among other things is the provision (Article L. 851–3) that the government may request telecommunications and internet service providers to automatically examine all metadata they process using certain algorithms in order to detect a potential terrorist threat (FRA Report, 2015, p. 24). The new law also introduces an independent oversight body called National Commission of Control of the

Intelligence Techniques (CNCTR) which provides the prime minister with a non-binding opinion on the algorithms and the parameters chosen. Still, according to the law, only the prime-minister can authorize this bulk collection power after consulting the CNCTR for an advisory opinion regarding the compatibility of the measure with the principles of necessity and proportionality.

In the Netherlands, the two institutions that are entitled to conduct bulk collection are the General Intelligence and Security Service (AIVD) and The Military Intelligence and Security Service (MIVD). The main law governing the bulk collection powers is currently the Dutch Intelligence and Security Services Act 2017 [WiV 2017] which went fully into effect on 1 May 2018 replacing the previous Dutch Intelligence and Security Act 2002. A combined institutional effort of the AIVD and MIVD is the Joint Sigint Cyber Unit [JSCU] established in 2014 and which overtook the role of the previous National Signals Intelligence Organisation [NSO]. The official aim of the JSCU is to specifically combat cyber threats. However, the launch of the JSCU with a new working method pushed for a need to update the legal framework governing the Dutch intelligence services. More exactly, the main piece of legislation in effect at the time known as the Dutch Intelligence and Security Act 2002 [Wiv 2002] did not allow the agencies to wiretap 'cable-bound communications' under any circumstances. When the law was drafted in 2002, the clause regarding cables was irrelevant due to the fact that all international voice, text and data communication was carried, at some point among the path, via a wireless connection. Yet, in the current environment most internet traffic goes via (fibre optic) cables. Hence, the Dutch intelligence agencies including the newly created JSCU were prohibited from conducting bulk collection via cables. All the interceptions of communication that is cable-bound (telephone and internet, glass-fibre cables) had to be targeted and they needed prior ministerial approval. Furthermore, it was assumed that the legislation in this field applies to overseas interceptions as well. With regard to the Wiv 2002, in December 2013 after a review of the existent regulation, the Intelligence and Security Act Evaluation Committee (also known as the Dessens Committee) decided that the existing statutory powers were no longer sufficient and must be augmented. The Committee also recommended the introduction of bulk interception of telecommunications but linked the increase of powers to improved statutory safeguards of privacy and oversight. This recommendation was one of the most criticized elements of the report, and even the executive advised that it needs further evaluation (van Eijk, 2014). Dutch NGOs such as Bits of Freedom have expressed concerns about the enormous potential for bulk interception that the Netherlands holds

given that the Amsterdam Internet Exchange Point (AMS-IX) is the second largest landing station in Europe (Bigo et al., 2013).

The Snowden revelations in 2013 had a profound impact on a variety of national legal frameworks in Europe. Particularly enough, in the Dutch case these ground-breaking revelations coincided with the due review of the Dutch Intelligence and Security Act 2002, a process already underway (van Eijk, 2014). The public opinion found out among other issues that the AIVD was hacking into websites and that the NSA had access to 1.8 million telecommunications metadata which apparently were delivered by the Dutch intelligence services. The complete denial of all these allegations by the interior minister at that time when summoned by the Parliament, led to a climate of tension within the Dutch public sphere. The subject generating the most negative reactions was the involvement of the Dutch agencies in handling over data to a foreign intelligence agency - the NSA (van Eijk, 2014). The new law regulating intelligence activities, the Dutch Intelligence and Security Services Act 2017 [WiV 2017] has been in the making for several years during which themes like 'mass surveillance', foreign intelligence agencies' influence in the Netherlands and privacy protection have been present in the public opinion debates. The Act which went into effect on 1 May 2018 colloquially named by the general public the 'Tapping Law' or the 'Dragnet Law', offers to the intelligence services new powers to tap cables and collect information. However, in an advisory referendum held on 21st of March 2018 with more than six million people taking part, the majority voted against the new 'dragnet law'. As the referendum is not legally binding, the law still went into effect. Yet, the members of the executive have highlighted in the Parliament the existing safeguards and announced that there will be some amendments. The amended version will supposedly stipulate tighter checks for the utilization of surveillance powers by the intelligence agencies. Also, it will make the exchange of data between the Dutch and other states' intelligence services more transparent by listing specific conditions under which it can take place.

Next, we will next on the case of the UK, a country that in recent years has reformed its surveillance legislation extensively. The UK is a particularly important case as a potential model of best practice given the massive influence that British legislation still has in over 25% of the UN's member states that still are part of the Commonwealth (Cannataci, 2016 A: 14).

2.5.2 The UK – a leading model in regulating bulk surveillance?

In the UK, the most significant development in recent years regarding the surveillance powers regime was the implementation of the *Investigatory Powers Act* 2016 [IPA 2016]. This piece of legislation adopted in November 2016 ratifies and even extends bulk collection powers, providing a new framework to govern the utilization and oversight of investigatory powers. It regulates interception and bulk acquisition of communications and other forms of data by intelligence agencies and law enforcement. The Act replaces or updates a series of ancestor legislation on which the investigatory powers were based including the Regulation of Investigatory Powers Act [RIPA] 2000, the Data Retention and Investigatory Powers Act [DRIPA] 2014 and the Intelligence Services Act [ISA] 1994. Most notably is the fact that the new law boldly assumes the notion of *bulk* (collection) which authorizes the issuance of bulk interception warrants, bulk acquisition warrants, bulk equipment interference warrants, and bulk personal datasets warrants. Concerning the aspect of governmental access to private-sector data, the new IPA allows SIS to request the Communications Service Providers [CSPs] to retain data on the activity of all their users which will then become available for the authorities to access through a more targeted process called the request filter (Cate & Dempsey, 2017, p. xxxi). IPA is especially important as a prototype of surveillance legislation because it establishes a legal basis for advanced modern surveillance techniques and hence providing an appropriate framework of analysis to address different issues (Murray & Fussey, 2019, p. 32).

A preceding comprehensive evaluation report on bulk powers commissioned by the government and conducted by the Independent Reviewer of Terrorism Legislation [IRTL], David Anderson Q.C. concluded that "there is a proven operational case for three of the bulk powers, and that there is a distinct (though not yet proven) operational case for bulk equipment interference" (Anderson, 2016, p. 1). For what concerns the existing alternative methods to these powers, the review found that "they are often less effective, more dangerous, more resource-intensive, more intrusive or slower" (Anderson, 2016, p. 1). However, the new law also dubbed by privacy advocates as the 'Snoopers' Charter', has been strongly criticized by civil society organizations in the UK. Gus Hosein from Privacy International referred to IPA as a "draconian and expansive piece of surveillance legislation that no other liberal democracy has had the gall to attempt" labelling it "a bad example for the world" (Hosein, 2017). Criticism also concerns the introduction of thematic warrants

in relation to targeted surveillance powers, a notion which according to critics enables the use of bulk collection disguised as targeted collection (Ryk-Lakhman, 2016).

The thematic warrant delegates to SIS the choice as to whose privacy will be interfered with, increasing this way the risk of arbitrary decision-making and challenging the implementation of effective judicial authorization. For example, a thematic warrant may authorize the hacking of all mobile phones of members of the Muslim faith in Birmingham, or the interception of the communications of anyone suspected of having travelled to Turkey in the last three months (Ryk-Lakhman, 2016).

An incontestably positive development brought by the IPA 2016 is the introduction of a series of oversight and accountability measures in order to improve the existing oversight regime. The key innovation was the introduction of a double-lock system which refers to the fact that the most sensitive and intrusive surveillance warrants authorized by a politician such as the Home Secretary or the Foreign Secretary will also require the review and approval of a senior judge. Furthermore, the Act established a new and better resourced independent oversight expert body, IPCO, to supervise how the bulk powers are used. Within the general architecture of the new oversight system, IPCO complements the important roles of two other institutions: The Intelligence and Security Committee of Parliament and the Investigatory Powers Tribunal. In his Statement at the End of Mission to the United Kingdom of Great Britain and Northern Ireland from June 2018, the UN SRP has praised the "significant progress" made by this country regarding its oversight system (Cannataci, 2018).

2.5.3 European case law on bulk surveillance

In Europe, the legality of bulk collection has been challenged ever since the judgment of the Court of Justice of the European Union (CJEU) in *Digital Rights Ireland* (2014) where CJEU annulled Directive 2006/24/EC, which set out rules for the retention of metadata by private companies for the purposes of their later use by law enforcement agencies. CJEU stated that the mere retention, even if the data were never used, interfered with the fundamental right to privacy under the European Charter of Human Rights (ECHR). Although some member states have tried to decrease the domestic effects of the CJEU's ruling by enacting national surveillance laws, courts are increasingly overruling them on constitutional grounds – often with references to CJEU's judgement in Digital Rights Ireland (Watt, 2017).

Another milestone ruling of the CJEU regarding bulk collection is the 2015 *Schrems v Data Protection Commissioner*. It refers to the fact that data transfers of EU citizens from Facebook European subsidiary, under the US *Safe Harbour* arrangement are not safe and should be suspended on the basis that the US does not afford satisfactory level of protection of personal data (Watt, 2017). In other words, the agreement permitting simplified transfer of personal data between EU and US companies was annulled by this judgement because of its lack of compliance with privacy and data protection obligations (Marin, 2017, p. 116). This decision must also be regarded in the context of realities emerged after Snowden's revelations about the various forms of bulk indiscriminate surveillance conducted by the NSA.

Bulk collection regimes in Europe have also been challenged by the judgements of the European Court of Human Rights (ECtHR) especially in two cases: *Zakharov v Russia* (2015) and *Szabo and Vissy v Hungary* (2016). In *Zakharov*, the ECtHR indicated that blanket access to all information, without specifying particular reasons, the categories of persons and crimes, do not achieve the requirements of necessity and proportionality (Watt, 2017, p. 237). It also established that given the inherent secret nature of surveillance, the individual under surveillance will unavoidably be prevented from seeking a remedy or taking part in any review proceedings. Consequently, the Court stated that "it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights" (ECtHR, 2015). Thus, the ECtHR delineated the elements of an effective remedy and underlined the challenges posed specifically by secret surveillance. In *Szabo* the ruling dealt with surveillance powers of the Hungarian intelligence agencies under the Police Act 1994. Under the European Convention on Human Rights framework, in both cases Article 8 regarding individual privacy was trespassed.

However, in a stream of landmark judgements issued by the ECtHR which tackled the topic of bulk interception, one can certainly notice an important change. Precisely, the decisions given in the cases of *Centrum För Rättvisa v. Sweden (June 2018)* and *Big Brother Watch and Others v. the United Kingdom (September 2018)* have clearly established that in certain circumstances and conditions the utilization of bulk powers is perfectly legal and legitimate. More exactly, it could be said that these new decisions are now endorsing "the new normal" in Europe (Lubin 2018), specifically the creation of intelligence laws with a *bulk* dimension. As Wetzling & Vieth (2018) observed, "most parliaments have expanded, rather than curtailed, surveillance powers in recent intelligence

reforms" (p. 10). In return, the ECtHR tries to complement this surveillance with conditions and safeguards. Thus, the legality *per se* of bulk collection policies is no longer the main concern but rather how to operate these investigatory powers.

In the case *of Centrum För Rättvisa v. Sweden* (2018; 2021) regarding bulk interception of electronic signals for foreign intelligence purposes, the court found that overall, the Swedish system of bulk interception provided acceptable and enough guarantees against arbitrariness and the risk of abuse. Also, the ECtHR "for the first time adopted the view that automated haystacks — databases of stored 'unprocessed information', raw materials not yet 'subjected to manual treatment'— do not trigger an Article 8 infringement" (Lubin, 2018, p.1). In 2021, the Grand Chamber of the ECtHR ruled that in the case of Sweden's bulk interception regime, there had been a violation of Article 8, the right to privacy.

The Swedish case was complemented by another important judgement, *Big Brother Watch and Others v. the United Kingdom* (2018; 2021) regarding bulk interception. While the Court found that the UK's bulk interception practices were unlawful because of inadequate safeguards and lack of oversight, it did not establish that bulk interception itself was unlawful *per se*. The Court went further by stating that: "It is clear that bulk interception is a valuable means to achieve the legitimate aims pursued, particularly given the current threat level from both global terrorism and serious crime" (ECtHR, 2018). Hence, by taking this decision the Court upheld the Swedish regime for bulk interception. Both judgements are indicating that this practice "is here to stay" (Wetzling & Vieth, 2018, p. 10) and also that the emphasis has now shifted on building more rigorous and effective oversight mechanisms. In May 2021 the Grand Chamber of the ECtHR unanimously ruled that GCHQ's bulk interception practices violated right to privacy.

Technical expertise has become a crucial dimension in making oversight more effective in the era of big data. As a former compliance director in the NSA put it, "the era of big data requires big compliance, and a fundamental part of big compliance is the reconciliation of the written rules with a very real set of technologies" (John DeLong quoted in Wetzling, 2017, p. 3). In order to appreciate the complexity of the risks involved for the fundamental human rights and democratic governance, oversight bodies need more than ever before to fully comprehend the whole process of creation and interlinking of pools of data derived from the manipulation of big data. Where the data is being created, where it is resident and who holds the data are becoming crucial aspects of the oversight process.

Oversight systems can also enhance citizens' trust and understanding of bulk collection practices and also to educate the public about the activities and role of SIS. They serve 'the ultimate goal of protecting the public against abuse in the implementation of surveillance measures.' (FRA Report, 2017, p. 87). An interesting example of transparency illustrating this direct contact with citizens can be found in Sweden where both expert bodies -SIUN and the Commission on Security and Integrity Protection (SIN) – may be approached by citizens asking to verify whether they are under surveillance, and whether this surveillance was lawfully conducted (FRA Report, 2017, p. 120). Another interesting example can be found in the U.K. where the independent oversight body IPCO has initiated a civil society dialogue on proportionality standards for the review of bulk powers. More exactly, IPCO asked NGOs and other members of civil society for an input in identifying the wide variety of aspects that the Judicial Commissioners should take into account when evaluating the proportionality of bulk warrants (Wetzling & Vieth, 2018, p. 47).

2.5.4 Bulk collection in the US

The 2013 revelations about the NSA's bulk collection programs have exposed clear structural fractures in the architecture of the American oversight system. The Snowden disclosures brought to light a conundrum laying at the very centre of the U.S. compliance-oriented oversight system, namely that intelligence activities can be lawful but nevertheless illegitimate. Put it differently, the main problem uncovered was not "a government agency run amok: the NSA never meaningfully exceeded the writ given to it by the White House, Congress, and the courts, at least not intentionally" (Byman & Wittes, 2014, p. 129). Indeed, the problematic aspect was rather how the intelligence community have been using powerful legal tools like Section 702 of the FISA and Section 215 of the USA PATRIOT Act, for purposes exceeding their original role. Precisely, these two legal tools designed to facilitate foreign intelligence investigation, have been instead exploited by the NSA for sweeping up vast amounts of communication data belonging to American citizens. The U.S. Executive has defended the legality of the exposed surveillance programs such as PRISM and the telephony metadata bulk collection program by actually invoking their compliance with Foreign Intelligence Surveillance Act (FISA) and its amendments.

Under the provisions of the now expired Section 215 of the PATRIOT Act, the NSA was able to petition the FISA Court to order the transfer of records or 'any tangible things' from third parties such as telephone companies to the SIGINT agency which could then

store and query them as needed. The sole necessary condition for the acquisition of such records was their alleged relevance to operations involving international terrorism, counterespionage, or foreign intelligence investigation. Nevertheless, the Snowden leaks have exposed how the NSA had relied on this legal instrument together with the authorisation from the FISA Court, in order to run a massive program of collecting in bulk, Americans' telephony metadata. The adoption of the USA Freedom Act in 2015 meant the end of this bulk collection program. Yet, the Freedom Act left intact other programs involving surveillance of U.S. citizens such as the programs conducted under the authority of Section 702 of the FISA.

Section 702 of the FISA was enacted in 2008 for legalising Bush administration warrantless wiretapping program and has been hailed ever since by the Executive and the intelligence community, as a crucial counterterrorism tool. Section 702 is directed towards targeted collection of communications belonging exclusively to non-U.S. persons believed to be located outside the U.S. It forbids surveillance of American persons, including the use of foreign targets as a vehicle for gathering intelligence about Americans. However, a backdoor search loophole allows the NSA to collect without a warrant, communications belonging to U.S. citizens as part of the collection process targeting foreigners and their communications with U.S. citizens. In the words of law professor Laura Donohue who also serves as Amicus Curiae for the FISC, "[by employing Section 702] the intelligence community monitors and collects Americans' international communications, as well as entirely domestic conversations, without oath or affirmation of wrongdoing" (Donohue, 2017, p. 2). The collection of emails and calls belonging to U.S. citizens caught up in the net of foreign intelligence acquisition is downplayed in the discourse of the intelligence community and described as 'incidental'. A further accountability challenge uncovered by Snowden is that the NSA shares the 'incidental' collection about American citizens with the other agencies, particularly the CIA and the FBI. Domestic law enforcement agencies like the FBI can therefore, access communications belonging to U.S. citizens by taking advantage of a legal tool intended for foreign surveillance. The FBI can comb the entire volume of data acquired under Section 702, in order to find specific information which can then be used in their domestic criminal investigations. In this manner, the FBI evades the requirement of obtaining a warrant for monitoring the communications of certain targets.

The pervasive effects of Section 702 including the high likelihood of trespassing Americans' constitutional rights, have been the subject of vigorous debates in the Congress. The lawmakers have requested the Executive to minimise the use, retention and sharing of

data belonging to US citizens and some of them like the Republican Jim Sensenbrenner called for reforms that will "put the F[oreign] back in FISA" (Laperruque, 2018). The example of Section 702 and the surveillance programs conducted under its authority is relevant for the point made earlier, that some intelligence activities can be lawful but nevertheless illegitimate. That is why, as Goldman (2016) put it, "[c]omplaints that intelligence agencies such as the NSA 'continue to evade oversight' therefore miss the mark […]; rather the failure is in the disjunction between what the American oversight system is designed to do, and what 'we the people' may expect of it" (p. 220). It can be stated, therefore, that the overreliance of the US oversight system on compliance has proven "unequal to the task of opposing the 'collect everything' mindset" (Schlanger, 2015, p. 205).

2.6 Conclusion

With bulk collection technologies already an operational reality, the challenge for the academic research in this field is striving to fill the gap between praxis and conceptualisation. The under-theorisation of such an important concept like 'bulk collection' can generate confusion and uncertainty, features which weaken the democratic governance of intelligence. That is why this chapter has tried to bring more clarity regarding the conceptual dimension by firstly tackling the bulk/targeted distinction and secondly, the *bulk collection*/*mass surveillance* terminological debate. The later distinction provides the pretext for a deeper discussion and has led us to question which are the fundamental differences -if there are any- between (domestic) intelligence collection in a democracy based on the rule of law and collection in a non-democratic, illiberal regime. After this conceptual treatment of the subject, in the second half of the chapter we focused on the technological and operational dimensions of bulk collection and briefly at how these new technologies are implemented in different countries including Australia, France, the Netherlands and especially in the U.K. One of the conclusions of the chapter is that the challenge for democratic governance has been the attempt to increase the legitimacy and effectiveness of these practices. The Snowden revelations damaged the trust at the societal level towards public authorities, in particular towards intelligence and national security apparatuses. How feasible is it that a contested practice like bulk equipment interference or bulk acquisition be integrated within a democratic framework based on the rule of law and protection of civil rights? A potential answer could be that "robust oversight practices and

good laws can serve as bulwarks against the erosion of fundamental rights" (Wetzling & Vieth, 2018, p. 6).

At the same time, it is also important for the current research that we understand the challenges in providing security generated by the large spectrum of versatile threats that intelligence services need to fight. A zero-sum condition means in this context that as a government, you will either make use of the new surveillance technologies or suffer major intelligence failures such as terrorist plots and attacks, foreign hostile interference in different sectors such as economy and critical infrastructure or even interference in domestic politics and electoral processes. Phenomena such as trans-nationalization of terrorism, money-laundering flows, political extremism and cyber-hostile actions require tools and means of countering that cannot override the use of information. Hence, the necessity to adapt to these new threats has produced an operational intelligence reality centred on technological innovation and intelligence cooperation which cannot be circumvented (Wetzling & Vieth, 2018). In this sense, investigatory powers such as bulk interception and bulk hacking must be properly regulated, and their use must be subject to enhanced monitoring by intelligence oversight bodies complemented by lawmakers, judiciary and diverse actors with different expertise, from civil society organisations and academi

CHAPTER 3 - FRAMING THE DEBATE THROUGH EXPERT DISCOURSES: GCHQ'S POST-SNOWDEN STRATEGY OF PUBLIC LEGITIMATION AND THE ROLE OF CRITICALLY ENGAGED ACADEMIA IN CHALLENGING THE INTELLIGENCE DISCOURSE

3.1 Introduction

The Snowden disclosures about the unlawful use of bulk surveillance led to public controversy and widespread questioning of intelligence organisations' commitment to the democratic principle of serving the public. In this sense, the disclosures opened up novel sites of critical interventions by problematising the relationship between the intelligence community and the public. In order to re-establish public trust and justify the surveillance practices exposed by Snowden, some intelligence agencies have taken major steps into the public arena through extensive communication efforts and unprecedented openness. This move is being pursued through different mediums, ranging from museum exhibitions to official policy documents inviting the public "to join" in the development of new strategies (GCHQ, 2021, p. 5). As part of this process, some official public reports have gone as far as to make detailed case studies about the use of bulk surveillance technologies in different reality-inspired scenarios and their operational outcomes.

Prior to the Snowden revelations, public information regarding the technologies of intelligence collection used by the secret services in the UK was scarce. Similarly, the move towards increased communication and engagement with the public continues to take place within the same expert knowledge framework which underpins the authority and credibility of intelligence agencies in these matters. The post-Snowden communication of intelligence practices aimed at the public consists mainly of technical discourse and is beset by an inherent power-knowledge dynamic (Lund Petersen, 2019). In other words, given that the information

is highly technical, most of the citizens do not understand and thus underestimate what is technologically possible or reversely overestimate what is possible. Therefore, the top-down expert discourse of intelligence and security professionals must be challenged by alternative expert perspectives originating outside the national security community. Topics such as technologies of bulk collection or the use of artificial intelligence (AI) for national security feature such a high degree of technical complexity that without proper decryption in the public sphere, they remain as opaque as classified information.

This chapter argues that academia, particularly critically engaged scholars, are best equipped to challenge the monopoly of the expert discourse of intelligence organisations. This is argued as due to their independence, multidisciplinary expertise, and cutting-edge research in relevant fields, such as computer science, combined with critical potential and transparency. In the context of openness and widespread discursivity around new intelligence technologies, independent academic research can bring much-needed diversity of perspective to this increasingly important policy area.

Critically engaged scholars can raise public awareness by providing useful insights for social activists and enriching public understanding of complex technical issues, such as bulk surveillance and the use of AI for national security. However, without a public platform, for example through an organised forum for discussions, scholarly interventions on controversial issues like surveillance remain at the level of normative critique. A material setting thus becomes essential for the political articulation of these interventions and the identification of ensuing public issues (Marres & Lezaun, 2011; Gros et al., 2017). This chapter offers an example of such a platform for debate on intelligence governance and oversight, bringing together a diversity of discourses and stakeholders from academia, government, politics, and civil society.

3.2 The Snowden moment as a paradigm shift

The Snowden disclosures allowed a rare peek into the modus operandi and collection practices of the two major SIGINT agencies in the democratic world, the NSA and GCHQ. The sheer scale of their collection programmes, both in reach and the sophistication of technologies employed, caught even "seasoned observers" by surprise (Bauman et al., 2014, p. 122). The disclosures generated discursivity around the technologies used coming from a number of intelligence experts willing to talk publicly about their activity in the surveillance field (Aradau, 2019). The increase in discursivity created openings for academic research on

the subject, hence the opportunity for a more diverse range of informed perspectives in the public debate on this expert issue. Specifically, the fragmentary lifting of the veil of secrecy enhanced critical scholars' potential to formulate more robust arguments and normative critiques against controversial security practices. Given the high technological complexity of the surveillance methods revealed by the 2013 leaks, the role of critically engaged scholars who can challenge the official intelligence discourse from a position of both power and knowledge have become more prominent.

While the Snowden revelations brought a better understanding of the contemporary technologies and methods of large-scale surveillance for academic security experts and surveillance scholars, it also provided valid empirical evidence for civil liberties activists which could be used in court (Ben Jaffel et al., 2020). However, the translation of the Snowden files from journalistic sources into valid evidence was not a straightforward process. As the first site where a formal debate on the Snowden disclosures took place, the LIBE Committee of the European Parliament witnessed a series of discursive struggles over the files' validity. Closely researching these hearings, a group of scholars wrote about "the material difficulty of contesting surveillance practices politically" (Gros et al., 2017, p. 86). More precisely, Gros et al. (2017) noticed that the purely normative treatment of the uncovered surveillance practices by most academic literature ignores the importance of materiality, understood as the concrete steps by which these practices become "known, contested, and regulated" (p. 75). Therefore, a precondition for the emergence of a public debate on a contested issue like bulk surveillance is the existence of a material platform such as a public forum for articulating a diversity of discourses from different stakeholders (Marres & Lezaun, 2011).

A deeper and long-lasting effect of the Snowden moment has been the fissure created within the relationship between intelligence institutions and the public. The revelations struck at the very core of the intelligence community's legitimacy, which rests on the idea that they serve the public interest. As such, the fallout of the disclosures jeopardised the "dominant ontology of intelligence work" (Ben Jaffel et al., 2020, p. 2), raising questions as to whether intelligence agencies ultimately serve the government or the public. In his subsequent speeches and social media posts, Snowden has constantly articulated into the public sphere the dichotomous narrative of serving the public as being different from serving the government. This idea is also expressed in his autobiography: "I myself had sworn an oath of service not to an agency, nor even a government, but to the public […]" (Snowden, 2020, p. 6). In other words, the revelations have uncovered the existence of a profound disjuncture between the public interest and the activity of intelligence agencies. As Bauman et al. (2014) observed, the

2013 revelations "seem to imply significant transgressions of established understandings of the character and legitimacy of those institutions concerned with security and intelligence operations" (p. 122).

3.3 The recent origins of democratic intelligence governance in the UK

Intelligence studies scholar Mark Phythian (2019) observed that "technology is central to surveillance, and surveillance is in turn central to social science approaches to understanding intelligence" (p. 19). Within this analytical framework, the topic of surveillance can be seen as a research gateway into the intricate field of intelligence and its democratic governance. For instance, charting the emergence of intelligence governance systems in liberal democracies such as the U.S. and the U.K., reveals that domestic surveillance scandals have played a formative role. From the 1970s media revelations about the warrantless surveillance conducted by the NSA intercepting international telegrams of American citizens to the 2013 Snowden disclosures, domestic surveillance public scandals have triggered pivotal steps in the establishment of existing intelligence accountability structures.

The rather recent historical emergence and evolution of intelligence governance reaches back to the great intelligence reforms of the mid-1970s in the U.S., followed by the U.K. some twenty years later with the adoption of the Intelligence Services Act. The first wave of reforms in the US was a direct effect of the congressional investigations led by the Church Committee into the NSA program of warrantless surveillance codenamed Shamrock, initially made public by The New York Times. In a similar fashion, it can be argued that the Snowden disclosures about the GCHQ surveillance program codenamed Tempora, made public by The Guardian, had an impact on UK policy leading to notable improvements in the field of intelligence governance.

In the UK, the main intelligence agencies have existed since the beginning of the twentieth century, while the establishment of parliamentary oversight of intelligence came much later, only in 1994. GCHQ and MI6 were placed on a statutory basis for the first time by the Intelligence Services Act 1994 [ISA] and MI5 through the Security Service Act 1989. Therefore, prior to the adoption of these laws, the agencies operated in the absence of an official acknowledgment, accountable only to the executive branch. As Herman (2001) noted, the three agencies were not "loose cannons", with MI5 being linked with the Home Office and MI6 and GCHQ under supervision of Foreign Office via the senior officials involved in the Joint Intelligence Committee (p. 123). Also, the Permanent Under-Secretary's Department,

responsible for Foreign Office liaison with MI6 and GCHQ, was to some extent, "a central authority for the oversight of foreign intelligence" (Herman, 2001, p. 123).

In spite of the strong intelligence ties between London and Washington, the congressional measures of establishing legislative oversight in the U.S. in the aftermath of 'the Year of Intelligence' (1975) did not prompt British lawmakers to adopt a similar approach at the time. It took the parliamentarians in Westminster almost twenty more years for establishing a statutory committee named the Intelligence and Security Committee [ISC], introduced via the 1994 Intelligence Services Act. Nevertheless, the ISC was not initially constituted as a parliamentary select committee but rather as a committee of parliamentarians reporting to the Prime Minister and with its componence chosen by the occupant of 10 Downing Street (Defty, 2020). These rules weakened the new oversight body's independence from the executive, whose activities it was supposed to review. It took British lawmakers another nineteen years to improve the ISC status via the Justice and Security Act 2013 which made it a statutory committee of the Parliament, meaning enhanced powers and credibility and expansion of its remit.

The British statutory scheme for national security surveillance operations does not have a long history either. Before the adoption of the Interception of Communications Act [IOCA] in 1985, operations like telephone tapping and mail opening by the British authorities, had no statutory footing other than the traditional royal prerogative power (Gill, 2016). The adoption of a statutory scheme for interception was a direct effect of the ECtHR decision in Malone v. U.K. [1984], that the tapping procedures upheld by the British Government at the time, were violating the right to privacy as it is defined in the Art. 8 of the ECHR. A significant provision of the 1985 act was the prerequisite of ministerial warrant for conducting interception. It also created two institutions with key roles in the subsequent development of the oversight system: the post of interception Commissioner with the role of reviewing the issuing of warrants, and a public complaints tribunal which preceded the Investigatory Powers Tribunal. It can be stated that the cornerstone of the oversight architecture in the U.K. was laid gradually between 1985 (IOCA) and 1994 (ISA), a development driven in the first place by the need to comply with the minimal requirements of the ECHR. (Gill, 2016). However, as Gill (2016) observed, this initial phase of development "was more about improving the management and control of the agencies than a triumph for democracy" (p. 5).

Another milestone in the development of surveillance accountability and the evolution of intelligence governance in the U.K., was the Regulation of Investigatory Powers Act 2000 [RIPA 2000] which replaced the 1985 Interception Act. RIPA 2000 enhanced the role played

by the commissioners in the oversight process by introducing two reformed institutions: The Interception of Communications Commissioner with the role of scrutinising the warrants issued by the Secretary of State and the Intelligence Services Commissioner (Scott, 2019). Statutory provision was made for the intelligence agencies to access 'communications data' (metadata), albeit without adequately distinguishing between metadata and content interception in a way corresponding to the contemporary technological environment (Leigh, 2019). Hence, given the weaker safeguards applied and the broader necessary grounds for collecting metadata, this definitional ambiguity allowed for collection of considerable amounts of personal information.

An important aspect worth highlighting here is the historical delay in the emergence of intelligence democratic accountability in the UK, when compared to other Western democracies. According to Gill (2016), this delay was mainly due to the British political culture of the time, largely favouring a tradition of secrecy and with deep roots in governance. The strong culture of secrecy coupled with a feeble judicial branch in matters of national security and a press generally ignoring the theme of civil rights, were major factors explaining the tardy development of the British oversight system (Gill, 2016). Furthermore, until 1998 when the Human Rights Act [HRA] was passed, the rights set out in the ECHR were not incorporated into British law, so they were not enforceable in the UK courts.

A different account for the delay in the evolution of intelligence oversight in the UK, is offered by Davies (2010) who emphasized the distinctiveness of the British model. Intelligence accountability mechanisms have generally emerged and developed as a result of endogenous factors, as it happened in the cases of the U.S. and Canada where public scandals and revelations about intelligence wrongdoing, played a pivotal role. The establishment of parliamentary oversight structures in the post-communist states from Central and Eastern Europe was also a result of endogenous factors, namely, a determination to break with the totalitarian methods of the past. In the UK though, as Davies (2010) put it, "no comparable endogenous factors have historically been at work" (p. 134). The major developments in the British system of intelligence accountability derived, instead, from exogenous factors such as the UK's memberships of the ECHR and the EU, external crises like the Falklands War or cases of Soviet espionage (Davies, 2010).

Finally, another interpretation of the British development of intelligence accountability and its modus operandi was offered by Moran & Walker (2016) who stated that the UK approach "seems to rest on the ideology of 'gentlemanly critique', based on peer review by ex- or serving legal and security professionals" (p. 312). In the next section, we look at how the

post-Snowden crisis of legitimacy has spurred changes in the way the intelligence community in the UK attempts to rebuild its legitimacy, namely through communication strategies targeting the general public.

3.4 GCHQ after Snowden: communicating transparency

The crisis of public legitimacy generated by the Snowden leaks forced some intelligence agencies to react. In the UK, GCHQ stepped into the public arena through a communication strategy with a twofold purpose. Firstly, to convey a message of institutional transparency, and secondly, to reassert the expert authority of the agency in the security field. Lund Petersen (2019) identified three types of discourses on communication practices currently functioning in Western intelligence: awareness, advice, and co-production. According to Lund Petersen (2019), public communication is "a cognitive framework for conceptualising a new vision of the relation between the intelligence organization and its surroundings" (p. 325).

Awareness refers to communication as a way to foster public accountability and transparency, both prerequisites of any state bureaucracy in a democratic regime. In this rhetorical framing, the principles of openness and transparency take centre stage and present the public with explanations about the workings and value of intelligence work and threat assessments (Lund Petersen, 2019, p. 320). However, this communication practice reiterates a hierarchical understanding of knowledge, with experts at the top and the public on the other end. These practices can be seen in GCHQ communication towards the public after 2013. In contrast to the complete opacity of the agency prior to its officially acknowledgement with the Intelligence Services Act of 1994, today the agency has a dedicated role of Director for Strategy, Policy and Engagement and since 2016, its own Twitter account.

In 2016, the Home Office published the "Operational Case for Bulk Powers". This was a milestone document in terms of transparency as it was "the first time that UK intelligence agencies had explained their work in such detail" (GCHQ, 2021, p. 19). This was followed by the publishing of the "Report of Bulk Powers Review" in 2016 by David Anderson QC, a document which, apart from assessing the necessity of these collection practices, relates in detail how bulk powers are employed in real situations and the operational impact they produce. It should be mentioned that Anderson's report was criticised by some civil society actors for its approach and conclusions. However, the report "went further than ever before" (IPCO, 2018, p.1) by publicly presenting sixty detailed case studies of operational scenarios provided

by MI5, MI6 and GCHQ. The case studies show broad utilisation of bulk powers, including in counter-terrorism, support of military operations, cyber-defence, fighting child sexual exploitation, and counter-espionage. Such a degree of transparency was unconceivable in the previous decades, especially regarding the working of SIGINT technologies. In an op-ed published in the Financial Times in 2021 about the application of AI in intelligence work, GCHQ director Jeremy Fleming emphasized transparency as a driving principle of the agency, stating that "[…] GCHQ is changing as we adapt to deliver our mission to keep the country safe. We expect AI to be at the heart of this transformation and we want to be transparent about its use" (Financial Times, February 24, 2021). These instances all reflect the unprecedented transparency and openness in GCHQ's engagement with the public.

Another important moment in GCHQ's post-Snowden communication strategy was the organization of a public exhibition in 2019-2020. The exhibition was organized in partnership with the Science Museum in London under the name "Top Secret: From Ciphers to Cyber Security." The event was carefully prepared over two years to mark the centenary of the agency and was intended as the GCHQ's "most revealing moment" to date (Design Week, August 5, 2019). An exhibition is "a strategic system of representations" (Ferguson, 2005, p. 128) using all available elements of design, from architecture to colouring and labels, in order to convey a message. For example, in the contemporary section of the GCHQ exhibition, the designer tried to represent a sense of transparency by using acrylic casements for displaying objects. The emphasis on transparency was also reflected in the words of the agency's director, Jeremy Fleming. Speaking on this occasion, he declared that "it is no longer enough [for GCHQ] to serve entirely in secret" but that it must "justify the trust of the people [it] seeks to protect" (The Guardian, July 9, 2019). Similarly, placed towards the end of the exhibition was a GCHQ poster directly addressing the visitors with the message: "We're not as secret as you might think…". The exhibition can be understood to reflect GCHQ's opening towards the public post-Snowden, with transparency firmly at its core.

A more subtle, yet significant, purpose of the exhibition was to publicly reinforce GCHQ's expert authority in the field of national security. The museum was a public arena in which the exhibition could provide a context for the expression of power/knowledge (Foucault, 1980). Through this lens, one can understand exhibitions as hierarchical structures producing "particular and general forms of communication" (O'Neil, 2007, p. 14). During the exhibition, the curators used backlit displays with written text briefly describing to the public the predominance of technology in the agency's diverse activity and its crucial relevance for

security. Technologies like data mining, encryption and even quantum computing were also referenced in different displays. This emphasis on the technologically advanced nature of GCHQ's work was further accentuated through the choice of the Science Museum as a host for the event. The same framing can be noticed in the presentation of the exhibition on the GCHQ's website, stating that the event explores "a century's worth of intelligence through […] technological stories that underpin GCHQ's role at the heart of the nation's security" (GCHQ, July 9, 2019).

The exhibition can also be seen as part of a larger effort of the intelligence community in the UK to push for normalisation of contested practices, such as bulk data collection. In the exhibition, the controversy surrounding GCHQ surveillance practices was presented mainly as a trade-off between security and privacy, with titles such as "the balance between security and privacy" and "bulk data: a difficult balance". In light of this, the exhibition clearly reflected GCHQ's communication strategy, aimed at reinforcing the agency's expert authority in the security field while serving the larger goal of normalising contested security practices in the eyes of the public.

3.4.1 A move towards normative rhetoric and public engagement

Substantial advances in AI over the past several years have significantly increased the technology's importance for the field of national security. In 2017, a Harvard Kennedy School study predicted that AI would be a game-changer for the field of national security historically comparable with the impact of nuclear weapons, computers, aircraft, and biotech (Allen & Chan, 2017, p. 1). One major effect has been the transformation of intelligence services into Big Data organizations (Aradau & Blanke, 2015). Illustrating this point is the recent cloud contract signed between GCHQ and Amazon Web Services (AWS). The contract, which allows for the digital storing of classified information in Amazon's high-security cloud system, is intended to boost the analytical capabilities of British intelligence agencies (Financial Times, October 25, 2021). Another consequence is that the highly complex nature of these methods reduces the potential for transparency. In other words, the intrinsically opaque nature of algorithmic security practices encumbers accurate communication towards the public.

In February 2021, GCHQ published the report "Pioneering a New National Security: The Ethics of Artificial Intelligence", whose rationale it is to establish an ethical framework to guide the future use of AI in intelligence collection. This policy document can be seen as a

long-term effect of the Snowden disclosures and part of GCHQ's discourse of justification and rebuilding of public trust. The report was hailed for its novelty, on the one hand for its integration of ethical reflection into security practice and on the other hand for its general message around transparency and trust (Murray & Fussey, 2021). The text's discursive approach is evidenced by statements directly addressing the public, such as "[t]he paper is the first step of a much longer journey: we'd like you to join us on it" (GCHQ, 2021, p. 5). This communicative construction, centred on the idea of a "journey", indicates an attempt of the intelligence agency to frame public engagement as a remedy for security governance. In so doing, GCHQ has developed an alternative avenue through which to address major controversies, e.g., the bias associated with AI technologies.

As a dimension of AI-driven security governance, public engagement would involve achieving consensus among diverse publics with diverse and often contrasting societal visions. This was reflected in the opinion piece of the GCHQ director, published in Financial Times, where he made a plea for building a consensus on AI rules and norms by stating:

> "[t]he way in which AI is developed, implemented and exploited must show we are serious about ethics, inclusion and democratic values. Shaping this is as important as the amazing potential of the underlying science — if not more so" (February 24, 2021).

The advent of AI in national security, thus, raises important normative questions related to inclusion and equal representation, and the issue of which public groups are represented and which are left out of the engagement process becomes crucial. By extension, the representation of marginalised groups in shaping the way AI is developed can be seen as a democratic prerequisite for the full adoption of this technology by security and intelligence services.

3.5 The role of critically engaged scholarship in challenging the intelligence expert discourse

As shown, characteristic of the post-Snowden period was a shift towards more public communication from within the UK's intelligence community. For GCHQ, this has meant showing transparency by communicating about the agency's activity and operational methods on an unprecedented scale. There are also signs that GCHQ's public communication is shifting towards a more normative approach focused on issues like consensus and inclusion. However, as Lund Petersen (2019) observed, there is a need for a new public communication model in intelligence work that would allow for the possibility of resistance and criticism as a way to

address “the power-knowledge relation implied in the communication of expert knowledge” (p. 325). According to Michel Foucault’s schema of power-knowledge, power produces knowledge and knowledge produces “effects of truth” which “in their turn reproduce power” (Foucault, 1980, p. 93).

Establishing democratic intelligence governance therefore becomes unattainable in the absence of the possibility of resistance and critique vis-à-vis the intelligence expert discourse. That is, diversity in the modes of knowledge and expertise in the formulation of security policies is essential for avoiding groupthink and thus for improving intelligence practices in accordance with the democratic ethos.

This chapter argues that critically engaged academic scholarship can fill this need for epistemic diversity in the field of intelligence policy. Epistemic diversity “often produces *dissent* on the theories or the strategies worth pursuing” and dissent produces “worthwhile criticism” (Solomon, 2006, p. 23). For example, in the context of AI proliferation for intelligence and national security, critically engaged scholars working in social sciences and data sciences can articulate strong critiques and even challenge the epistemic credibility of the intelligence expert discourse. Such an effort can also offer civil society a much stronger basis for resistance and critique whenever it is the case. Some authors even state that the defining condition of security scholars encompasses a democratic responsibility to “act as theorist-citizens in the public and civil sphere” (Ish-Shalom, 2015, p. 241).

The new algorithmic technologies deployed by intelligence agencies are highly complex, making it difficult to ensure accountability within the field. Nonetheless, academia is well positioned to play a leading role in addressing such gaps, including as they regard controversial subjects such as the use of Big Data and machine learning. For example, Aradau and Blanke (2015) demonstrated the potential of a collaborative approach between social and computer science to challenge the credibility of intelligence experts and the discourse of justification put forth by intelligence organisations. In relation to contested issues, like bulk surveillance and algorithmic security, their work shows academia’s capacity for providing robust critiques against the official discourse. Critical approaches such as this are rooted in the post-structuralist paradigm which “sees itself carrying out a form of oversight of power at the level of discourse” (Phythian, 2008, p. 64). By encouraging a more critical understanding of opaque technologies and challenging the monopolised expert discourse of intelligence professionals, their intervention offers an expanded framework for the democratic governance

of intelligence. By extension, this fashions a way forward for critique from both academia and civil society.

Understood as part of the democratic repertoire of intelligence governance, academics' public engagement should be routed through specific public platforms where their normative critiques of controversial intelligence practices can be turned into political claims. Within this analytical framework, the emergence of public issues is conditioned by the material existence of public platforms. In other words, "the material arrangements of public engagement matter to the ways in which political claims can be articulated, enacted, or denied" (Gros et al., 2017, p. 77). A relevant example of such a platform is the International Intelligence Oversight Forum (IIOF) inaugurated in 2016. Organised under the auspices of the UN Special Rapporteur on the right to privacy, IIOF is an important platform for expert debates on aspects of security and surveillance involving challenges to human rights and identifying better safeguards. The forum is attended by a diverse range of stakeholders, including government officials, intelligence officials, members of national intelligence oversight bodies, NGOs, and academics. Although closed to the public eye, the expert platform of IIOF has offered the opportunity for some academic security experts to interact directly with intelligence and security practitioners on various topics.

From the angle of practice theory, academia's engagements with security practitioners can be seen as a form of participant observation. According to Bueger & Mireanu (2015), "what should define security scholarship is a well-negotiated *proximity* to practice" (p. 118). They endorse an instrumental understanding of academic research as social practice. In other words, security scholarship should concentrate on addressing problems at the societal level and employ pragmatism in solving them rather than just pursuing a purely normative critique. In this sense, a platform like IIOF provides not only an excellent opportunity for academic security experts to engage with practitioners of security, but also an opportunity for them to articulate their critiques outside their academic community. Here it is also worth mentioning the collaboration of the UK's intelligence oversight expert body (IPCO) with the University of Essex, which has resulted in workshops and debates on best practices in the oversight of digital surveillance and surveillance technologies. IPCO later acknowledged the impact of these workshops in improving their own understanding of certain public fears about the use of bulk surveillance powers, such as metadata collection (IPCO, 2020, p. 24). This is yet another example of how academic expertise can be employed in an instrumental manner, specifically towards the improvement of intelligence governance.

Another dimension of critical scholarship is the capacity for challenging the speech acts of securitization articulated by security agencies and practitioners. Since security as an academic discipline has been fundamentally linked to policy relevance since its inception, the normative issue of responsibility has been a core topic for debate within the field. As Wæver (2015) observed, both the European and American variants of this debate have evidenced "the centrality of social-scientists-in-society in shaping sciences of security" (p. 100). In other words, security expertise has a constitutive practical dimension likely to produce political consequences and normative implications.

The proximity to the security sector, makes security scholars liable to potential co-optation, thus running the risk of assisting "the manipulative dynamics of securitization" (Ish-Shalom, 2015, p. 229). For example, the practices of bulk data collection deployed by the NSA and GCHQ, as exposed by the Snowden leaks, can be understood as part of the securitization of terrorism. Within the analytical framework of critical security, securitization is a negative process which should be fought against by security scholars, who should instead strive for desecuritization. However, there are also security scholars who do not consider all types of securitization necessarily negative. In developing a theory of just securitization, Floyd (2019) tried to addresses to security practitioners and scholars alike, with a set of criteria that can guide practitioners on what matters for the justice of securitization and scholars on evaluating the justice of securitizations.

Other scholars like Bigo (2012), asserted the possibility of democratizing securitization and security. Democratising security would involve an examination and contextualisation of how certain transnational groups of security professionals define and prioritize risks and how their conceptions of what constitutes threat become dominant on the national security agenda (Bigo, 2012, p. 278). Democratising securitisation would involve the improvement of public and civic debates on security in order to better consider the experiences and needs of common citizens and marginalised groups (Ish-Shalom, 2015). In both cases, the public role of academic security expertise is significant. We can find this credo clearly expressed in the words of intelligence studies scholar, Peter Gill (2010): "[…] whenever possible, we [academics] have an obligation to try to explain and elucidate complex matters in such a way that reason does not submit to security panics" (p. 54). Thus, security and intelligence scholars can fulfil a key role in the public sphere by countering or transforming the processes of securitization.

3.6 The future of intelligence governance in the context of AI proliferation

A fundamental aspect of intelligence governance in the post-Snowden context is understanding the modus operandi of the highly complex technologies of intelligence collection. The role of diverse multidisciplinary expertise will be even more important as AI is the principal direction of development in intelligence collection and analysis. As observed in a recent US Congressional Report on the use of AI for national security, AI technology "is expected to be particularly useful in intelligence due to the large data sets available for analysis" (Hoadley & Sayler, 2020, p. 10). In early 2021, GCHQ released "Pioneering a New National Security: The Ethics of Artificial Intelligence", a blueprint document addressed directly to British citizens which sketches major ethical considerations that will govern British intelligence agencies' use of AI. The document defines AI as "as a type of software that can learn to find complex patterns in data [and] can provide us with new insights or forecast future trends" (GCHQ, 2021, p. 9). This definition reflects what has become the "doxa" of intelligence agencies, i.e., a modus operandi centred on "knowledge discovery" and forecast through the mining of large sets of data and metadata (Aradau, 2015, p. 22). As a prerequisite to train algorithms to discover complex patterns, AI technology needs large volumes of data. Consequently, the deployment of AI technologies, such as machine learning as part of large-scale surveillance techniques, will require a vigilant system of oversight based on a diverse set of expertise and modes of knowledge. In other words, intelligence governance in the age of AI will need to include "a strong system of vernacular accountability […] with contributions from individuals from a diverse range of backgrounds, questioning everyday practice and policy assumptions" (Gaskarth, 2020, p. 120).

The full adoption of AI technologies in the field of national security will require a consistently updated legal framework. However, the anticipatory function of these algorithmic technologies challenges legal reasoning by inviting law on a speculative ground. While legal knowledge has a past orientation centred around legal evidence, the algorithmic technologies and security practices of "knowledge discovery", which are based on digital data, are oriented towards prevention of future threats (Aradau, 2017). This tension between law and security and the frailty of legal knowledge when confronted with the anticipatory character of these technologies negatively affects the entire edifice of intelligence governance.

Due to the proliferation of algorithmic techniques for security, legal knowledge must be complemented by a variety of modes of knowledge and perspectives to improve the governance of intelligence. A constant critical inquiry into the mechanisms and constitutive

elements of these technologies and techniques is the only way to keep pace with their rapid development and overcome the continued challenge of their opacity. By examining the "calculative modalities that inform their [algorithmic technologies] programming" (Amoore & Raley, 2017, p. 8), some critical studies argue that these new methods cannot remain impenetrable to scholarly inquiry. For example, the previously mentioned collaborative approach between social and computer sciences can offer substantial insights into these algorithmic security practices by using epistemic tools across disciplines (Aradau & Blanke, 2015). Furthermore, the emerging field of critical data studies provides research instruments for examining the impact of Big Data and algorithmic technologies on various societal aspects (Iliadis & Russo, 2016).

Other approaches emphasize the primacy of human rights law with the driving principles of necessity and proportionality as a basis from which to address the emergence of AI exploitation by intelligence agencies. For example, some scholars like Murray & Fussey (2021), have expressed concerns towards the GCHQ's AI report for prioritising a "vague ethical approach" (p. 1) over a less ambiguous human rights-based approach. Either of these scholarly frames deliver critiques which can improve intelligence policy, thus reflecting Gill's (2016), observation that "[e]stablishing democratic governance of intelligence is a constant process; it will never achieve the same reach as for other policy areas […]" (p. 213).

3.7 Conclusion

This chapter aimed to demonstrate the importance of epistemic diversity in expanding the democratic repertoire of intelligence governance. Critically engaged academic expertise can play a leading role in the democratization of intelligence expert discourse, thus enriching and strengthening the capability of civil society for resistance and critique of present and emerging intelligence policies and practices. Countering the monopoly of intelligence expert discourse in this way is a key dimension of improving security policy and establishing democratic intelligence governance. Technologies of bulk collection and AI-driven practices in the field of national security have a high degree of technical complexity, meaning that without proper expertise in civil society, they remain obscure to the public sphere. We arrived at this conclusion through a case study analysis of the way GCHQ has been communicating towards the public in the post-Snowden landscape.

By examining a series of communicative modes such as official reports, public messages from its leadership, and a museum exhibition, we traced a series of unprecedented

moves towards public engagement and a normative rhetoric centred on transparency. We argued that the rhetorical framing is part of a discourse which aims to (re)construct GCHQ's legitimate knowledge authority in the field of national security and technology.

CHAPTER 4 - UNDERSTANDING THE POTENTIAL OF EXPERT OVERSIGHT BODIES FOR INFORMING PUBLIC DEBATES ON CONTROVERSIAL SECURITY PRACTICES: THE CASE OF THE UK'S IPCO IN THE SOCIETAL DEBATE ON BULK SURVEILLANCE

4.1 Introduction

Intelligence oversight institutions are key actors in shaping the societal framing and public understanding of intelligence collection technologies in liberal democracies. This is because the rationale of an intelligence oversight mechanism is to protect citizens against misuse of these technologies and to facilitate informed public debate on ensuing societal issues. Having said that, an issue which has yet to be adequately addressed is the increased reliance of intelligence services on Big Data and bulk data collection.

While civil society organizations, academia, and intelligence and security actors, all contribute to and shape the public debate on technologies of bulk data collection, these actors are limited in their understanding of the matter by some uncontrollable factors. In the case of academia and civil society activists the lack of access to classified information may prevent a complete representation of existent security risks and operational contexts. Similarly, the bureaucratic character of intelligence and security institutions can make these actors less sensible to critical and civic perspectives.

Oversight expert bodies, on the other hand, are optimally placed to act as a liaison between the intelligence community and the community of citizens due to their access to classified information and direct working with intelligence agencies. This privileged position permits oversight institutions to initiate and play a key role in framing relevant public debates on important public issues, such as the use of bulk data collection for national security. Given their independent status, oversight bodies are thus "ideally placed

to provide credible and reliable information to educate the public about the activities and role of intelligence services" (FRA, 2017, p. 87).

This chapter, therefore, argues that oversight institutions are better equipped than all other societal stakeholders for informing and eventually and indirectly, shaping the current and future public debates on intelligence and security practices involving controversial technologies such as bulk collection and algorithmic surveillance. The high-level security clearance and reliance on experts on the one hand, and the ability to engage with civil society and citizens in an open manner on the other, are features that place independent oversight bodies in a pivotal position for shaping this societal debate.

The chapter employs a qualitative approach and will start with a literature review of theoretical approaches on how intelligence oversight can engage more with the public. Next, we will examine how this approach has been implemented in practice by focusing on the UK's main oversight bodies, the Investigatory Powers Commissioner's Office (IPCO) and the Intelligence and Security Committee of Parliament (ISC). Finally, we will analyse how the activities, discourse, and reports of these two oversight bodies have been reflected by civil society. In this way, we can get a sense of how the oversight has been shaping the public debate on bulk surveillance in the UK.

4.2 The elements of an intelligence oversight system

Intelligence oversight can be broadly interpreted as a function of controlling intelligence services both in democratic and non-democratic systems, albeit with different objectives. Intelligence oversight as a functional concept is an attribute of liberal democratic systems and formally emerged in the US in the 1970s as a result of the congressional investigations into the misconducts of the intelligence community. Used interchangeably with terms such as "accountability" and "review", intelligence oversight refers fundamentally to "mechanisms for scrutinizing the intelligence services, with the aim of ensuring their compliance with specific standards or guidelines, such as legal frameworks, executive directives, or international law" (Wegge, 2017, p. 688).[2]

[2] It is important to note that, for the sake of clarity, we decided to use 'oversight' as a general term with reference to all branches of power and institutions involved in the accountability of intelligence community, including internal compliance departments of intelligence agencies, external expert bodies and watchdogs.

In a democracy, therefore, intelligence oversight must fulfil a twofold role. One the one hand, it must oversee the quality and efficiency of the intelligence product, and on the other hand, try to guarantee that intelligence activities are conducted legally and in accordance with citizens' rights and liberties. Hence, another defining feature of intelligence oversight is this duality, referred to by Clift (2007) as the "coin of intelligence accountability." Nevertheless, the side of the coin which is of interest for our current research is the one about the propriety of the intelligence services, namely their conduct and compliance with legal and ethical norms required in a democracy (Caparini & Born, 2007). These dimensions are especially important, if not necessary, in order to have an open and comprehensive public debate on a sensitive topic such as the use of bulk surveillance. In other words, the activities and policies of intelligence agencies must be reviewed in terms of legality, proportionality and effectiveness. In this way, intelligence oversight is a vital element for both democratic mechanisms and national security as "[g]etting it [intelligence oversight] right is hard and getting it wrong is dangerous" (Zegart, 2011, p. 5).

4.2.1 Main actors and scope of control

According to the *Report of the Special Rapporteur Martin Scheinin*, "intelligence services are overseen by a combination of internal, executive, parliamentary, judicial and specialised oversight institutions whose mandates and powers are based on publicly available law" (United Nations Human Rights Council [UNHRC], 2010, as cited in FRA, 2017, p. 63). In addition, there are actors performing watchdog functions in democratic states, such as media, national human rights institutions, civil society organisations, ombuds institutions and whistle-blowers (FRA 2017). In this way, intelligence oversight is usually a function shared between all three branches of state power – executive, judicial and legislative – of which parliamentary oversight has been the most analysed and discussed (Krieger, 2009). However, while most democracies have a hybrid oversight system (e.g. the UK, France, the Netherlands), in which the intelligence oversight function is shared between several branches of power, some countries assign the intelligence oversight function exclusively to a single branch of power: executive oversight (e.g. Malta), legislative oversight (e.g. Romania), and judicial oversight (e.g. Ireland).

Executive actors exerting control on intelligence agencies include cabinet ministers (usually foreign and interior ministers) and the head of government. In the UK, for example, the Secretary of State is supported by teams of policy officials who have full access to

classified activities of the intelligence agencies. Executive control of intelligence agencies can be exerted in various manners: through appointments of the agencies' senior management, by setting up priorities, or authorising certain surveillance measures (FRA, 2017). Although in a strictly technical sense, internal control within the intelligence services and control by the executive do not qualify as components of an oversight mechanism, executive and internal actors play an important role in ensuring the accountability of intelligence activities.

Parliamentary or legislative oversight is perhaps the most widespread form of intelligence oversight, becoming a standard practice for democracies and thus carrying considerable symbolic weight. Parliaments usually oversee intelligence services via specialised or non-specialised parliamentary committees. As the legislative power, it is responsible for enacting intelligence legislation and approving intelligence agencies' budget. Additionally, parliamentary committees can play a key role in scrutinising intelligence operations and policies on the basis of their legality and compliance with fundamental rights.

Judges provide valuable independent oversight and judicial review is thus an essential component of an effective intelligence oversight system. More concretely, judicial participation in oversight of intelligence agencies is related to issuing of warrants and monitoring of surveillance measures (FRA, 2017). Judges are independent, sometimes specialised, and have the task of evaluating ex-ante requests from intelligence services for the use of surveillance. In some countries, such as Ireland, judges also do ex-post oversight. Their oversight role is therefore focused on the aspects of legality and fundamental rights protection. As a report issued by the Venice Commission states, "the value of judicial control depends upon the expertise the judges in question have in assessing risks to national security and in balancing these risks against infringements in human rights" (2007, para. 206, as cited in FRA, 2017, p. 94).

Independent expert bodies are valuable oversight actors, focusing primarily on aspects of legality and intelligence policies but also on fundamental rights protection. Their strong expertise and independent status are usually complemented by a high-level access to classified information. Prominent examples of independent expert bodies are, as mentioned, IPCO in the UK, Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) in the Netherlands, and Commission nationale de contrôle des techniques de renseignement (CNCTR) in France. Some of these independent expert

bodies have developed strategies and procedures of engagement with the civil society organisations, as we will return to in a later section.

Finally, watchdogs, e.g., civil society organisations, media, academia, and whistle-blowers, have an important role in ensuring the effectiveness of oversight. Watchdogs focus on policy aspects of intelligence and the protection of human rights (FRA, 2017). As illustrated in the drawing (see Figure 8), oversight entities are located between intelligence services and the public sphere, serving as a liaison between the intelligence community surrounded by secrecy, on the one hand, and the community of citizens in an open democratic society on the other.

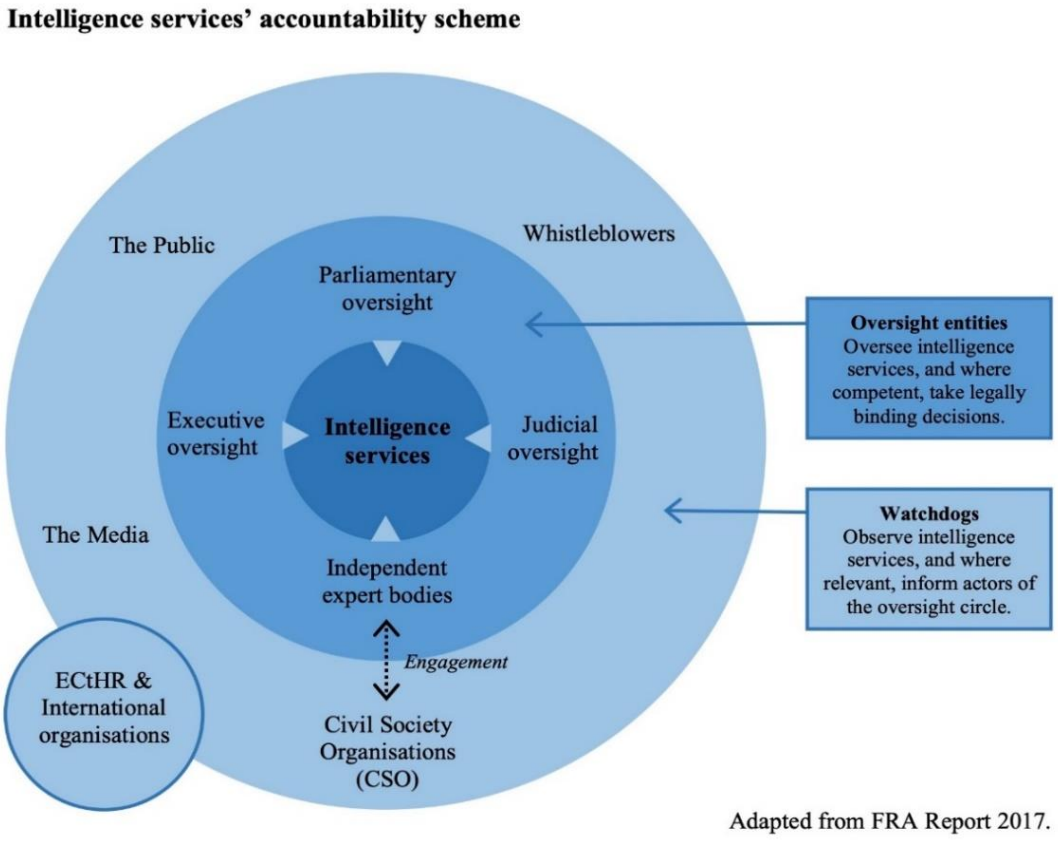

Figure 7 : Intelligence oversight actors (Adapted from FRA Report, 2017).

4.2.2 Stages of oversight: ex ante, ongoing and ex post

When oversight occurs before the surveillance measures are implemented, it is a case of *ex ante* authorisation or approval by an oversight body. Activating the control

mechanism prior to the implementation of surveillance in this way is an important safeguard against the misuse of bulk surveillance powers (Wetzling & Vieth, 2018). Moreover, *ex ante* oversight offers the possibility to review the necessity of surveillance operations requested by the intelligence authority in question. This form of oversight usually involves an independent body authorising the warrant or reviewing and approving a signed warrant before its entering into force. The latter model can be observed in the UK where intrusive surveillance warrants must be authorised first by the Secretary of State and then approved by an independent Judicial Commissioner as part of a "double-lock" approval process (Investigatory Powers Act [IPA], 2016).

Ongoing monitoring and *ex post* review are forms of oversight occurring at a later stage, either while the surveillance operations are being implemented or retroactively after the operation has ended, respectively. For example, IPCO has an *ex post* oversight function concerning the use of investigatory powers by intelligence agencies: after carrying out their audits, IPCO inspectors can share observations acquired during the review process with the Judicial Commissioners, especially when their findings are relevant to the warranty process (IPCO, 2018b).

By carrying out retrospective in-depth inspections of intelligence operations, in addition to the review of warrants mentioned earlier, IPCO is an oversight institution that performs both stages of oversight, ex ante and ex post. Combining these two responsibilities is considered very beneficial by IPCO authorities as it provides them with "a detailed level of insight into the factors relevant to applications for warrants and the use of covert powers which otherwise would not exist" (IPCO, 2018b, p. 10). Conversely, some scholars and think-tanks endorse a clear institutional separation between the two functions, arguing that the dual role of IPCO is a "basic error" which predisposes it to "conflicts of interest" (Gill, 2020, pp. 9-10; RUSI 2015). In the UN Special Rapporteur on the right to Privacy's *Legal Instrument on Government-led Surveillance and Privacy*, Cannataci (2018b) lists an independent pre-authorisation authority (*ex-ante* oversight) and an independent operational oversight authority (*ex-post* oversight) as essential components of a system of checks and balances for government-led surveillance.

4.3 Intelligence oversight and public engagement

The Snowden disclosures in 2013 have exposed significant limitations in the existing oversight systems in some major Western democracies and confronted them with a diversity of new challenges generated by the rapid technological developments. The impact of the revelations is also reflected in scholarship, namely in the way intelligence oversight is being reconceptualized as part of a broader framework of democratic intelligence governance. The use of *governance* as a research framework has translated into more focus on improving and drafting new modes of oversight, especially as it concerns bulk surveillance (*see* Bradford Franklin & King, 2018; Goldman & Rascoff, 2016; Omand & Phythian, 2018; Vieth & Wetzling, 2019). In light of this, an important avenue of research has been the exploration of various strategies for increasing engagement between oversight institutions and the public on matters of intelligence policy. Through engaging with the public, oversight institutions can better represent and protect citizens' interests and values and can play a crucial role in building public trust and confidence in intelligence agencies. To illustrate this, Goldman and Rascoff (2016) make a case for expert bodies, such as the Privacy and Civil Liberties Oversight Board (PCLOB) in the US, to acknowledge and strengthen their roles as proxies for the American people in the governance of intelligence. Worth mentioning here is the PCLOB's capitalization on public input as part of their review process of the surveillance program based on Section 702.[3] More specifically, the Board organised public hearings with participants from a variety of fields, including privacy advocacy and academia, and temporarily introduced an online public comment section (Renan, 2016). The outcome of the PCLOB's review was a public report, published in 2014, offering recommendations for the adjustment of the surveillance program, making it a valuable resource for policymakers. In this way, the PCLOB has been framing the policy debate on bulk surveillance in the Congress. In the words of Zachary Goldman:

[3] Section 702 of the Foreign Intelligence Surveillance Act was enacted in 2008 for legalising the Bush administration's warrantless wiretapping program and has been hailed ever since by the Executive and the intelligence community as a crucial counterterrorism tool. Section 702 is directed towards targeted collection of communications belonging exclusively to non-US persons believed to be located outside the US. It forbids surveillance of American persons, including the use of foreign targets as a vehicle for gathering intelligence about Americans. However, a backdoor search loophole allows the National Security Agency to collect without a warrant, communications belonging to US citizens as part of the collection process targeting foreigners and their communications with U.S. citizens.

> "[i]n an era of unprecedented threat and unprecedented transparency, institutions of governance must be able to mediate between the I[ntelligence]C[ommunity] and the people in order to ensure that intelligence activities in this [the US], and in all Western democracies, remain effective, legitimate, and sustainable" (Goldman & Rascoff, 2016, p. 208).

A convincing case for increasing the public engagement in the oversight process was made by Bradford Franklin and King (2018). They argue that the engagement between civil society organisations and oversight bodies can be an effective mechanism for limiting the risks posed by certain practices of intelligence collection to civil rights and liberties. They observe that engagement between oversight bodies and civil society entities largely concerns the oversight bodies' "policy or governance roles" (Bradford Franklin & King, 2018, p. 7), and, after examining the relationship between civil society organisations and bodies conducting oversight of surveillance in eight different democracies, identified several distinct models of engagement.

An important model of engagement outlined by Bradford Franklin and King (2018) is "cooperation toward a shared goal." This refers to the mobilisation of resources and expertise offered by civil society organisations in order to strengthen oversight or improve legislation with new safeguards. Particularly important is their technological expertise as it can offer valuable insights into current digital intelligence practices, including the modus operandi of bulk collection technologies and algorithmic practices.

Another model of engagement is "promoting better understanding between civil society and oversight" via public forums and meetings under Chatham House rule (Bradford Franklin & King, 2018, p. 13). While public forums can help educate the public at large on aspects of intelligence activity, meetings under Chatham House rule between representatives from the governmental sector and civil society can help deepen trust and foster dialogue (Bradford Franklin & King, 2018).

Concerning the potential obstacle posed by the secrecy restrictions that govern a large part of oversight activities, Bradford Franklin, a former Executive Director of the PCLOB, argues that these restrictions make the regular consultation with civil society groups even more valuable for both parties. Specifically, "it helps oversight bodies to not only diversify their views, but also to identify and address civil liberty risks, and it allows non-government actors to better understand declassified documents and have their voices heard" (Bradford Franklin, 2020, para. 1). A relevant example for both models of

engagement described above is IPCO. The British independent oversight body organises periodic consultations with civil society organisations on various aspects of intelligence accountability. One of these public consultations, for example, was focused on the issue of proportionality standards for the review of bulk powers. This illustrates IPCO's model of engagement with civil society for outside assistance and input, described by Wetzling and Vieth (2018) as "open oversight" (p. 94).

The post-Snowden trend of rethinking intelligence oversight as a more public and participatory process is also captured in David Omand's "social compact model" of security and intelligence work. Largely modelled on the British experience after 2013 and conceptually framed as a social contract, the model is based on:

> "an ideal of a democratic licence to operate being given, after open debate, to the security and intelligence authorities […] that defines their lawful purposes, regulates their intrusive methods, provides for independent oversight by judicial commissioners and by a committee of senior parliamentarians, and establishes a specialist court (the Investigatory Powers Tribunal) to investigate and adjudicate on allegations of abuse" (Omand & Phythian, 2018, pp. 50-51).

In other words, intensifying public dialogue and open debate as to why secret intelligence activities are important for a democratic society would eventually persuade the public and their parliamentary representatives into accepting the ratification of such investigatory powers. Under the social compact model then, intelligence operations are being "tolerated" on the condition of the three Rs: rule of law, regulation, and restraint (Omand & Phythian, 2018, p. 51). Omand and Phythian's (2018) conceptualization focuses on the ethical risks of intelligence collection, drawing on Just War theory and its conceptual apparatus, an analogy first introduced in intelligence studies by the British military thinker Michael Quinlan (2007). The classic concepts of *jus ad bellum* (right to resort to war) and *jus in bello* (right conduct in war) are applied in an analogous manner to the field of intelligence collection under the newly coined expressions *jus ad intelligentiam* and *jus in intelligentia* (Quinlan, 2007).

Jus ad intelligentiam can be found in laws, publicly available codes of practices and other documents justifying secret intelligence activity, all of which are debated and ratified democratically (Omand & Phythian, 2018). Through the means of ratified statutes and codes, the range of purposes considered legitimate for intelligence agencies is limited. In other words, *jus ad intelligentiam* represents the social contract between the legislative and

the executive branch, the latter of which includes the intelligence community itself. The contract determines the role which should be assigned to intelligence within a democracy, "a subject that can sensibly be debated publicly at a suitably general level of principle" (Omand & Phythian, 2018, p. 99) prior to its application.

Jus in intelligentia refers to the translation into action of existing statutes and ethical standards through classified orders and internal rules and authorisations. *Jus in intelligentia* concerns all the routine intelligence activities and decisions conducted under the veil of secrecy, subject to scrutiny through internal and external oversight and "hopefully […] consistent with a set of ethical principles" (Omand & Phythian, 2018, p. 100). Therefore, the open public debate and the input of the public on the role that secret intelligence activity should play in a democracy is possible in the initial phase of the making of such a social contract (*jus ad intelligentiam*). The appropriateness of intelligence agencies' behaviour under conditions of secrecy (*jus in intelligentia*), namely compliance and adherence to certain ethical standards, is reviewed ex post by oversight bodies that should protect the interests of the public. In other words, oversight bodies, such as IPCO, can serve as proxies for citizens by "reflecting their views and their values in an arena in which secrecy poses an obstacle to utilizing the normal mechanisms of obtaining popular assent" (Goldman & Rascoff, 2016, p. 220). As mentioned previously, the UK is one of few states in which there has been a public debate concerning the use of mass surveillance for national security purposes. In the next section, we explore the UK case in more detail.

4.4 How oversight institutions have been framing the societal debate on bulk surveillance in the UK

A major effect of the 2013 Snowden disclosures in the UK was to expose the existence of a gap between an outdated statutory scheme for surveillance, and the novelty of technological capabilities employed by intelligence agencies. In other words, existing legislation could no longer provide an adequate regulatory framework of surveillance in light of dramatic technological changes. The uncovering of this gap through the Snowden leaks has generated a series of policy debates between different social forces engaged in the process of shaping the new legal framework of surveillance policy. Within this analytical framework which focuses on the 'politics of policy-making', surveillance policy

can be seen as "a site of struggle between different social forces" (Hintz & Dencik, 2016, pp. 1-2), and the resulting legislation, as a direct effect of this complex dynamics.

The process of defining a post-Snowden surveillance policy in the UK has involved a variety of actors, such as oversight institutions, civil society organisations, media outlets, parliamentarians, national security institutions, and private companies. In particular, the comprehensive review carried out by the Independent Reviewer of Terrorism Legislation (IRTL) and the Intelligence and Security Committee of Parliament (ISC), had a key role in shaping the policy debate that eventually led to the adoption of the IPA of 2016. The IRTL at the time, David Anderson QC, was commissioned by the Executive to review the activities of the UK intelligence agencies on an ad hoc basis and with the highest level of security clearance.

Anderson's first report, *A Question of Trust: report of the investigatory powers review* (2015), became a blueprint for the IPA of 2016. Equally impactful was the report compiled by the ISC, *Privacy and Security: A modern and transparent legal framework* (2015), offered for the first time in a consolidated form, a review of all intrusive capabilities available to the British intelligence community. As such, it can be seen as "a landmark in terms of openness and transparency surrounding the agencies' work." (ISC, 12 March 2015.). As Hintz and Dencik (2016) observed, these reports "provided a strong normative framework (and limitation) for the government's intended expansion of surveillance powers" (p. 7).

A further report published by Anderson in 2016, *Report of the Bulk Powers Review,* assessed the operational case for the different bulk collection powers available to the British intelligence agencies. Through these public reports, the IRTL has also facilitated the framing of the public debate on bulk collection. However, our main focus is the two independent oversight bodies in the UK, IPCO and the ISC, and how they have been shaping this debate. We look next at instances when these two oversight bodies have engaged with civil society actors and how their reports have been reflected in the UK news media.

4.4.1 Direct engagement with civil society actors

Engagement with civil society was listed by the first Investigatory Powers Commissioner, Lord Justice Fulford, as one of the guiding principles underpinning the

work of IPCO (IPCO, 2017). The rationale behind this engagement policy has multiple dimensions. A key dimension, as stated by IPCO itself, is to enhance public confidence in the use of investigatory powers. Other dimensions of the engagement process are to explain IPCO's role to all stakeholders, including NGOs and academia, and to consult and seek their views on relevant aspects of intelligence activities.

An examination of the two IPCO Annual Reports published to date (for 2017 and 2018 respectively) reveals a consistent collaboration of the expert oversight body with academics and NGOs working in the field of human rights. For example, in 2018 IPCO was involved in a project at the University of Essex called the *Human Rights, Big Data and Technology Project.* As part of the project, it contributed to debates and workshops about best practices in the oversight of new surveillance methods (IPCO, 2018b). As the Report states, these workshops "enhanced IPCO's understanding of some of the public concerns about intrusive powers, including bulk collection of communications data […]" (IPCO, 2018b, p. 24). Another instance of civil society engagement is the involvement of prominent representatives from key NGOs in the induction and training programme for the Judicial Commissioners (IPCO, 2017). Moreover, the Investigatory Powers Commissioner liaised with NGOs on matters related to the use of bulk powers and organised meetings with representatives from Privacy International (PI), among others (IPCO, 2018b).

Although the lack of security clearance at times restricts the possibility of fully informing civil society representatives on intelligence operations and capabilities, IPCO's purpose, as stated by its former head, Adrian Fulford, is "to act as a bridge" (IPCO, 2017, p. 11). Engaging with civil society directly, as it is the case with IPCO, thus opens the possibility of influencing the public debate on bulk surveillance in a more pivotal manner. Given that civil society actors are liaising with the general public, making them part of the oversight process and integrating their input increases IPCO's influence and messages at a societal level. At the same time, the privileged position of having access to classified information offers IPCO a principal role when compared with the other stakeholders shaping the societal debate on bulk surveillance. Given their access to classified information and ability to review secret documents, reports published by these oversight bodies constitute a valuable resource for NGOs in the field and an important way to understand more about the use of surveillance technologies.

4.4.2 Shaping the public debate on bulk surveillance through publishing reports

Oversight institutions also shape the public debate by publishing reports of activity or specific programs. These are then covered and disseminated through media and NGOs, although sometimes in a critical manner. In this sense, analysing how NGOs and the media relate the findings of these reports and the following discourse is key for understanding how oversight bodies shape the public debate on bulk surveillance.

A good example of an influential report is the *Report on the draft Investigatory Powers Bill* issued by ISC in February 2016. The report was well received by the civil society and its demands for more privacy protection and transparency regarding the use of bulk powers were propagated in the public space by prominent NGOs in the field. Gus Hosein, Executive Director of PI, stated in a press release that the ISC's report "is clear on the requirement of a root and branch reconsideration of the legislation, pushing privacy to the forefront" (Lomas, 2016, para. 5). Hosein also emphasized the strong legitimacy of the report given the ISC's privileged position and access to secret documents. Another civil society organisation, the Open Rights Group (ORG), also praised the report, with its executive director, Jim Killock, declaring that the ISC "should be given credit for highlighting the Bill's failure to consistently apply privacy protections" (ORG, 2016, para. 3). Furthermore, the report was hailed by actors from the tech sector in the UK. As the deputy CEO of TechUK put it, the ISC report "makes it clear that the bill lacks clarity on fundamental issues, such as core definitions of key terms, encryption and equipment interference" (Holden, 2016, para. 12).

Another example of the impact of publications issued by oversight bodies was the reports of inspections carried out by IPCO in 2019 regarding the inadequate manner in which MI5 stored and mishandled data obtained under warrants. These reports became public, albeit in redacted form, because of a judicial review brought against the new IPA by the UK human rights organisation Liberty and other privacy campaigners. The inspection reports and other documents, such as correspondence between IPCO and MI5, reveal important observations concerning privacy safeguards raised by IPCO at the time. In one of these documents, Commissioner Fulford characterised the MI5's handling and storage of collected data as being managed in an "undoubted unlawful manner" (Bond,

2019, para. 6). The disapproval of MI5's approach to data handling is also present in IPCO's Annual Report from 2018, which states that:

> "[t]here were serious deficiencies in the way the relevant environment implemented important IPA safeguards, particularly the requirements that MI5 must limit to the minimum necessary the extent to which warranted data is copied and disclosed, and that warranted data must be destroyed as soon as there are no longer any relevant grounds for retaining it" (IPCO, 2018b, p. 42).

Thus, we can argue that IPCO's inspection reports and the Commissioner's declarations regarding MI5's lack of compliance has influenced the debate on bulk surveillance powers by raising concerns about the effectiveness of existing safeguards. In light of these disclosures, Liberty and PI have initiated joint international legal action against MI5 (Liberty, 2019), illustrating IPCO's contribution to civil society's efforts to ensure accountability of intelligence agencies.

Oversight bodies' findings and reports regarding intelligence activity normally reach the general public through the media. The informed views of oversight authorities, which are based on expertise and access to classified information, are conveyed to citizens through the media in a less technical language. Consequently, the manner in which media frame the information and findings delivered by oversight reports on the issue of bulk surveillance influence the way and extent to which oversight institutions shape the public debate on this issue.

4.5 IPCO as a model for informing the public debate on controversial security practices

The efficient oversight of bulk and algorithmic intelligence collection practices in the post-Snowden landscape can be seen as a key test for contemporary democracies. Bulk collection technologies are raising serious difficulties to legislative and judicial oversight authorities who often lack technical and operational expertise, resources and access to relevant information. The Snowden case has acted as a major catalyst for rethinking the role and design of intelligence oversight across the liberal democratic world towards more public engagement.

With parliamentary oversight displaying clear limits and legal compliance deemed insufficient to cover the complexities of the new digital intelligence practices, a novel category of external independent oversight bodies has emerged in recent years. These external entities have been described under different names, as 'expert bodies' (FRA 2015; 2017), 'institutions of governance' (Goldman & Rascoff, 2016) or 'hybrid institutions' (Scott, 2019). As the FRA Report (2015) states, "[e]xpert oversight is exceptionally valuable as it allows for the actions of the intelligence services to be scrutinised by those familiar with the subject, who have time to dedicate to the matter, and are independent of political allegiances" (p. 41).

The main point that we would like to emphasize here is that these independent expert bodies combine specific features that place them in an optimal position for shaping the societal debate on bulk surveillance. These core features are: reliance on experts -especially technological experts-, high level security clearances, openness towards collaboration with civil society and independence from executive. This set of characteristics allows them to shape the public discourse and dialogue on important controversial matters like bulk surveillance. While these bodies are neither judicial, nor legislative or executive, they are 'hybrid' in that they 'marry' some of the features typical of political institutions with features typical of legal institutions (Scott, 2019).

The UK sets an example of how to effectively develop intelligence governance in the context of Big Data proliferation. The IPA 2016 was the outcome of a series of public policy debates sparked by the Snowden disclosures, trying to address major deficiencies in the accountability of intelligence and surveillance in the U.K. The act marks the transition towards a new phase of 'expert oversight' (Leigh, 2019) through the establishment of IPCO. The new oversight body described by Anderson (2018) as a "larger, more powerful and outward-facing regulator", introduced the consolidated position of Investigatory Powers Commissioner [IPC] assisted by a number of Judicial Commissioners. IPCO took over all the prerogatives and responsibilities of three precursor organisations: The Office of Surveillance Commissioners, the Interception of Communications Commissioner's Office and the Intelligence Service Commissioner's Office. In this sense, IPCO not only that operates a broader range of functions than its precursors, but also does so in a post-Snowden societal context defined by widespread public awareness of the national security activities carried out by the executive (Scott, 2019). Furthermore, as Leigh (2019) observed, "instead of being a responsive institution that either reports or is tasked the IPC

has own-initiative powers to conduct thematic reviews of capabilities and to investigate serious errors" (p. 576).

The game-changing shift brought by the IPA 2016 is the prior approval function of the Judicial Commissioners, applicable to surveillance warrants authorised by the cabinet ministers. Within this approval system known as the 'double-lock' (see Figure 9), the Judicial Commissioners assisted by a Technology Advisory Panel, review all warrants for targeted surveillance and bulk powers on the basis of their compliance with the principles of necessity and proportionality. As an IPCO document states, "the purpose of the so-called *double lock* provisions of the Act are to provide an independent, judicial, safeguard as to the legality of warrants, in particular to their necessity and proportionality" (IPCO, 2018a, S. 19).

From a historical point of view, the introduction of the 'double-lock' put an end to a centuries-old practice under which cabinet ministers were the sole authority granting warrants for interception (Leigh, 2019). From an institutional perspective, an important consequence of the 'double-lock' scheme is the allocation to Judicial Commissioners of a prerogative (granting warrants) that has traditionally been monopolised by the executive power (Scott, 2019). Moreover, under the new law, a Judicial Commissioner "may carry out such investigations, inspections and audits as the Commissioner considers appropriate for the purposes of the Commissioner's functions." (IPA 2016, S. 235). This provision reflects the high degree of access to classified information that Commissioners are granted with.

The 'double-lock' mechanism is underpinned by a significant expertise component, in the sense that all Judicial Commissioners are appointed only if they hold or have held a high judicial office (IPA 2016, S. 227). The judicial "double-lock", can therefore be seen as a strong safeguard against the use of the most intrusive techniques including bulk interception and bulk hacking. By requiring that warrants must be reviewed by a Judicial Commissioner before they enter into force, the "double-lock" system establishes IPCO as an ex ante mechanism of intelligence oversight. This component of judicial review has been commended by the UN Special Rapporteur on the right to Privacy who described it as "one of the most significant new safeguards introduced by the IPA" (Cannataci, 2018a, para. 9).

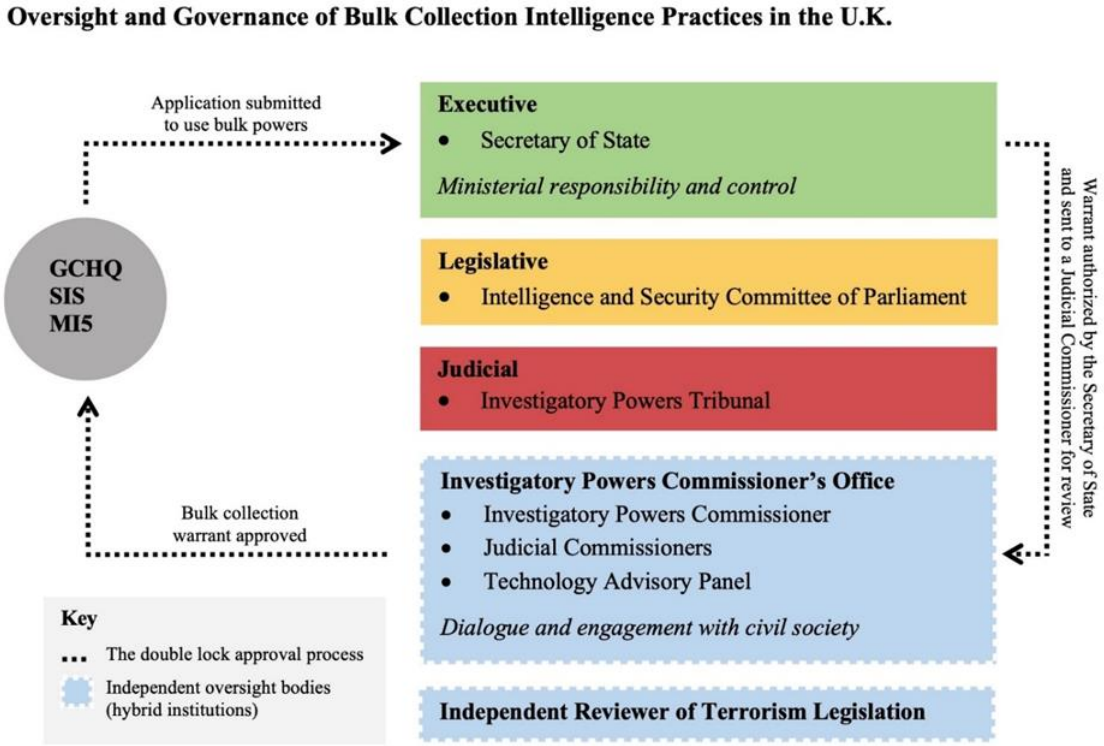

Figure 8 : The 'double-lock' approval process

Besides IPCO in the UK, other examples of expert oversight include CTVID in the Netherlands and CNCTR in France. It is important to highlight that both CTVID and CNCTR have an enhanced form of access to classified information via technical oversight interfaces that offer them direct digital access to intelligence databases. A technical interface with access to collected data opens the possibility of random oversight inspections and reviews at any time and generates more incentives for intelligence agencies to comply with the regulations (Wetzling & Vieth, 2018).

4.6 Conclusion

This chapter has demonstrated that a key stakeholder in the process of shaping the societal debate on bulk surveillance in a democracy is represented by intelligence oversight institutions themselves. It focused on the public dimension of oversight and their various strategies of engagement with civil society actors. We argued that independent expert oversight bodies are better equipped than all other societal actors for shaping the public debate on bulk surveillance. While societal actors like media outlets, civil society organizations, politicians, national security institutions and judicial courts all contribute

and shape the public understanding of this complex issue, they still have obvious limitations.

Media and civil society organizations can benefit from expert views and have a strong voice in the public arena but they lack access to classified information and, thus, to a comprehensive understanding of the matter. Although some politicians as members of parliamentary oversight committees have special security clearances, they usually demonstrate a lack of knowledge in technological aspects of intelligence collection nonetheless. Moreover, a laborious activity restricted by the rule of secrecy becomes less attractive for MPs and their electoral logic. Judicial courts have other limitations in this sense, mainly related to the exceptional character of the national security field but also because of the legislation lagging behind the new technology of surveillance.

The chapter's main argument is that external independent oversight bodies such as IPCO in the UK can play a pivotal role in the societal debate on bulk collection given their unique blend of institutional features and statutory power. The high-level access to classified information and reliance on experts on the one hand, and the ability to engage with civil society and citizens in an open manner on the other, are features which allow this independent expert oversight body to shape the societal debate on bulk surveillance and contribute to democratic governance of intelligence.

CHAPTER 5 – MAPPING THE DISCURSIVE LANDSCAPE OF THE DEBATE ON BULK SURVEILLANCE IN THE UK

5.1 Data Sampling

The assembly of the data corpus was guided by the attempt to answer the research question of our study and was conducted through a gradual strategy of sampling. First, we assembled a database of empirical material in textual format addressing the topic of bulk collection after 2013 in the UK by various social actors from various fields such as litigation, civil society, governmental. From this larger corpus of data fitting the discursive field surrounding the issue of bulk collection, we selected further data for fine analysis, a search process that is "open and criteria-driven" (Keller 2013, p. 100). Thus, for our research we adopted the methodology of *theoretical sampling* (Glaser & Strauss, 1999) that involves an iterative data collection process constantly adaptive in order to fit the emerging theory.

In qualitative research, "sampling decisions determine substantially what becomes empirical material in the form of text, and what is taken from available texts concretely and how it is used" (Flick, 2009, p. 125). In light of this step-by-step method of data collection, our sampling decisions start at the level of societal stakeholders involved in the debate on bulk collection. These actors fulfil the role of speakers in discourses and were selected based on their potential of providing insights into the discursive constitution of bulk collection in the UK. Thus, we chose to start the data sampling primarily according to these social actors that we identified to be relevant: civil society organizations, academia, intelligence agencies, intelligence oversight bodies and international bodies and courts. At the level of discourse, the resources available for "articulation and the production of resonance" (Keller, 2013, p. 71) are unequally distributed and vary greatly among the social

actors identified. This dimension is also reflected by the different formats of the empirical material available for compilation i.e. from laws to academic articles and petitions.

The selected texts (see Appendices) can, hence, be seen as "discourse fragments" (Jäger and Maier, 2009), and for our research they represent the main selection of data for fine analysis. The compilation of data consisted of documents issued in the UK or addressing a case from the UK in a time interval spanning from 2013 to 2021. The main criterium was the identification of the key texts/passages in the discursive engagements with the issue of bulk surveillance of each relevant actor. In other words, *we selected the texts based on their potential to assist us in the reconstruction of a certain discourse structure*. Thus, relevant to our research is a sampling strategy which aims at those texts that promise "the greatest insights" (Flick, 2009). We next assess these documents from a discourse relevance perspective and decide if they perform the same or rather a competing discourse. In some of these documents, more than one discourse is represented.

A further strategy we apply for the selection of documents to be analysed and the structuring of data assembly is the *maximal contrasting method* (Strauss & Corbin, 1998). The application of maximal contrast principle allows a charting of the whole "spectrum of the discourse(s) within a corpus" (Keller, 2013, p. 100). In other words, we start the data collection process by searching for the most dissimilar data in order to map the outlines of the whole discursive structure on the issue of bulk collection in the UK.

In our study, the case for justifying bulk powers as it was made by the intelligence community and the Home Office in the document "Operational Case for Bulk Powers" is contrasting with the view from the civil society (Don't Spy on Us coalition of NGOs) according to which bulk powers are fundamentally incompatible with democracy and human rights and equal mass surveillance. Hence, in documents issued by NGOs such as Privacy International and Liberty, bulk powers are always associated with negative metaphors such as Orwellian or Big Brother. According to this civil society coalition, the Investigatory Powers Act which normalizes the use of bulk powers, is "the most extreme surveillance law in our history". Thus, at one end we identified a master narrative operating with a specialist language and which encompasses a series of other sub-narratives like the necessary balance between security-privacy, while at the other end we found a critical master narrative that contests any form of untargeted surveillance. In-between these two discursive positions we researched the whole discursive spectrum and found a set of documents indicative of more nuanced discursive positions centred around human rights and technology.

Further selection criteria were applied for data sampling for the following actors as follows:

a) academia: We selected all academic works (articles and books) dealing with bulk surveillance in the UK, and which have a critical component / take a stance vis-à-vis this issue. Hence, we did not consider descriptive-only scholarly pieces in this selection.

b) ECtHR: between 2013-2021 we found two major cases dealing specifically with the UK bulk surveillance regime. These are Big Brother Watch and Others v. the United Kingdom (2018) and Privacy International and Others v. the United Kingdom (2016). For mapping the ECtHR discourse, we used the judgment/decision sections from these documents. However, for the coding process we separated the parties' submissions sections from these documents and considered them as standalone documents as the case may be, either for the mapping of the Civil Society discourse or for the Executive/SIS discourse.

5.1.1 Key documents for in-depth discourse analysis

At the end of data sampling phase, we counted a total of 30 documents (See Appendices 1-5) selected for the coding process. We only coded the relevant sections from these documents, related to bulk surveillance and expressing an opinion on the issue. Thus, apart from Parties' submissions in the Court documents, we looked specifically at the Findings of the IPCO Reports, Written evidence from the Parliament in the ISC's Reports and Assessment and Recommendations from the Independent Reviewer of Terrorism Legislation. As we already mentioned, some documents include more than one actor's discursive fragments on bulk surveillance. For example, for Civil Society we found relevant sections in the Written evidence given by different activists to the Joint Committee on the Draft Investigatory Powers Bill in the Parliament. All the documents selected for each stakeholder can be checked in the Appendices.

5.2 Data analysis

The next phase of our research is data analysis. In this sense, we apply methodological tools to collected material in order to "generate empirically grounded hypotheses about the discourse to hand" (Angermuller, 2015, p. 512).

For detailed analysis of collected data for each stakeholder we will use the following stages:

1. Identification in the text/statement of the discourse analytical instruments such as metaphors, frames, tropes, narrative structure, meaning patterns

2. Identification of the text/statement's argumentation/style/rhetoric, i.e. polemical, emotionalised, presentation, factual

5.2.1 MAXQDA

As a strategy for detailed analysis we opted for the use of a qualitative text-processing software (MAXQDA), a method which not only that facilitated but also enriched the interpretation of collected textual data. In this sense, we believe that the chosen software employed for analyzing qualitative data is a valuable tool with significant discourse-analytic potential.

We designed an initial coding scheme (see Annex 6) on the basis of the literature review. We started with a deductive set of two broad thematically contrasting codes derived from the literature: "bulk surveillance as solution" and "bulk surveillance as threat". To these two parent-codes we added more inductive sub-codes in order to explore the main frames in more detail.

Through an inductive process, we subsequently added more codes and sub-codes. At the end of the coding process, we counted 66 codes (Appendix 2), 2079 coded segments from a total of 30 documents structured in 5 document groups according to stakeholders.

With the help of MAXQDA we identified the topical structures of the existing discourses on bulk surveillance and the nodal points in each stakeholder's case. We then compared the various resulting analytical models from each stakeholder and looked after similarities, overlap in frames and narrative patterns in order to identify any potential discourse coalitions and map the entire discursive landscape on bulk surveillance in the UK.

5.2.2 Nodal points and floating signifiers

As a scholar of critical research methods noted, "a discourse takes place around nodal points [which can be described as] privileged signifiers around which moments are ordered in chains of equivalence and whose meaning within a discourse has already been

established" (Müller, 2011). Nodal points differ from floating signifiers which are elements "open to differential ascriptions of meaning" (Müller, 2011). Therefore, floating signifiers can be seen as the main fighting ground between different discourses. Once the meaning has been established, they become nodal points (Herschinger, 2011, p. 80).

In our study, the nodal points were identified at the end of the coding process, by looking at the total frequency of their appearance[4] and at the highest number of co-occurrences (see Figure 10), within all textual data. The nodal points around which the debate on bulk surveillance revolves are: "human rights", "necessity and proportionality", "oversight and safeguards". As we show in the section F of this chapter, at least one of these nodal points is a common occurrence between the discourses of any two stakeholders analyzed.

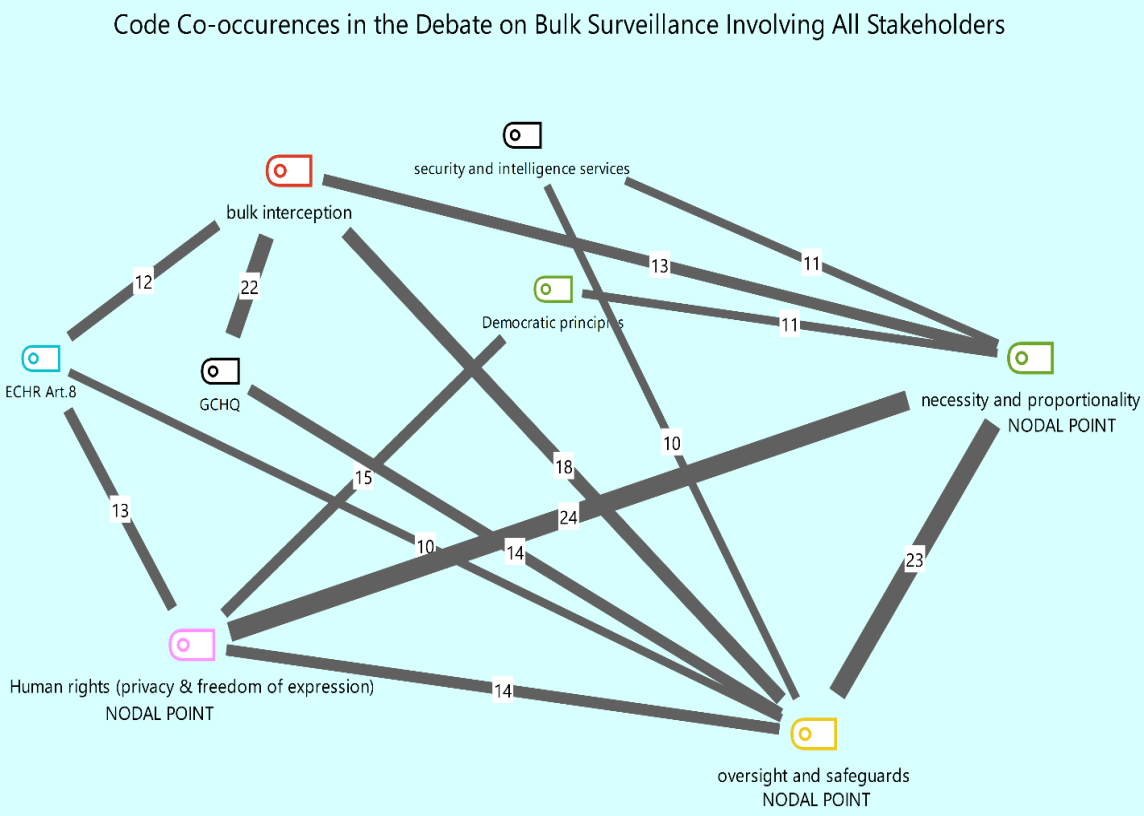

Figure 9 : Nodal points structuring the policy debate on bulk surveillance in the UK

A nodal point "creates and sustains the identity of a discourse by constructing a knot of definite meanings […] [having] a structural role of unifying a discursive terrain"

[4] "Oversight and safeguards" (142); "Necessity and proportionality" (134); "Human rights" (100).

(Herschinger, 2011, p. 79). References to “human rights”, “necessity and proportionality” and “oversight and safeguards” represent a common discursive ground for all the stakeholders taking part in this expert debate. However, the construction of nodal points is a practice which can fix meaning only partially (Laclau & Mouffe 2001, p. 113). The nodal points are framed differently in each actor’s case in order to fit different discursive strategies and goals. To grasp these frames, we had to look at the unique narrative elements in each actor’s discourse. Thus, after comparing the topical structures of the discourses articulated by the different stakeholders (section F), we found specific topics for each of the identified stakeholders. Analyzed in conjunction with the nodal points, these specific narratives help us in reconstructing the discourses on bulk surveillance for each stakeholder.

The obvious floating signifier in our case is “bulk surveillance” because its meaning is still subject to contestation and struggle between different discourses. As we will show, the discursive struggle is reflected in a set of contrasting frame-pairs such as bulk surveillance as threat vs solution, as indispensable vs unnecessary, as transparent vs opaque etc. as well as in the terminological ambiguity surrounding the topic: mass surveillance vs bulk collection. The very fact that there is still no agreement on a basic aspect such as terminology, indicates an ongoing discursive struggle. We can assert that the attempt to establish a fixed meaning for bulk surveillance -not limited to its legal meaning- is the core dimension of the whole debate we are examining.

5.2.3 Qualitative policy research

Our aim is to identify and reassemble specific narrative patterns and meanings in order to obtain, through an interpretive process, a representation of the major societal discourses on bulk surveillance in the UK. This move will assist us in achieving the larger goal of improving our understanding on a key policy phenomenon. In this regard, our approach can also be assigned to the field of qualitative policy research. A sound comprehension of the whole policy debate and discursive struggle on bulk surveillance will also help to better understand another emerging policy debate in the UK, that is the use and normalization of AI for national security and intelligence purposes. A debate on such a critical topic was clearly announced by the GCHQ director Jeremy Fleming in a rare GCHQ public paper from 2021 conceived as a guide for the agency’s future use of AI:

"At GCHQ, we believe that AI capabilities will be at the heart of our future ability to protect the UK. […] We need honest, mature conversations about the impact that new technologies could have on society. This needs to happen while systems are being developed, not afterwards" (GCHQ, 2021, pp. 4-9).

5.3 Mapping the discourses on bulk surveillance

We structured the groups of existing documents (data) according to the stakeholders identified. These are the results after all data modelling using MAXQDA. We offer here a graphical outline of the research methods employed.

A) Mapping the governmental and intelligence discourse

Arguably, the key document coming from the executive/SIS is "Operational case for bulk powers". It is a key document for several reasons. Firstly, because we are presented directly with the voice of the executive and the SIS regarding bulk surveillance. The self-proclaimed scope of the document is to explain "how bulk powers are used by the security and intelligence agencies today and why they are so valuable to our security" (Operational case, 2016, p. 5). A careful examination of this document can reveal important discursive features and fragments. Secondly, it is a key document because in this special field marked by restrictions there is a scarcity of public texts representing directly the position of SIS on such matters. As the GCHQ director noted a few years later, it was "the first time that UK intelligence agencies had explained their work in such detail" (GCHQ, 2021). The presentation of case studies and reality-based scenarios in a public document was unprecedented, making its inclusion in our discourse analysis essential.

It can be noticed that, "oversight and safeguards" is a topic which, surprisingly enough, shows up as part of the executive discourse when measuring frequency (see Figure A1). The fact that the executive discourse is construed around and includes elements such as oversight and frequent references to the legal principles of necessity and proportionality, indicates a discursive strategy of legitimation and trust building. The same framing is also reflected by the words of the former GCHQ director, David Omand: "[…] considerations of protecting society from harm suggest strongly that outlawing intelligence-gathering techniques such as bulk access to digital data would be a mistake and instead argue in favour of allowing their use under strict controls and oversight" (Omand and Phythian, 2018, p. 30).

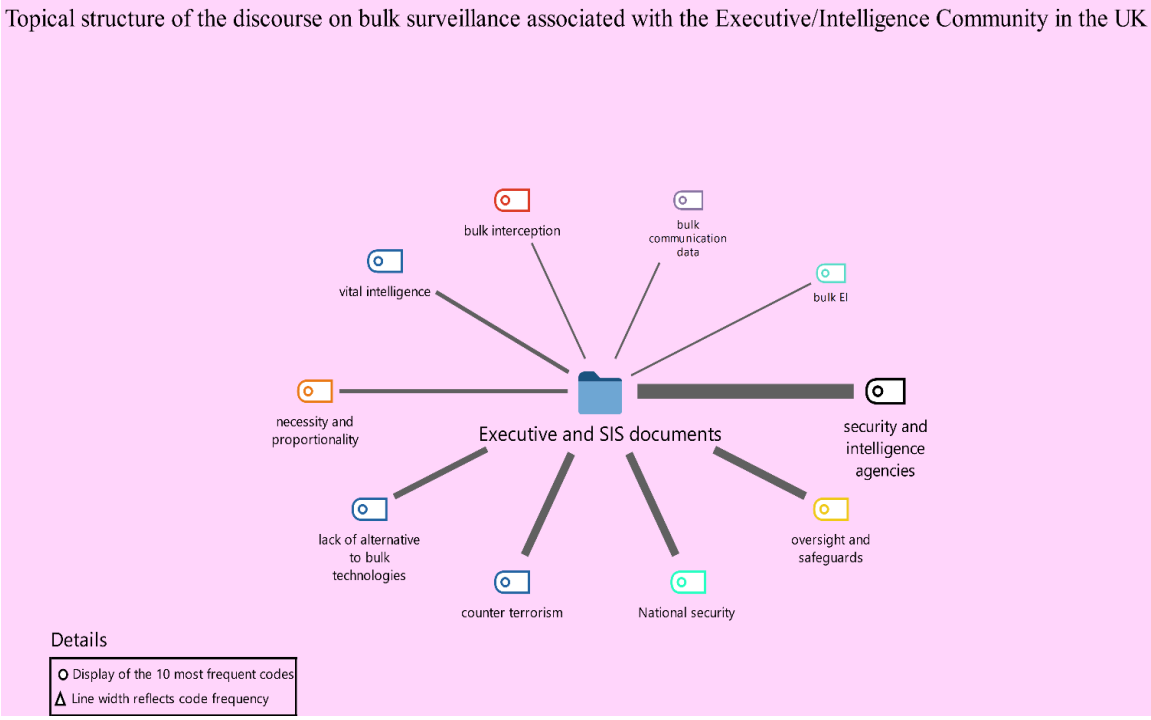

Figure A 1: A representation of the topical structure of the discourse on bulk surveillance belonging to the Executive /SIS

The emphasis on oversight and safeguards is also a way to respond to criticism coming from civil society organizations which have been accusing intelligence agencies of unconstrained power and of practicing indiscriminate "mass surveillance". In this sense, the topical structure of the executive/SIS discourse reflects a narrative strategy aimed at neutralizing the criticism from civil society. Democratic importance and efficiency of oversight and safeguard mechanisms, are invoked here rather to legitimize the use of bulk surveillance as the only way to protect society. In other words, bulk surveillance is legitimate and should not be outlawed as long as there are strong oversight mechanisms in place safeguarding the principle of democratic accountability. Therefore, "the critique of disproportionate surveillance as generalized is recast through the balance of proportionate action, which limits infringements of rights while generalizing security" (Aradau & McCluskey, 2022b, p. 11). This narrative framing is coupled with the idea that without bulk surveillance, intelligence agencies would not be able to properly protect society from potential dangers like terrorism.

The most frequent way to justify bulk surveillance as a solution, is by invoking its crucial importance in countering terrorism (see Figure A2). The fight against terrorism is the most prominent frame within the discourse of Executive/SIS regarding bulk

surveillance practices. Featuring with the second highest frequency is a frame that presents the use of bulk technologies as unavoidably necessary because of the lack of alternative security solutions in some scenarios. Lastly, acquiring vital intelligence given the time constrains in some security crises, is another important frame of the discourse justifying the obligatory use of bulk surveillance.

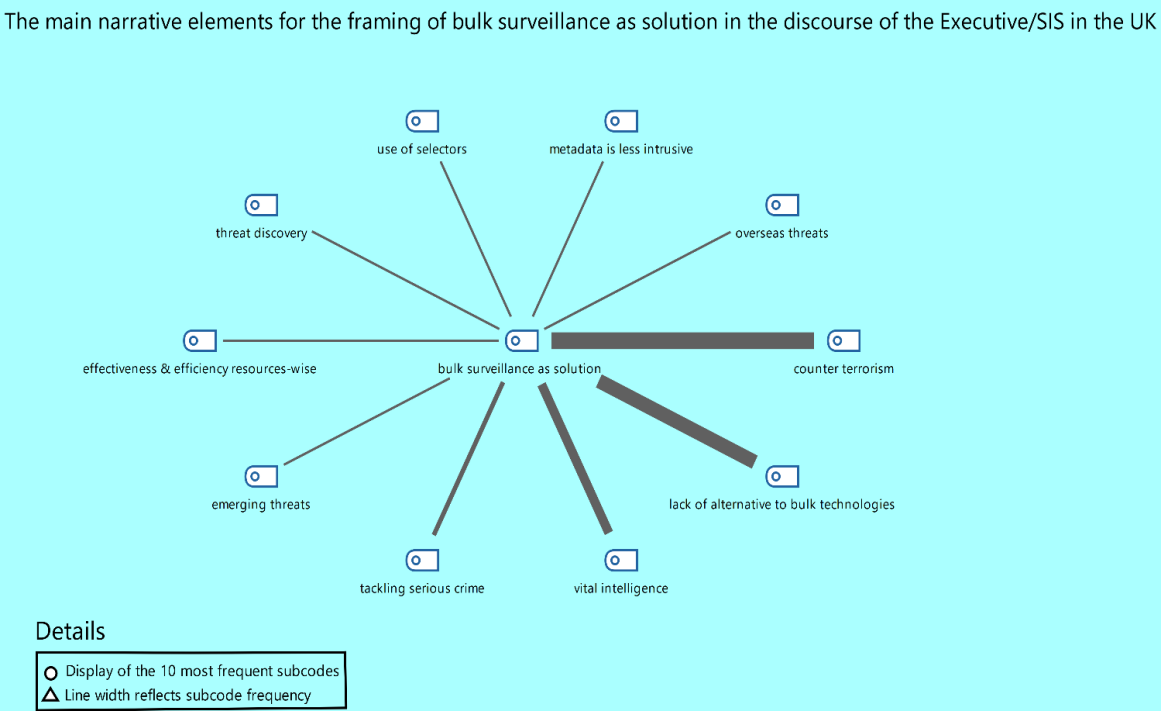

Figure A 2: Relationship between parent code bulk surveillance as solution and its subcodes

The overlaps in lines of discourse are depicted in the table below (see Figure A3). This function is particularly useful for understanding of how framing is used:

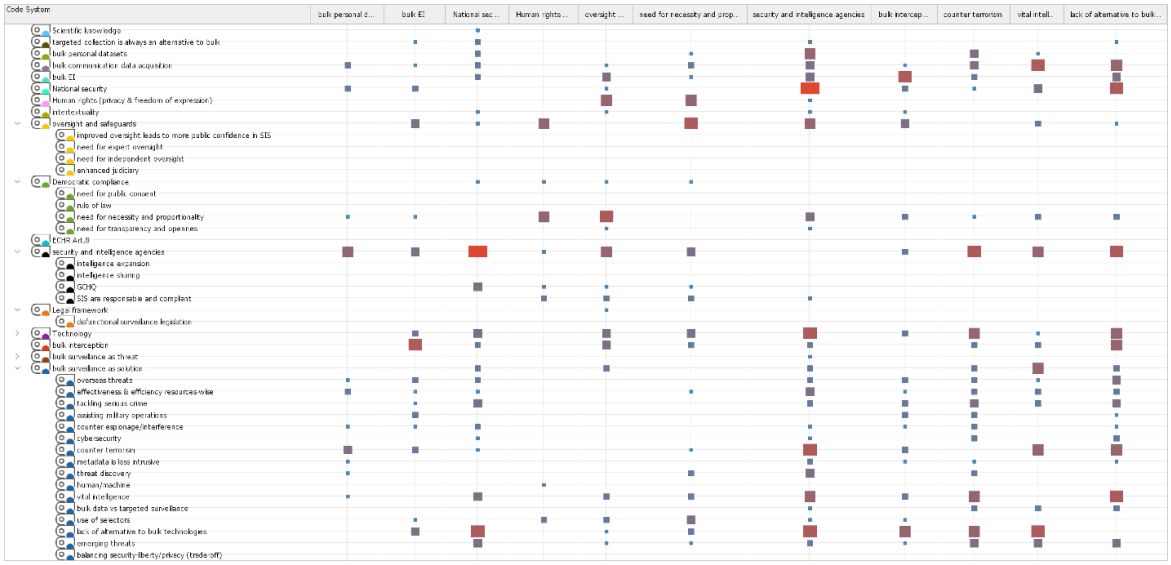

Figure A 3: Code relations browser for Executive/SIS – which codes occur together more often or less often based on the size of the squares

Based on this function, we found several overlaps. The code "national security" overlaps significantly with "lack of alternative to bulk technologies" and "SIS" (see Figure A3). The first overlap reveals a framing of national security as being reliant on the use of bulk technologies or that bulk technologies are essential for the preservation of national security. The second overlap emphasize the central role of the SIS in preserving national security.

Another overlap is the one between "SIS" and "technology" and "SIS" with "counter-terrorism": this overlap indicates a discursive framing of the intelligence agencies as tech-savvy actors possessing the necessary expertise to properly exploit highly intrusive and complex technologies such as the bulk powers frequently deployed in counter-terrorist operations.

Finally, "vital intelligence" overlaps with "bulk acquisition" and with "lack of alternative to bulk technologies": in this overlap, bulk powers such as acquisition of communication data are framed as indispensable for obtaining vital intelligence, for example in operations where time is of the essence. In some contexts, using bulk technologies is the only option for saving lives according to this framing and therefore it is justified.

B) Mapping the civil society's discourse

Civil society organisations have been influencing the debate on bulk collection mainly through litigation and advocacy. In order to reconstruct the core elements of their

discourse and how they have been framing their critiques, we examined, from a discourse perspective, the argumentation put forward in written submissions of key litigation cases such as "Big Brother Watch". As one can deduct from the drawing (see Figure B1), the most prominent topics of the discourse on bulk surveillance articulated by civil society organisations in the UK, are “need for necessity and proportionality”, “human rights” and “oversight and safeguards”. Their critique is thus framed, “by and large, in terms of establishing safeguards and legal mechanisms of necessity and proportionality” (Aradau & McCluskey, 2022b, p. 10). A possible explanation for this topical structure of the civil society discourse centred on legal principles, could be found in the constrains imposed by the language and approach of litigation, either before domestic courts or before ECtHR.

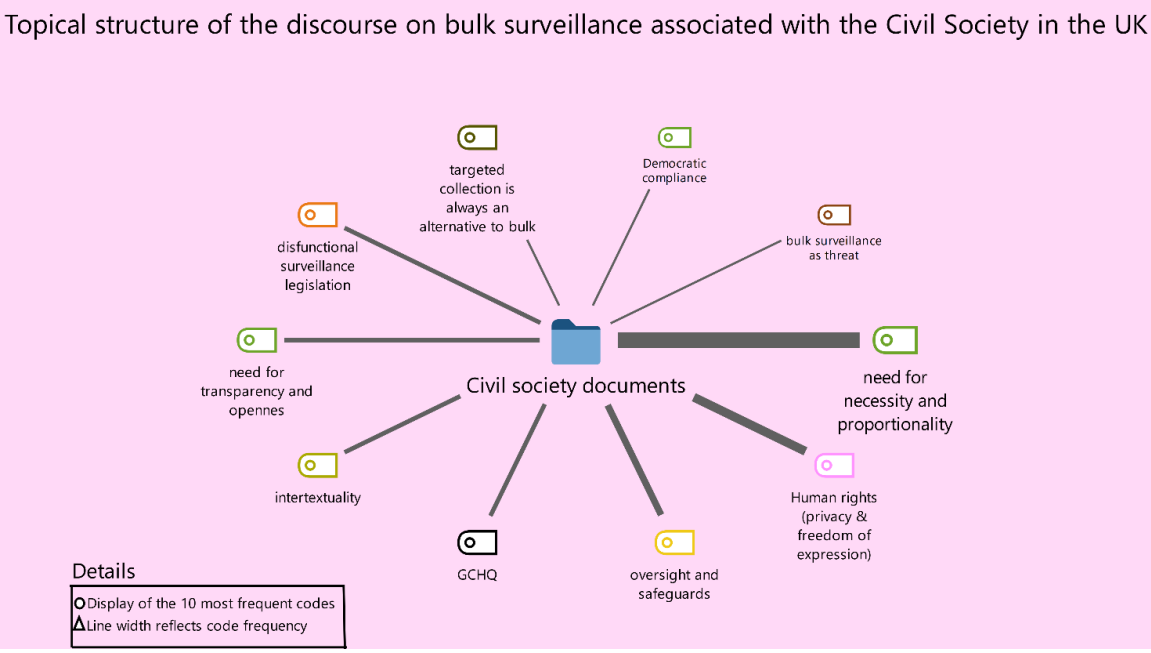

Figure B 1: A visual representation of the topical structure of the discourse on bulk surveillance belonging to the civil society

The most frequent way to frame bulk surveillance as a threat, is by invoking the term “mass surveillance” (see Figure B2). Already discussed earlier in the thesis, the terminological debate on bulk surveillance is normatively loaded. Thus, “mass surveillance” implies rights infringements on a general scale, invoking tropes of a totalitarian state reminiscent of Orwell’s dystopic universe or historical examples like East Germany’s total surveillance regime. Moreover, the reference to Snowden revelations, a scandal with a significant negative reverberation into the UK’s public sphere, is also a key narrative device for framing bulk surveillance as threat.

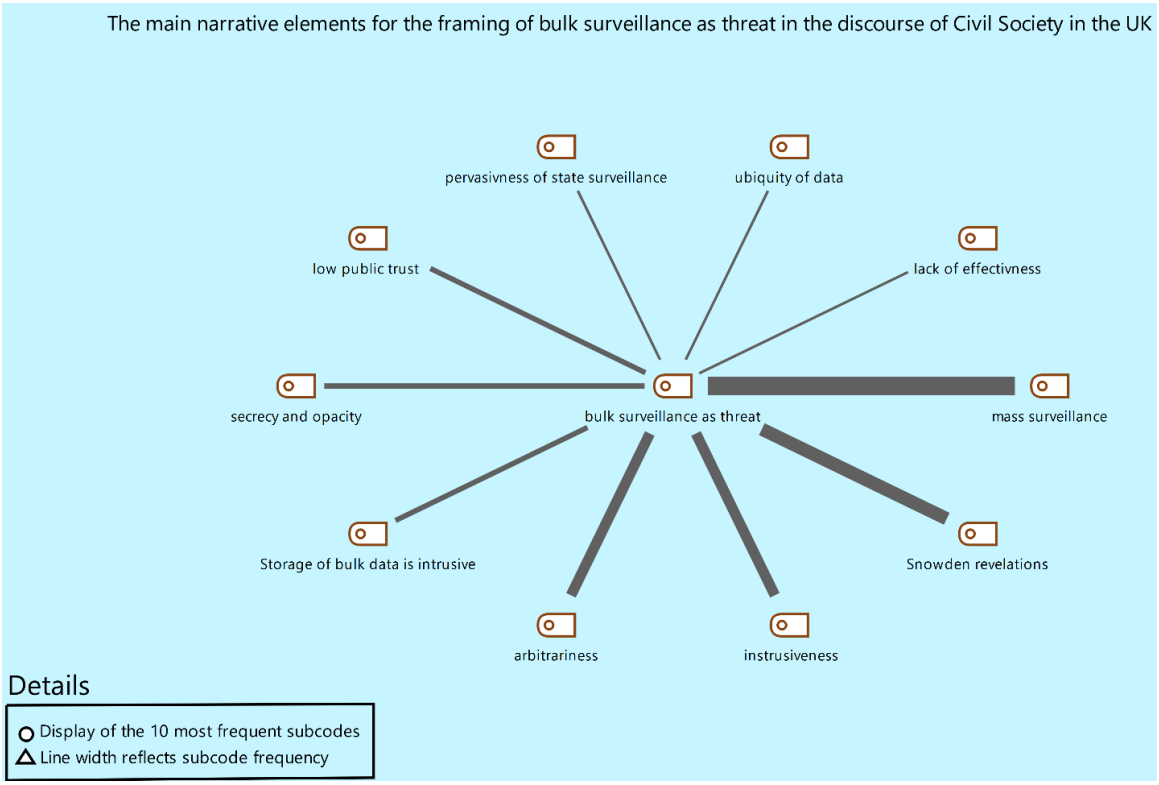

Figure B 2: Relationship between parent code bulk surveillance as threat and its subcodes

Next, the overlaps in lines of discourse for civil society, are depicted in the table below (see Figure B3). We found that the code "need for necessity and proportionality" has a significant overlap with several other codes: "targeted collection is always an alternative to bulk", "human rights (privacy and freedom of expression)" and "bulk surveillance as threat". These overlaps reveal a framing of targeted surveillance as the only surveillance method that can be used in accordance with the principles of necessity and proportionality while deductively, bulk collection is framed as a method that could never qualify as necessary and proportionate. Also, part of this framing is the narrative of necessity and proportionality as essential safeguards for the protection of privacy and freedom of expression.

Figure B 3: Code relations browser for Civil Society – which codes occur together more often or less often based on the size of the squares

Framing of bulk surveillance as a technique that can never be justified is also made through critical references to the influential review reports authored by David Anderson QC. Such intertextuality is present in key documents that we used as primary data. Anderson's review reports are often referenced and criticized in documents from civil society organizations such as Liberty and Privacy International. For example, one of the documents from Privacy International (2016) states: "David Anderson's recent report does not make a robust case. Instead, it asks the security and intelligence agencies to explain how these powers are effective, and accepts their justifications, even where they are merely hypothetical" (p. 10).

Another pair of overlapping codes is "oversight and safeguards" with "dysfunctional surveillance legislation". One of the major elements of the civil society's discourse on bulk surveillance, is the criticism of the legal framework for the investigatory powers. According to this framing, the central problem of the legal framework is the lack of proper oversight and safeguards. Although appraised by some critical scholars as not being contesting enough, this line of discourse emphasizing the importance of legal oversight and safeguards, has been a constant occurrence in the utterances coming from the civil society.

Finally, the code "need for transparency and openness" overlaps with "SIS". Part of the criticism coming from the civil society regarding bulk surveillance refers to the opacity and lack of transparency previously manifested by the intelligence community. With the crisis of public trust generated by the Snowden disclosures, the civil society actors in the UK have been advocating for more transparency and openness in the realm of intelligence and national security. Consequently, this frame has become a constituent element of their discourse on the use of bulk surveillance, presented as opaque and arbitrary.

C) Mapping the oversight institutions' discourse

It is rather unsurprising that the most frequent topic in the discourse of oversight institutions is related to oversight and safeguards against bulk surveillance (see Figure C1). However, what may seem surprising for a discourse articulated by intelligence oversight institutions, is the high frequency occurrence in this structure of the code "SIS are responsible and compliant". It is higher than "need for transparency and openness" for example, and significantly higher than "human rights". A potential explanation for this frequent occurrence is the soft tone of the parliamentary oversight body (ISC) towards the intelligence community in the early years following the Snowden disclosures. For example, in the 2015 report published by the Intelligence and Security Committee of Parliament it is stated that:

> "We are satisfied that the UK's intelligence and security Agencies do not seek to circumvent the law – including the requirements of the Human Rights Act 1998, which governs everything that the Agencies do. […] We are satisfied that they [GCHQ] apply levels of filtering and selection such that only a certain amount of the material on those bearers is collected" (ISC Report, 2015, p. 2).

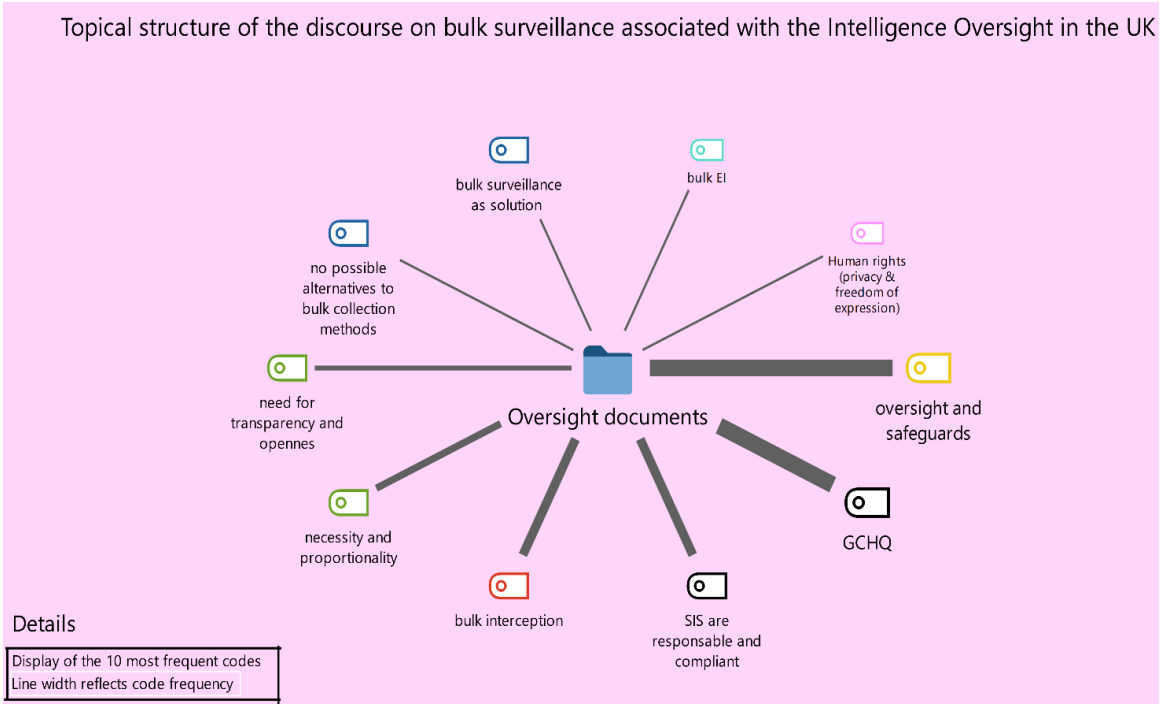

Figure C 1: A visual representation of the topical structure of the discourse on bulk surveillance belonging to the intelligence oversight bodies in the UK

Next, in the visual representation below (see Figure C2), one can detect which codes occur together more often or less often based on the size of the squares. It can be observed that the code "SIS are responsible and compliant" overlaps significantly with "GCHQ". As previously mentioned, this analytical function is particularly useful for understanding of how framing is used.

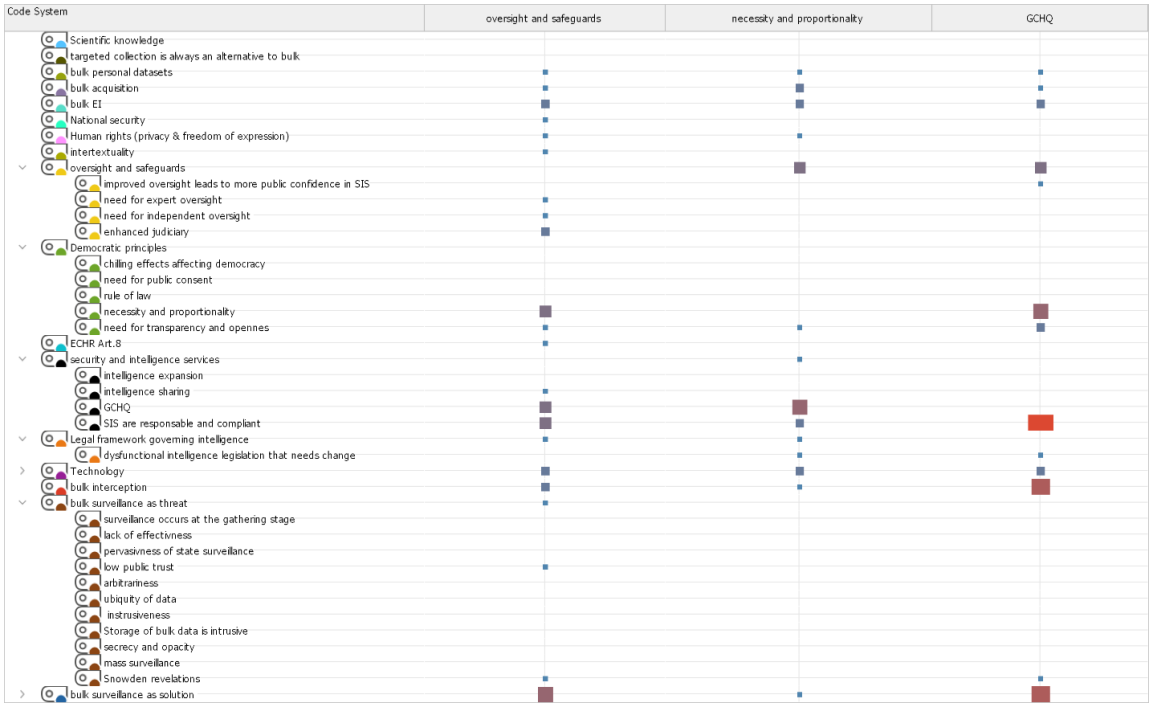

Figure C 2: Code relations browser – observing the potential overlaps in lines of discourse

The framing of GCHQ, the main intelligence actor associated with bulk surveillance, as responsible and complying with the democratic principles is part of the oversight discourse in the UK. In the IPCO Annual Report 2017 & 2018 it is stated that: "GCHQ carries out robust retrospective audit checks" (IPCO Annual Report 2017, 2019, p. 66) [and that] "we [IPCO] have been satisfied that the use of bulk powers is appropriate (IPCO Annual Report 2018, 2020, p. 118).

Another overlap is "Bulk surveillance as solution" with "GCHQ". This framing suggests not only that bulk surveillance represents a legitimate tool for countering different security threats, but also that GCHQ is the main institution with the appropriate resources to manage these powerful technological capabilities. As the members of the oversight parliamentary committee declared, "[…] we acknowledge that GCHQ's bulk interception is a valuable capability that should remain available to them" (ISC Report, 2015, p. 33).

D) Mapping academia's discourse

In the case of academia, we found that the topic of "metadata" has been the main focus of various scholarly takes on bulk surveillance (see Figure D1). In this discourse, metadata is represented as being at least as or even more intrusive and dangerous for human rights than content data. Although it has been used in the past in some professional fields, the term metadata was catapulted into the public sphere and vocabulary by the Snowden

scandal, thus acquiring a negative connotation (Aradau & Blanke 2015). Metadata has become a concept associated with controversial security practices.

There are a few possible explanations of why "metadata" is a central topic of the academic discourse in the UK on bulk surveillance. One of these is that scholars writing on surveillance post-Snowden have been trying to demonstrate that metadata is at least as dangerous for human rights as content. In this sense, as Bauman et al., (2014) observed:

> "[t]here's nothing as direct or as in-your-face as Big Brother on a glaring telescreen, of course, but rather a more Kafkaesque unease that the ostensibly innocent metadata (the location, duration and recipients of calls, for instance) do in fact have consequences" (p. 141).

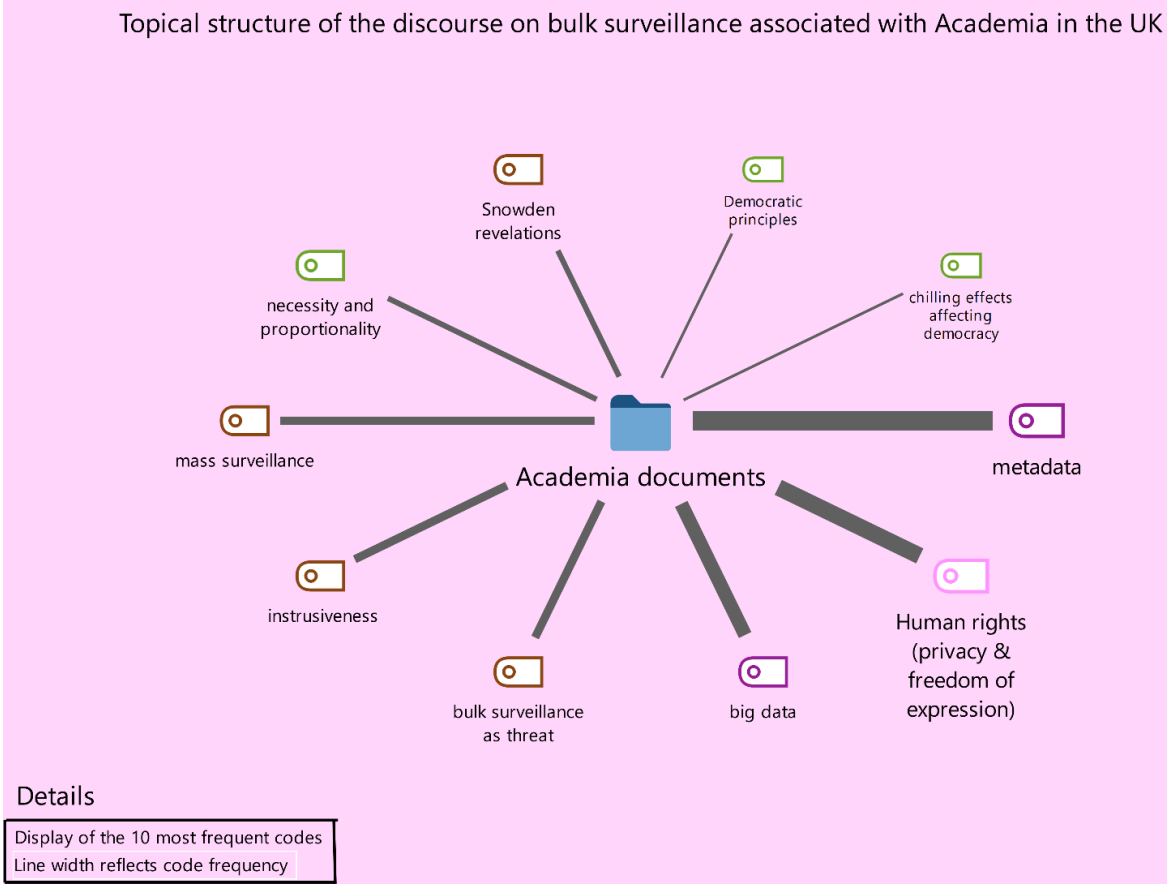

Figure D 1: A visual representation of the topical structure of the discourse on bulk surveillance belonging to academia, in the UK

An examination of the overlap in lines of discourse, reveals that the most frequent connection between codes is the one between "metadata" and "intrusiveness" (see Figure D2).

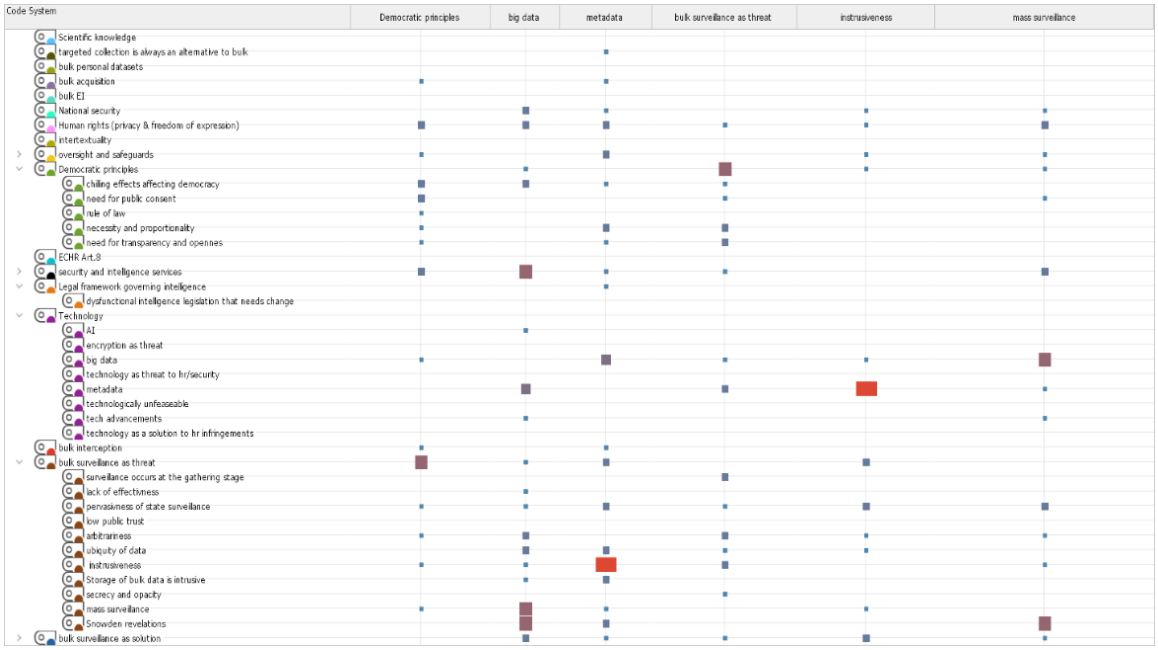

Figure D 2: Code relations browser for academia – which codes occur together more often or less often based on the size of the squares

Compared to content data, metadata is "differently intrusive" (Bernal, 2016, p. 260) and can have a harmful impact on other rights beyond privacy, such as freedom of expression, association and assembly and respect for human dignity (Murray & Fussey, 2019). In this sense, we can state that the academic discourse has a warning undertone regarding the impact of metadata collection by intelligence agencies. Precisely, it is suggested that metadata collection is a technique which should not be underestimated by the legal and human rights approaches to bulk surveillance.

The problematization of metadata (e.g. how it is produced), is an important step towards challenging the "justificatory discourses of security professionals" (Aradau & Blanke, 2015, p. 4). Metadata is also a gateway concept for understanding how intelligence agencies function as Big Data organizations. From this perspective, an assessment of bulk surveillance practices employed by GCHQ would require a critical understanding of how bulk data is produced, in the first place.

E) Mapping ECtHR discourse

As two critical scholars of surveillance recently observed, "[t]he ECtHR has been a productive site for disputing digital surveillance both before and after the Snowden disclosures" (Aradau & McCluskey 2022b, p. 4). We identified two key cases disputing bulk surveillance practices in the UK, lodged before the ECtHR since 2013. The applicants

in these cases were 14 civil society organisations in the UK and other individuals. The most frequent topic in ECtHR decisions on bulk surveillance is "oversight and safeguards" (see Figure E1). Regarding the use of bulk interception, the Court recommended that it should be authorised by an independent body, unrelated to the Executive (BBW v the UK, paragraph 351). The emphasis on oversight and safeguards is present at all levels of recommendations, including how the selectors should be used:

> "enhanced safeguards should be in place when strong selectors linked to identifiable individuals are employed by the intelligence services. The use of every such selector must be justified – with regard to the principles of necessity and proportionality – by the intelligence services and that justification should be scrupulously recorded and be subject to a process of prior internal authorisation providing for separate and objective verification of whether the justification conforms to the aforementioned principles" (BBW v the UK, paragraph 355).

The Court is also stressing the importance of proper oversight for the operations involving metadata in bulk:

> "the Court is not persuaded that the acquisition of related communications data through bulk interception is necessarily less intrusive than the acquisition of content. It therefore considers that the interception, retention and searching of related communications data should be analysed by reference to the same safeguards as those applicable to content" (BBW v the UK, paragraph 363).

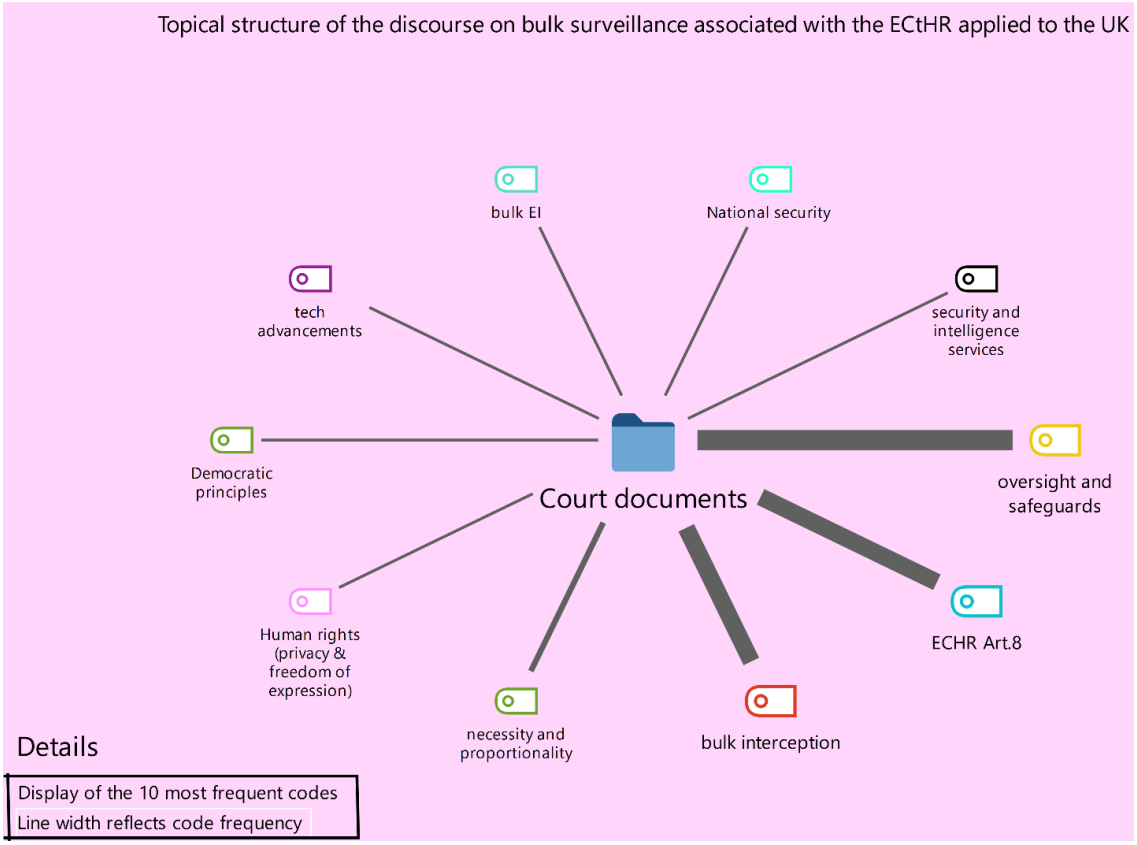

Figure E 1: Topical structure of the discourse on bulk surveillance in the UK as articulated by the ECtHR judgments

As illustrated in the table below, the codes which occur together most often are "bulk interception" and "Article 8 of ECHR" (see Figure E2).

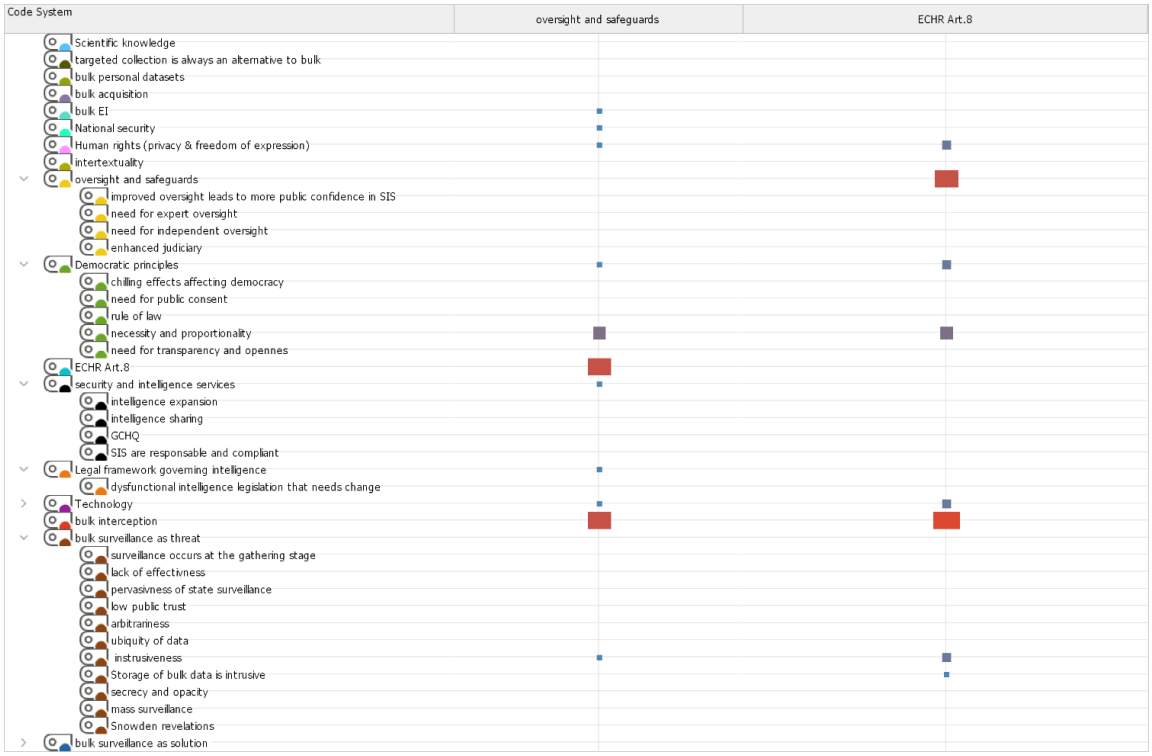

Figure E 2: Code relations browser for ECtHR– which codes occur together more often or less often based on the size of the squares

F. Comparative analysis

A data analysis comparative function was used, in order to visualize what are the common relevant topics that occur in the existing discourses, and the exclusive topics for each stakeholder. Analyzed in conjunction with the nodal points, these specific narratives help reconstructing the discourses on bulk surveillance, for each stakeholder.

By using this comparative function, two aspects were measured:

- The topics that are exclusive for each stakeholder in relation to the other stakeholders. These are the codes displayed on the sides, with the highest frequency of occurrences. In other words, by using this scheme we identify the specific narrative elements for each stakeholder.

- The conceptual distance and thus the potential for discourse coalition between different pairs of actors. This is achieved by comparing the codes displayed on the sides (one for each actor) that have the highest frequency for each comparative set of stakeholders. We identified the different conceptual distances between

discourses/stakeholders by using our own organizing, interpretive scheme of the concepts which resulted after the empirical analysis of the texts.

Executive/SIS discourse in comparative perspective

a) Specific narrative elements

The specific narrative elements for the executive/SIS in relation to other stakeholders, selected based on the highest frequency, are: "emerging threats"**,** "no possible alternatives to bulk collection methods" and "counter-terrorism". These three frames are combined with the nodal points "human rights", "oversight and safeguards", "necessity and proportionality" in order to articulate the discourse on bulk surveillance.

The nodal points which are located in the middle section of the figures, represent a common ground of the two discourses. It may seem surprising that executive/SIS discourse employ frames such as "need for necessity and proportionality", "oversight" and "human rights". However, as we already stated, they reflect the new discursive strategy of trust-building pursued by the intelligence community in the UK post-Snowden. As former GCHQ director David Omand explained:

> "We have moved into a new era and I am personally very glad of that. A lot of trouble would have been saved if, say, even five years ago the codes of practice—it would not necessarily have taken new legislation—on equipment interference, investigative powers and so on had all been updated to the modern digital world. For one reason or another that was not done. The shock of discovering what was happening, for very good reason—to defend the public and our security—was all the greater. I think the lesson has been learnt" (Report Parliament on Draft investigatory powers bill, 2016, p. 87).

The narrative element "no possible alternatives to bulk collection methods" present in the executive/SIS discourse, emphasizes the absolute necessity of bulk technologies in some cases in order to save lives and defend "the public and our security". It is also discursively used as a way to counter the narrative of "targeted collection is always an alternative to bulk collection" put forward by civil society organizations. According to this framing, bulk powers are indispensable for fighting terrorism and emerging threats. Apart from terrorism, they include "serious crime, the resurgence of state-based threats and cyber-attacks" (Operational case, 2016, p. 3). Within this narrative framework, intelligence

agencies are thus faced with risks and unexpected security threats which they can only defuse with the help of powerful tools such as bulk technologies.

b) Conceptual distance from the other stakeholders

After an examination of the figures F1.1, F1.2, F1.3 and F1.4, we found that the furthest away from the executive/SIS discourse is the discourse articulated by academia. The contrast between the two conceptual standpoints is captured by the opposing pair of specific narratives with the highest frequency: "bulk surveillance as threat" vs "no possible alternatives to bulk collection methods" (see Figure F1.1). These two positions are thus incompatible.

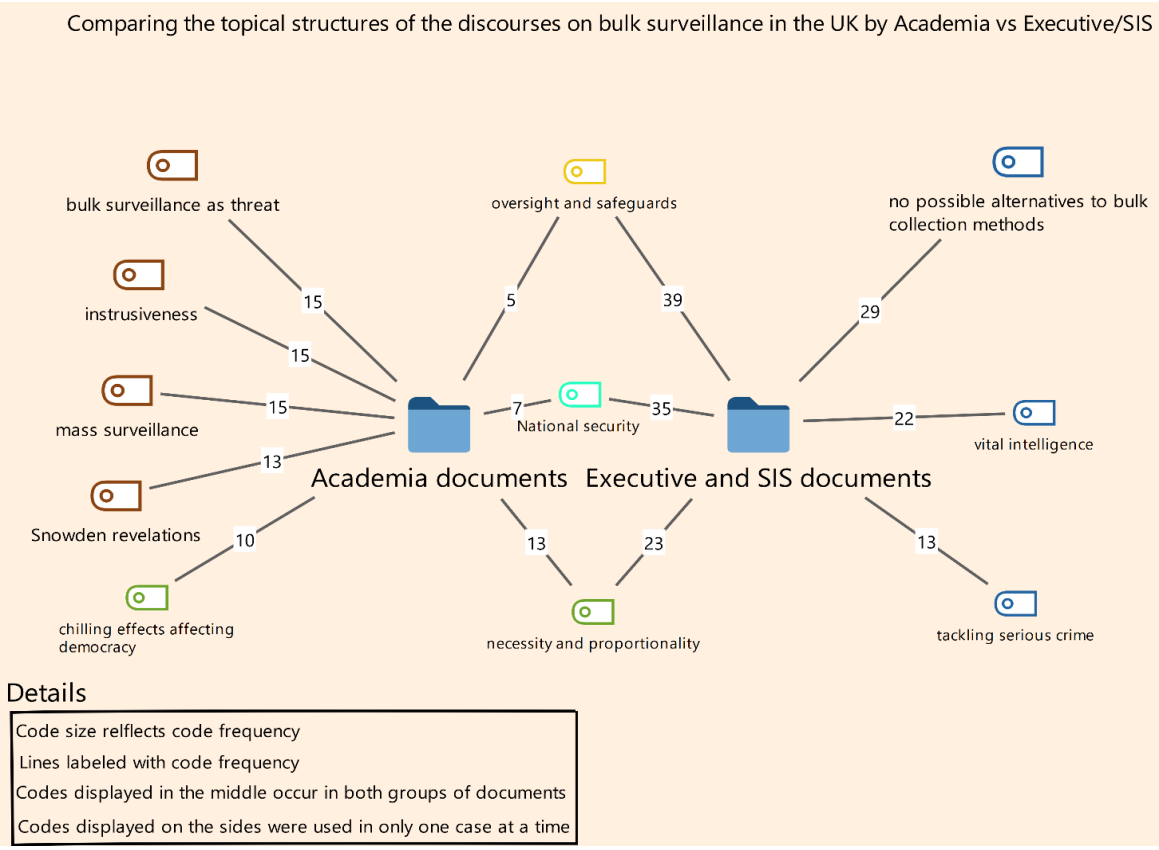

Figure F1. 1: Executive/SIS vs Academia

A comparison between topical structure of the executive/SIS discourse with civil society (see Figure F1.2) reveals also a conceptual significant distance through the pairs of narrative elements "emerging threats" vs "dysfunctional surveillance legislation" and "emerging threats" vs "bulk surveillance as threat". Although the standpoint of civil society is normatively similar to the one of academia, the reference to legislation is part of the

litigation constrains we mentioned earlier. In other words, civil society has been using a more legal language in their discourse, in order to fit the litigation discourse before the domestic and international courts.

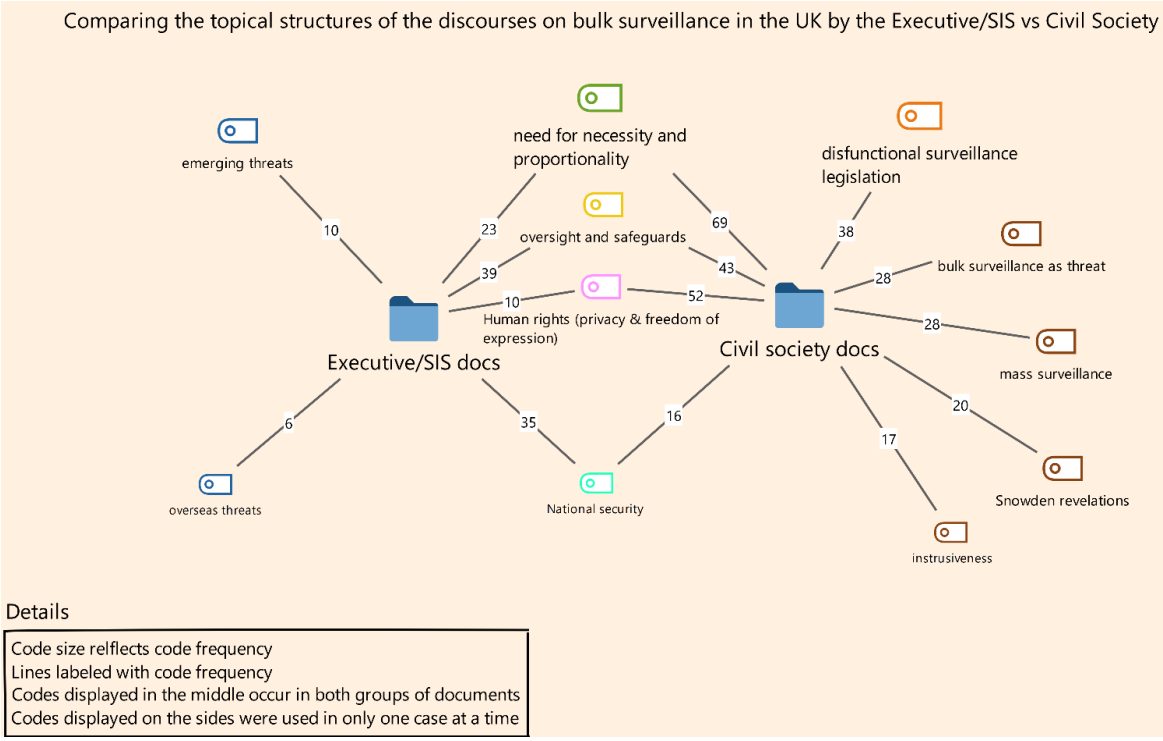

Figure F1. 2: Executive/SIS vs Civil Society

Between oversight and executive/SIS (see Figure F1.3) there is a weaker contrast captured by the pair of narratives “emerging threats” as opposed to “dysfunctional legislation” or “need for independent oversight”. We don’t find here a strong frame rejecting completely bulk surveillance like in the cases of academia and civil society. This weaker contrast suggests more compatibility between these two stakeholders, subject to further legal and technical changes and updates. The oversight discourse is not hence, a contesting discourse, but rather a technical, legally-oriented discourse which is not fundamentally incompatible with the executive/SIS discourse.

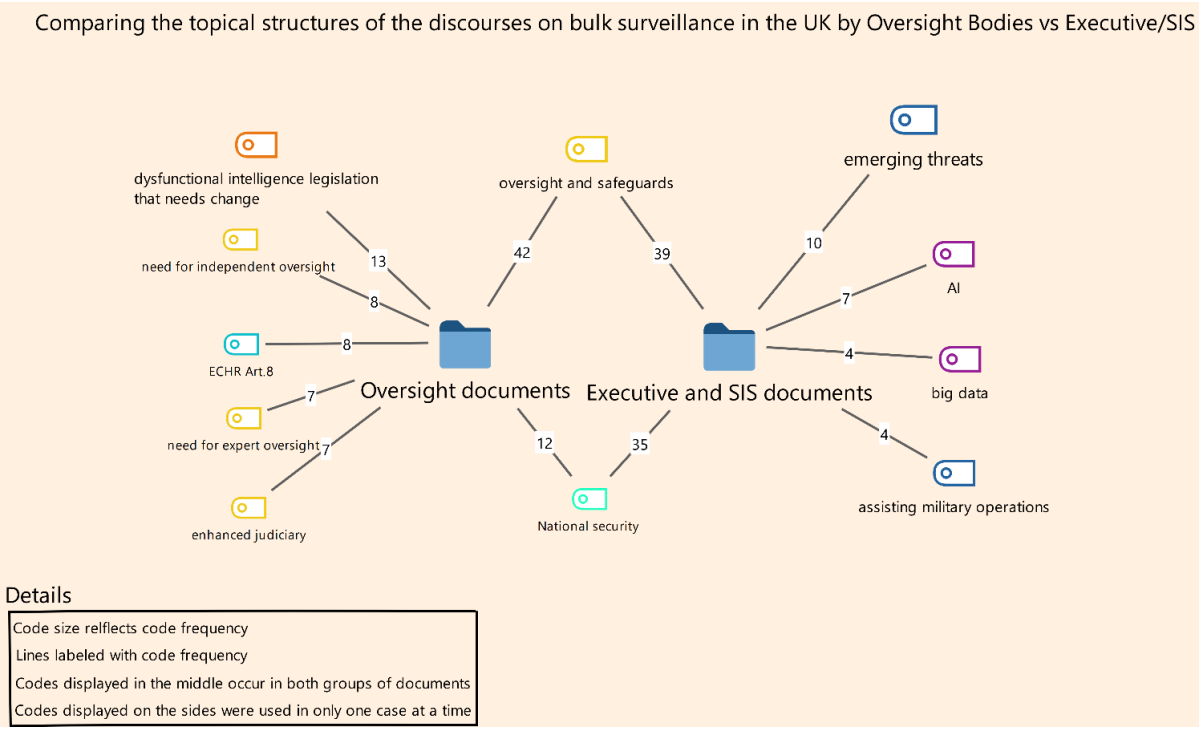

Figure F1. 3: Executive/SIS vs Oversight

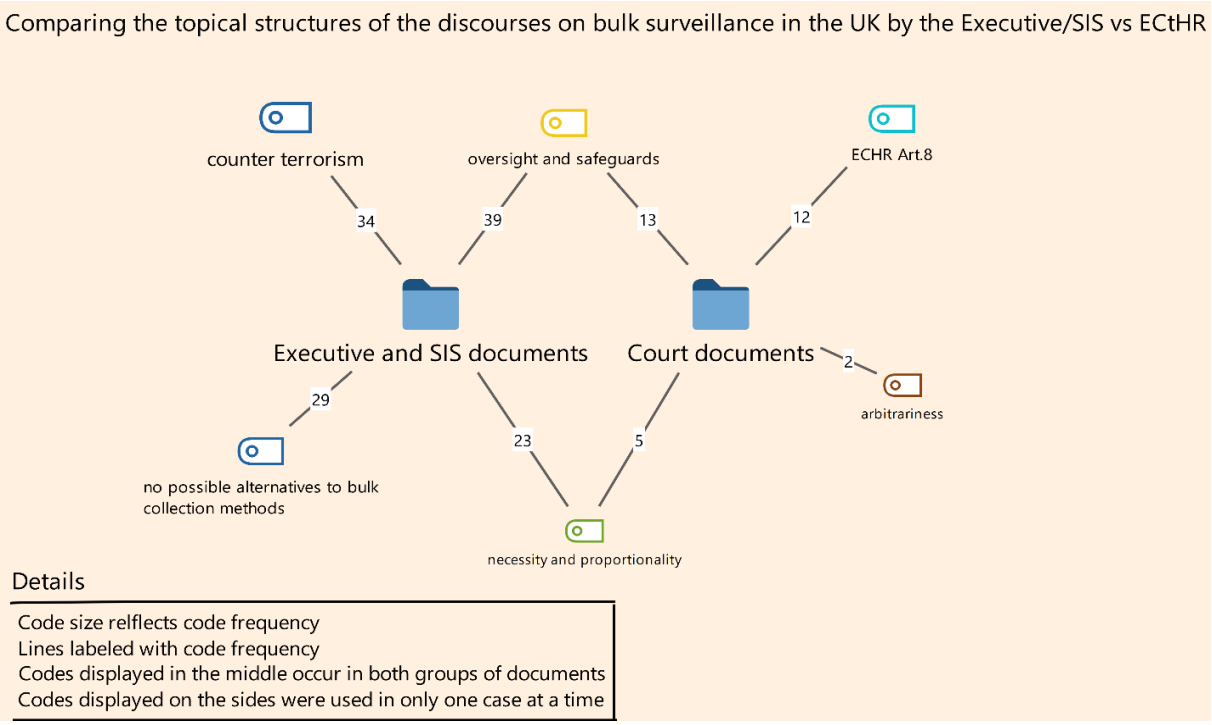

Figure F1. 4: Executive/SIS vs ECtHR

Civil Society discourse in comparative perspective

a) Specific narrative elements

The following specific topics of the civil society discourse, were found: “storage of bulk data is intrusive”, “technology as threat to human rights/security”, “dysfunctional surveillance legislation that needs change”.

b) Conceptual distance from the other stakeholders

In terms of conceptual distance, we found the highest compatibility at the level of discourse between civil society and academia (see Figure F2.1). We can observe fewer exclusive codes. The specific topics with the highest frequency in this case are “chilling effects affecting democracy” and “technology as a threat to human rights”. Normatively, they point to the same dangers of bulk surveillance technology, either for democratic participation or for human rights, two interconnected values. Without real freedom of expression and privacy, a democracy cannot survive. The discursive overlap between civil society and academia, offer the highest potential for a discourse coalition.

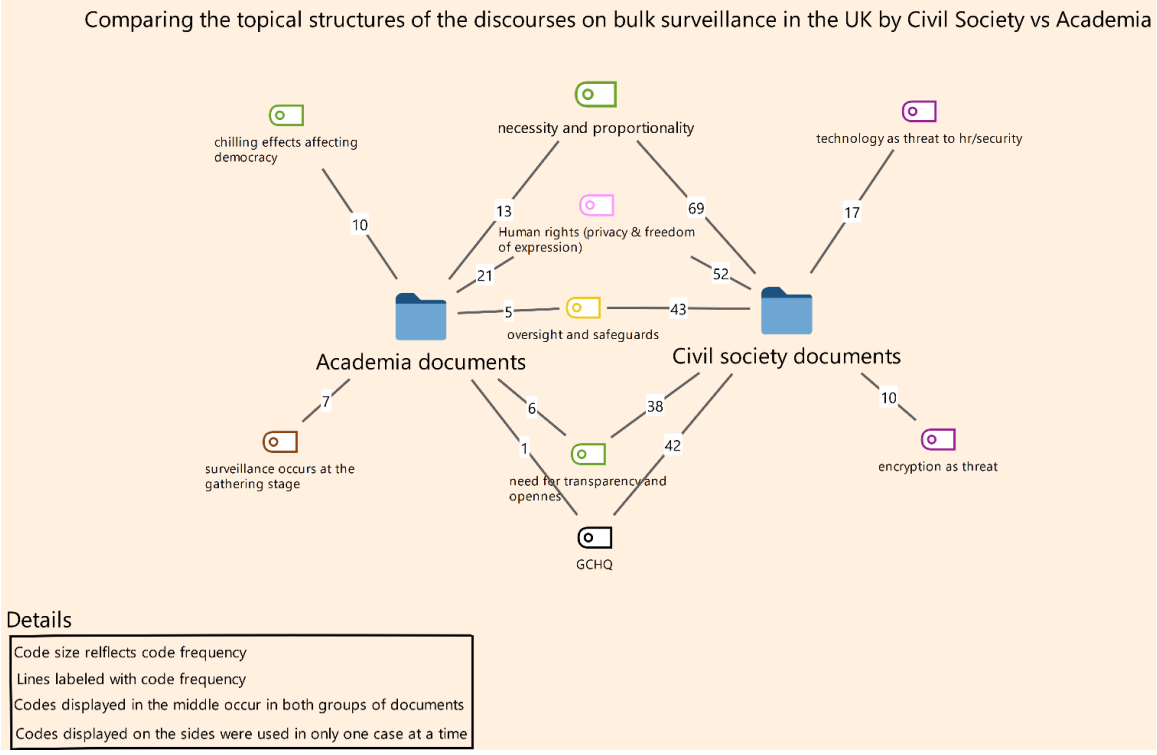

Figure F2. 1: Civil Society vs Academia

We also found a high degree of compatibility between civil society and oversight discourses (see Figure F2.2). In this case, one can observe a significant overlap but also that the oversight discourse does not have exclusive topics in relation to civil society

discourse. This shows that oversight discourse is influenced, and adopts themes, that are put forward by civil society.

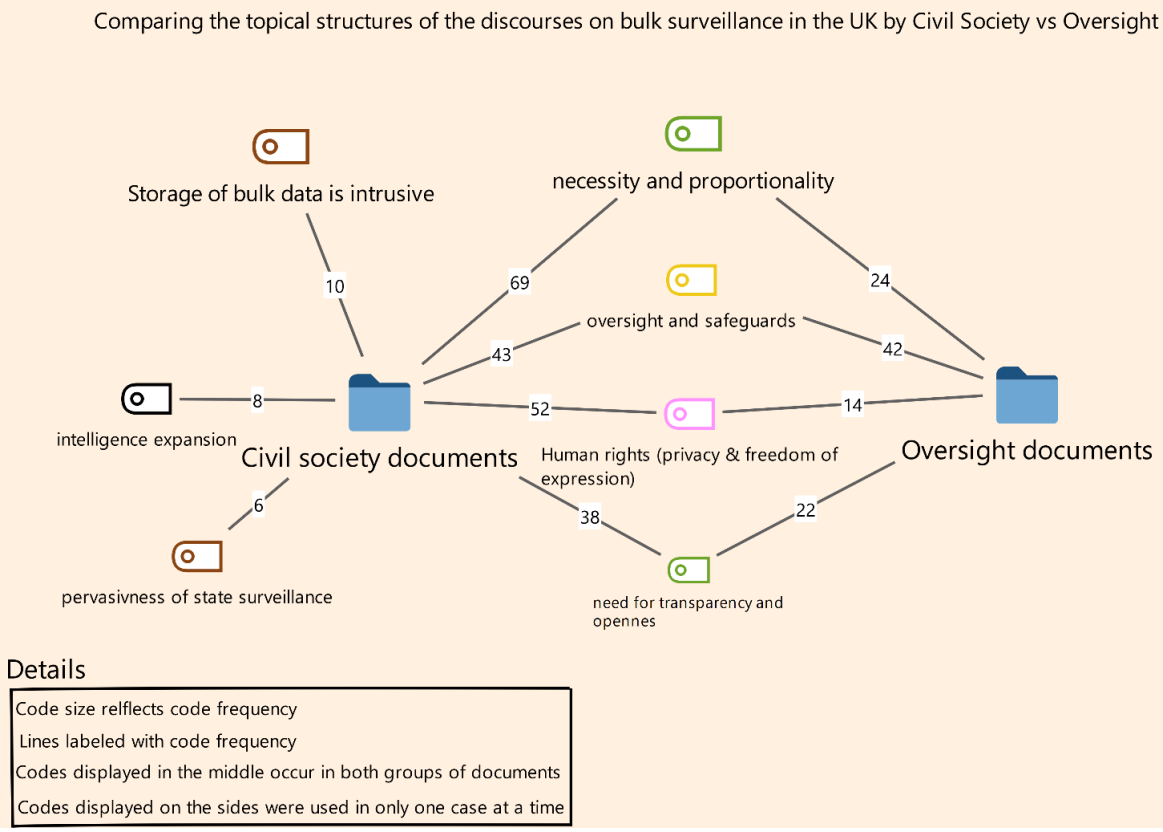

Figure F2. 2: Civil Society vs Oversight

Oversight discourse in comparative perspective

a) Specific narrative elements

For oversight, the following specific narrative elements were found: "dysfunctional intelligence/surveillance legislation", "SIS are responsible and compliant".

b) Conceptual distance from the other stakeholders

When comparing oversight discourse with academia's discourse (see Figure F 3.1), the results are mixed, revealing that the two discourses have both compatible and less compatible narratives. Some significant differences are captured by the opposing side pairs "SIS are responsible and compliant" vs "chilling effects affecting democracy" and "no possible alternatives to bulk collection methods" vs "storage of data is intrusive". The narrative framing of bulk surveillance is different in the case of these two actors.

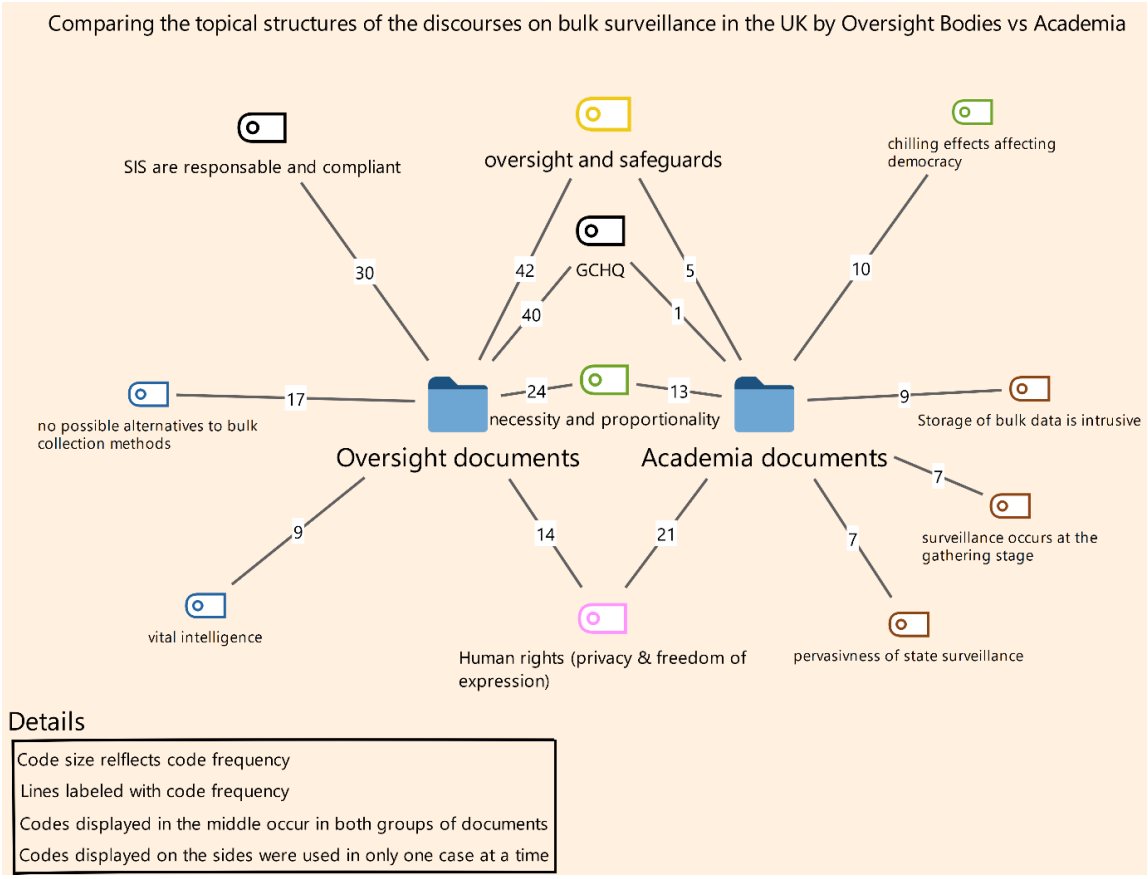

Figure F3. 1: Oversight vs Academia

5.4 Conclusion

The interpretive scheme we used in the comparative section, helped us to make refined findings like the fact the discourse of academia is more contrasting than the oversight discourse vis-à-vis the intelligence discourse. Thus, based on the interpretive scheme of the concepts resulting after we conducted the textual analysis with the help of MAXQDA, we were able to make assertions about the compatibly or lack of compatibility between the different discourses/stakeholders.

The first part of this chapter focused on mapping the discourses on bulk surveillance by discovering the most frequent frames or narratives. The second part of the chapter was more focused on the interpretive analysis and comparison of discourses, making different empirical claims about the discursive dynamics/relationships between the different stakeholders of the debate.

CONCLUSION

Bulk surveillance as a significant societal issue for democracies in the post-Snowden age

This study aimed to investigate the discursive construction of the issue of bulk surveillance as a societal topic in the UK after 2013, by focusing on the stakeholders involved in this process. The results indicate that the debate on bulk surveillance in the UK has been the driving force behind some important transformations of intelligence and its oversight, with significant implications for the democratic norms and mechanisms.

Analysing and bringing to light the existent discourses on bulk surveillance is a way to understand how the relationship between democracy and security in the UK is being reconfigured in the context of new and emerging technologies of surveillance. Therefore, the debate around the issue of bulk surveillance can be seen as a gateway towards a broader debate about the reconsideration of the role of intelligence actors and their oversight in a democracy, in the context of major technological advancements within the field of security. In other words, the way intelligence actors and their democratic oversight are adapting to these technological developments has normative and empirical consequences for democracy and human rights.

The Snowden revelations had a spill-over effect, setting in motion a myriad of long-term changes. Before the disclosures, the intelligence agencies in the UK have been exercising bulk surveillance powers 'in the dark', most often in the name of national security. After 2013 the UK intelligence actors moved from total secrecy to more transparency and openness, a crucial first step in subjecting bulk surveillance practices to democratic accountability. The debate on bulk surveillance at this level of complexity and scale represents a novelty for the British society. The post-Snowden landscape in the UK's regulatory field for intelligence and security has been characterised by a state of competing discourses on the issue of bulk surveillance. Therefore, this unprecedented debate offered

a valuable research opportunity of a societal issue with significant normative and practical impact on democratic norms and mechanisms.

Novelty of research

The expert debate on bulk surveillance at society level in the UK, provided a ground-breaking framework for researching the dynamics between intelligence and its democratic oversight in an advanced democracy. This framework for analysis was made possible mainly by the unprecedented discursivity and openness manifested by the intelligence community in the UK after 2013. The present study used discourse as framework for analysis and approached the topic of bulk surveillance from the normative angle of democratic intelligence governance.

An element of originality this thesis brings is the focus on intelligence from a critical-discursive perspective. Because intelligence actors are in general surrounded in secrecy, it is notoriously difficult to study them, especially from a discourse perspective. This study represents a novelty not only because of the topic but also because it examines an intelligence agency through discursive lenses. This was made possible by the specific context created in the aftermath of the Snowden revelations, in an advanced democracy, where intelligence actors have started for the first time ever in their history to speak publicly and openly about their collection practices.

The debate generated by the use of bulk surveillance technologies determined intelligence actors to engage into a complex discursive struggle taking place in the public sphere. In other words, the post-Snowden discursive context has lured intelligence community outside their traditional field of secrecy and positioned them in the highly unusual posture of speaker. In this sense, the current study examined key instances of GCHQ's public articulations such as policy documents, speeches, scholarly works of former practitioners and even a museum exhibition. Considering that GCHQ was not even officially acknowledged in law until 1994, the possibility to study their public communication and discursive strategy on the issue of bulk surveillance is noteworthy.

The Snowden disclosures hence, opened a window of opportunity for studying the discourse of some of the most important intelligence agencies in the democratic world. In this sense, a discursive research method can shed light on changes in the institutional behaviour of some intelligence actors post-2013. By employing the tool of discourse analysis for examining the debate on bulk surveillance in the UK, this study was able to

uncover some important transformations of both intelligence and its oversight. The study contributes to the burgeoning field of critical intelligence by demonstrating the importance of discursive analysis in exposing the monopolistic feature of the intelligence expert discourse.

Key Findings

1. *The debate on bulk surveillance had a transformative impact on the way intelligence community in the UK construe themselves in the public space, as part of the democratic framework.*

In the case of the intelligence discourse, we found that bulk surveillance is framed as a legitimate solution to security threats, as long as it is accompanied by strong safeguards and oversight mechanisms. By employing a discourse featuring references to oversight and proportionality, the intelligence actors manage to effectively defuse the critique of disproportionate surveillance. At the same time, they persuasively argue in favour of the absolute necessity of bulk surveillance in order to protect society.

The intelligence discourse focused on oversight and proportionality is complemented by two narratives: the first is that without bulk surveillance, intelligence agencies would not be able to properly protect society from potential dangers like terrorism and the second is that intelligence community have unmatched technological expertise on the issue of bulk surveillance. The technical language is a particular feature of the intelligence discourse and it is aimed at reinforcing the image of intelligence agencies as primary experts in the field of national security and technology and at rebuilding of public trust. As a specialist discourse, it requires translation into other narrative forms in order to have a public and societal impact. This explains the prevalence of some metaphors such as 'needle in the haystack' as part of this hegemonic expert discourse on bulk surveillance.

By articulating this specific discourse on bulk surveillance, the intelligence agencies in the UK, especially GCHQ, have been exposed to a transformative process, becoming discursive actors in the public sphere. Coupled with the language of human rights and democratic accountability, intelligence expert discourse is built on the idea that GCHQ has the best expertise to properly handle the complex technologies of bulk collection.

2. *References to human rights and democratic principles, represent a common discursive ground (nodal points) for all the stakeholders taking part in this expert debate, helping intelligence discourse to become hegemonic.*

The study showed that nodal points like "oversight" and "necessity and proportionality" are framed differently in each actor's case in order to fit different discursive strategies and goals. Hence, the study explained why some concepts have different meaning for different actors. To uncover the existing frames, we searched for the particular narrative elements in each actor's discourse.

The empirical section of the thesis revealed how discursive elements about democracy and human rights are now taking precedence over more traditional references to "national security" in the intelligence discourse on bulk surveillance. With the help of these nodal points the intelligence discourse has successfully framed bulk surveillance as compatible with the principles of human rights and democratic accountability. This framing has been combined with the specific narrative of bulk surveillance as an absolute requirement for protecting society from threats such as terrorism and with the specific narrative of unrivalled expertise of intelligence actors in using these technologies. As a consequence, the intelligence discourse on bulk surveillance has gained advantage in this public policy debate, becoming the hegemonic discourse. At the same time, it has become more resilient to the radical critique which frames bulk surveillance powers as fundamentally incompatible with human rights and democracy.

3. *The empirical analysis found important discursive similarities between civil society organisations, academia and oversight bodies*

The debate on bulk surveillance has determined a reinterpretation of democratic intelligence governance, highlighting the importance of expert oversight and of the oversight of power at the level of discourse. The empirical research of this study revealed significant discursive overlap between civil society organisations, academia and oversight bodies. The highest thematic compatibility was found between civil society and academia, with frequent particular references to chilling effects of bulk surveillance and technology as a threat to human rights.

From a normative perspective, both discursive articulations frame bulk surveillance as a direct threat to human rights and democratic participation, with freedom of expression and privacy rights deeply affected. The research also found a high degree of compatibility between civil society and oversight bodies' discursive structures and also that oversight bodies' discourse is influenced and adopts themes that are put forward by civil society organisations.

Implications and practical recommendations

The proper understanding of the highly complex technologies of intelligence collection has become a vital aspect of democratic intelligence governance. With intelligence discourse becoming hegemonic and thus more resilient to a radical contestation critique of bulk surveillance, democratic intelligence governance will require a form of constant oversight of power at the discursive level centred on contesting the intelligence actors' monopoly of expertise. Expert oversight institutions will benefit from collaborating with academia and civil society in order to be able to respond to the increased sophistication and complexity of new intelligence collection technologies based on big data and algorithmic reasoning and also to constantly challenge the dominance of the intelligence expert discourse in public sphere.

The input from scholars, especially interdisciplinary and critically engaged scholarly expertise must be properly integrated within the extended framework of democratic intelligence governance. One way to achieve this goal would involve organising institutionalised open forums and public platforms to bring together academics from diverse fields of knowledge like social sciences, technology and information science and law. These forums should also be attended by independent oversight expert bodies and civil society actors in the field of human rights and surveillance. Although many of these expert oversight entities have access to classified information, it should not restrict their officials' collaboration with academia. On the contrary, oversight officials must forge channels of collaboration and work around these secrecy restrictions that are often artificially imposed by intelligence agencies. This last aspect is particularly important because multidisciplinary scholarly research can deliver transparent results and innovative insights on emerging technologies and practices from a fundamentally different standpoint to that of intelligence and security professionals.

By embracing a more diverse set of perspectives and modes of knowledge, democratic intelligence governance would be better equipped to face both present and future ethical, legal, and social challenges related to the use of controversial intelligence practices. Public platforms, such as discussions expert forums, can mobilize scholarly interventions on controversial issues like bulk surveillance, from the level of normative critique towards political articulation and policy improvement. In this way, and in the observed context of openness and widespread discursivity around new intelligence

practices, scholars can bring a diversity of epistemic perspectives in this increasingly important area of security policy.

Limitations of the study and recommendations for future research

The present study has some obvious limitations. First of all, the case-study focused on the UK may raise questions about generalisability. The UK case was selected based on the potential to provide the richest insight into the societal construction of the bulk surveillance phenomenon in a democratic framework. However, the resulting findings from studying an advanced democracy like the UK may not be applicable to young democracies with a less institutionalized civil society, among other factors.

Another weakness is the general scarcity of available data when studying the intelligence field, being notoriously difficult to study intelligence actors. Nevertheless, the discourse analysis employed in this research would have benefited from more data obtained through conducting direct interviews with experts representing the other stakeholders involved in this debate. The study only used textual data.

A further limitation of the study is the lack of coverage for the cooperation between the intelligence agencies and private sector in order to conduct bulk surveillance. The study did not include private companies as a stakeholder in the debate, treating this aspect sketchily. However, we believe that the relationship between the private sector and the state in facilitating bulk surveillance practices, would require ample investigation, potentially in a future study.

There are signs that the advent of intelligence and security technologies based on AI and how they will affect democracy and human rights, could be the topic of a similar societal debate in some advanced democracies like the UK. GCHQ released in 2021 a blueprint document addressed directly to British citizens which sketches major ethical considerations that will govern the UK's intelligence agencies' use of AI. Thus, future research on this subject will be able to build on the present study and its discursive examination of the debate on bulk surveillance.

The way in which the societal debate on bulk surveillance has been developing, signals a new era for intelligence and its oversight in advanced democracies, a reassessment of their role, design and modus operandi. The experience of taking part in a democratic societal debate could prove formative for both intelligence and oversight actors in the UK. Moreover, it can open the path towards a broader societal debate about the impact of

emerging surveillance technologies such as AI, on democracy and human rights. Last but not least, the debate on bulk surveillance in the UK can provide valuable lessons to other democracies about intelligence reforms and democratic intelligence governance in the context of rapid technological advancements.

BIBLIOGRAPHY

1. Allen, G., and Chan, T. (2017), "Artificial intelligence and national security", Belfer Center for Science and International Affaris, Harvard Kennedy School, Cambridge, https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf
2. Amoore L, and Raley R, (2017) ,"Securing with Algorithms: Knowledge, Decision, Sovereignty," *Security Dialogue* 48, no. 1, 8, https://doi.org/10.1177/0967010616680753
3. Anderson, D. (2015). *A Question of Trust – Report of the Investigatory Powers Review*. Independent Reviewer of Terrorism Legislation. https://terrorismlegislationreviewer.independent.gov.uk
4. Anderson, D. (2016). *Report of the Bulk Powers Review*, Independent Reviewer of Terrorism Legislation, London https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf
5. Andregg, M. (2007). "Intelligence ethics: Laying a foundation for the second oldest profession". in *Handbook of intelligence studies* pp. 52-63. Routledge.
6. Angermuller, J. (2015), "Discourse Studies", In: Wright, James D. ed. *International Encyclopedia of the Social & Behavioral Sciences,* Second Edition. Amsterdam*:* Elsevier, pp. 510–515, https://doi.org/10.1016/b978-0-08-097086-8.03216-5
7. Aradau, C. (2015). "The signature of security: Big data, anticipation, surveillance". *Radical Philosophy*, 191, pp.21-28. https://www.radicalphilosophy.com/commentary/the-signature-of-security
8. Aradau, C. (2017), "Assembling (Non)Knowledge: Security, Law, and Surveillance in a Digital World," *International Political Sociology* 11, no. 4, pp. 327-342, https://doi.org/10.1093/ips/olx019

9. Aradau C, (2019), “Technology, agency, critique: An interview with Claudia Aradau”, in *Technology and Agency in International Relations*, edited by Marijn Hoijtink and Matthias Leese, London and New York: Routledge.
10. Aradau, C. and Blanke, T. (2015), “The (Big) Data-Security Assemblage: Knowledge and Critique,” *Big Data and Society*, 2(2). https://doi.org/10.1177/2053951715609066
11. Aradau, C., & Mc Cluskey, E. (2022a). "Critical Security and Intelligence Studies", in *A Research Agenda for Intelligence Studies and Government*, edited by Dover R., Dylan, H., Goodman M., pp.9-20, Cheltenham, UK: Edward Elgar Publishing, https://doi.org/10.4337/9781800378803.00007
12. Aradau, C., & Mc Cluskey, E. (2022b). “Making digital surveillance unacceptable? Security, democracy, and the political sociology of disputes”. *International Political Sociology*, 16(1), pp.1-19, olab024, https://doi.org/10.1093/ips/olab024
13. Bauman Z, Bigo D, Esteves P, Guild E, Jabri V, Lyon D (2014). ‘After Snowden: Rethinking the Impact of Surveillance’, *International Political Sociology*. June, vol. 8, No. 2, pp. 121-144.
14. Ben Jaffel, H, Hoffmann A, Kearns, O and Larsson S, (2020): “Collective Discussion: Toward Critical Approaches to Intelligence as a Social Phenomenon”, *International Political Sociology* 14, no. 3: pp.323–344, https://doi.org/10.1093/ips/olaa015
15. Bean, H, (2013) “Rhetorical and Critical/Cultural Intelligence Studies”, *Intelligence and National Security* 28, no. 3 495-519, doi: 10.1080/02684527.2012.699284.
16. Bean, H. (2018). “Intelligence theory from the margins: questions ignored and debates not had”. *Intelligence and National Security*, 33(4), pp. 527-540.
17. Bean, H., de Werd, P., & Ivan, C. (2021). “Critical intelligence studies: introduction to the special issue”. *Intelligence and National Security*, 36(4), pp.467-475.
18. Benson A. R (2021). “Interview – Rita Floyd.” E-International Relations, last modified May 2, https://www.e-ir.info/2021/05/02/interview-rita-floyd/
19. Bernal, Paul (2016) ‘Data gathering, surveillance and human rights: recasting the debate’, *Journal of Cyber Policy*, 1:2, pp.243-264
20. Bigo, D. (2006) ‘Protection. Security, Territory and Population’, in J. Huysmans, A. Dobson and R. Prokhovnik (eds) *The Politics of Protection. Sites of Insecurity and Political Agency*, London: Routledge, 84–100

21. Bigo, D. (2012),"Security, surveillance and democracy", in *Routledge Handbook of Surveillance Studies*, ed. Kirstie Ball, Kevin D. Haggerty and David Lyon Abingdon: Routledge
22. Bigo D. et al. (2013), "Mass Surveillance of Personal Data by EU Member States and Its Compatibility with EU Law," a study commissioned by the European Parliament
23. Bond, D. (2019, June 11). MI5 under fire for 'unlawful' handling of personal data. *Financial Times*. https://www.ft.com/content/986ebc26-8c49-11e9-a1c1-51bf8f989972
24. Bradford Franklin, S., & King, E. (2018). *Strategies for Engagement Between Civil Society and Intelligence Oversight Bodies*. Washington DC: Open Technology Institute, New America Foundation.
25. Bradford Franklin, S. (2020, January 29). Public engagement is key for robust intelligence oversight. *About:Intel*. https://aboutintel.eu/public-engagement-intelligence-oversight/
26. Bueger, C., & Mireanu, M., (2015), "Proximity", in *Critical Security Methods: New frameworks for analysis*, 1 edition., edited by Claudia Aradau, Jef Huysmans, Andrew Neal, and Nadine Voelkner, London and New York: Routledge
27. Byman, D., & Wittes, B. (2014). "Reforming the NSA: How to spy after Snowden". *Foreign Aff.*, 93, 127.
28. Cannataci, J. (2016), Statement by Mr. Joseph Cannataci, Special Rapporteur on the right to privacy, at the 71st session of the General Assembly, New York, 24 October, available at: https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=21240&LangID=
29. Cannataci, J. (2018a). *End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland*. United Nations, Office of the High Commissioner for Human Rights. https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E
30. Cannataci, J. (2018b). *Report to the Human Rights Council, A/HRC/37/62, Appendix 7 Working Draft Legal Instrument on Government-led Surveillance and Privacy*. United Nations, Office of the High Commissioner for Human Rights.

https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf

31. Caparini, M., & Born, H. (Eds.). (2007). *Democratic Control of Intelligence Services: Containing Rogue Elephants* (1st ed.). Routledge. https://doi.org/10.4324/9781315576442
32. Cate, F. H. and Dempsey J. X. eds. (2017) *Bulk collection: systematic government access to private-sector data*, New York, Oxford University Press
33. Clift, A.D. (2007). The Coin of Intelligence Accountability. In L. Johnson (Ed.), *Intelligence and Accountability: Safeguards against the Abuse of Secret Power, Strategic Intelligence* (vol. 5, pp. 165-182). Westport: Praeger Security International.
34. Cohen, E. D. (2014). "A History of the Mass Warrantless Surveillance Network". In *Technology of Oppression: Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance*, pp. 10-31. New York: Palgrave Macmillan US.
35. Corera, G. (2016). *Cyberspies*. Simon and Schuster.
36. D'Angelo, P. (2017). Framing: Media Frames. In P. Rössler, C. A. Hoffner, & L. van Zoonen, *The International Encyclopedia of Media Effects* (pp. 1-10). John Wiley & Sons Inc.
37. Davies, Philip H.J., (2010), "Britain's machinery of intelligence accountability: Realistic oversight in the absence of moral panic", in *Democratic oversight of intelligence services*, edited by Baldino, D., pp.133-160, Federation Press.
38. De Werd, P.G. (2018), *Critical Intelligence: Analysis by Contrasting Narratives*, PhD Dissertation, Utrecht University Repository, https://dspace.library.uu.nl/handle/1874/373430
39. Deacon, D. (2007). Yesterday's papers and today's technology: Digital newspaper archives and 'push button' content analysis. *European Journal of Communication*, *22*(1), 5-25. https://doi.org/10.1177%2F0267323107073743
40. Defty, A. (2020). "From committees of parliamentarians to parliamentary committees: comparing intelligence oversight reform in Australia, Canada, New Zealand and the UK". *Intelligence and National Security*, 35(3), pp.367-384.
41. Deleuze, G. (1992) "Postscript on the Societies of Control." *October*, Winter, vol.59, pp.3-7

42. Der Derian, J. (1993), “Anti-diplomacy, intelligence theory and surveillance practice”, *Intelligence and National Security* 8, no. 3: 29-51, doi: 10.1080/02684529308432213
43. Dewey C. (2013), How the NSA spied on Americans before the Internet, *The Washington Post*, https://www.washingtonpost.com/news/the-switch/wp/2013/08/23/how-the-nsa-spied-on-americans-before-the-internet/
44. Donohue, L. K. (2017), “The Case for Reforming Section 702 of U.S. Foreign Intelligence Surveillance Law”, Council on Foreign Relations, https://www.cfr.org/report/case-reforming-section-702-us-foreign-intelligence-surveillance-law
45. Dover, R., Dylan, H., & Goodman, M. S. (2022). "Introduction to A Research Agenda for Intelligence Studies and Government", *A Research Agenda for Intelligence Studies and Government.* Cheltenham, UK: Edward Elgar Publishing.
46. Electrospaces.net (2014), ‘INCENSER, or how NSA and GCHQ are tapping internet cables’, Nov 29, available at: https://electrospaces.blogspot.com/2014/11/incenser-or-how-nsa-and-gchq-are.html
47. Electrospaces.net (2016), ‘A perspective on the new Dutch intelligence law’, Dec 16, available at: https://electrospaces.blogspot.com/2016/12/a-perspective-on-new-dutch-intelligence.html
48. Entman, R. M. (1993). Framing: Toward clarification of a fractured paradigm. *Journal of Communication, 43*(4), 51–58. https://doi.org/10.1111/j.1460-2466.1993.tb01304.x
49. Evans, Hayley (2018) Summary: The U.K. Court of Appeal Ruling and What’s Next for the Investigatory Powers Act, February 6, available at: https://www.lawfareblog.com/summary-uk-court-appeal-ruling-and-whats-next-investigatory-powers-act
50. Ferguson B. W., (2005), “Exhibition rhetorics: material speech and utter sense”, in *Thinking about exhibitions*, ed. Reesa Greenberg, Bruce W. Ferguson and Sandy Nairne, London and New York: Routledge
51. Fleischaker, J. (2014,). Mapping the language we use to describe surveillance. Melville House. https://www.mhpbooks.com/mapping-the-language-we-use-to-describe-surveillance/

52. Fleming, J. (2021). “We have a chance to build a consensus on AI rules and norms.” *Financial Times*, February 24, https://www.ft.com/content/c05e1d70-63c2-4868-946c-f8b613a0dd77.
53. Flick, U. (2009) *An Introduction to Qualitative Research*, (4th ed.). Sage Publications Ltd, London
54. Floyd R, (2019), *The morality of security: a theory of just securitization*, Cambridge: Cambridge University Press
55. Foucault, M., (1980), “Two Lectures,” in *Power/knowledge*, New York: Pantheon, 78-108
56. Friedewald, Michael; J. Peter Burgess; Johann Čas; Rocco Bellanova; & Walter Peissl, (eds.), (2017) *Surveillance, Privacy and Security. Citizens’ Perspectives*. London: Routledge. PRIO New Security Studies
57. FRA (2015), European Union Agency for Fundamental Rights, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU Volume I: Member States’ legal frameworks* https://fra.europa.eu/en/publication/2015/surveillance-intelligence-services-volume-i-member-states-legal-frameworks
58. FRA (2017), European Union Agency for Fundamental Rights, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU Volume II: field perspectives and legal update*. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf
59. Gaskarth, J, (2020), *Secrets and Spies: UK Intelligence Accountability after Iraq and Snowden*, Washington, DC: Brookings Institution Press
60. GCHQ, “Pioneering a New National Security - The Ethics of Artificial Intelligence” (2021), https://www.gchq.gov.uk/files/GCHQAIPaper.pdf .
61. Gerring J (2004), "What is a case study and what is it good for?", *American political science review*, 98, no. 2, pp. 341-354, https://www.jstor.org/stable/4145316
62. Gibbs, Graham R. (2013) Using software in qualitative analysis. In: SAGE Handbook of Qualitative Data Analysis. Sage, London, UK, pp. 277-295
63. Gill, L. (2018). Law, metaphor, and the encrypted machine. *Osgoode Hall LJ*, 55, pp.440-477. http://dx.doi.org/10.2139/ssrn.2933269
64. Gill P. (2016), *Intelligence Governance and Democratization*, London and New York: Routledge

65. Gill, P. (2010) “Theories of Intelligence”, in *The Oxford handbook of national security intelligence*, edited by L.K. Johnson, Oxford: Oxford University Press
66. Gill, P. (2020). “Of intelligence oversight and the challenge of surveillance corporatism”. *Intelligence and National Security, 35*(7), pp.970-989. http://dx.doi.org/10.1080/02684527.2020.1783875
67. Gizzi, M. C., & Rädiker, S. (Eds.). (2021). The Practice of Qualitative Data Analysis: Research Examples Using MAXQDA. BoD–Books on Demand
68. Glaser, B.G., & Strauss, A.L. (1999). *The Discovery of Grounded Theory: Strategies for Qualitative Research* 1st ed.. Routledge. https://doi.org/10.4324/9780203793206
69. Goldman, Z. K., & Rascoff, S. J. (Eds.). (2016). *Global Intelligence Oversight. Governing Security in the Twenty-First Century*. Oxford: Oxford University Press.
70. Goldman, Z. K., (2016), “The Emergence of Intelligence Governance”, in *Global Intelligence Oversight. Governing Security in the Twenty-First Century* edited by Zachary Goldman & Samuel Rascoff, Oxford: Oxford University Press.
71. Granick, J, (2017), *American Spies: Modern Surveillance, Why You Should Care, and What to Do about It*, Cambridge; New York, Cambridge University Press
72. Greenberg, J., & Hier, S. (2009). CCTV Surveillance and the poverty of media discourse: A content analysis of Canadian newspaper coverage. *Canadian Journal of Communication*, *34*(3), 461–486. https://doi.org/10.22230/cjc.2009v34n3a2200
73. Gros,V. de Goede M,, and İşleyen, B, (2017), “The Snowden Files Made Public: A Material Politics of Contesting Surveillance”, *International Political Sociology* 11, no 1 73–89, https://doi.org/10.1093/ips/olw031
74. Haggerty K and Ericson R (2000) “The surveillant assemblage”. *The British Journal of Sociology* 51(4): pp.605–622
75. Haggerty, K. D. (2006). “Tear down the walls: on demolishing the panopticon”. In D. Lyon (Ed.), *Theorizing Surveillance* (1st ed, 23-46). London: Willan. https://doi.org/10.4324/9781843926818
76. Hajer, M. A. (1995). *The politics of environmental discourse: Ecological modernization and the policy process*. Clarendon Press.
77. Herman, M. (2001), *Intelligence services in the information age: theory and practice*, Frank Cass, London
78. Herschinger, E. (2011). *Constructing global enemies: hegemony and identity in international discourses on terrorism and drug prohibition*. Routledge

79. Hijmans, H., & Hijmans, H. (2016). Internet and Loss of Control in an Era of Big Data and Mass Surveillance. The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU, pp.77-123.
80. Hintz, A., & Dencik, L. (2016). The politics of surveillance policy: UK regulatory dynamics after Snowden. *Internet Policy Review, 5*(3), 1-16. http://dx.doi.org/10.14763/2016.3.424
81. Hoadley, D., and. Sayler,K, (2020), "Artificial Intelligence and National Security" | Report by the Congressional Research Service for members and committees of Congress, R45178, Library of Congress, https://crsreports.congress.gov/product/pdf/R/R45178
82. Holden, M. (2016). Parliamentary committee criticises surveillance bill over privacy concerns. *Reuters*. https://www.reuters.com/article/uk-britain-security-surveillance-idUKKCN0VI0UC
83. Hosein, G. (2017), 'The UK Investigatory Powers Act: A Bad Example for the World', *The Cipher Brief,* available at: https://www.thecipherbrief.com/article/tech/the-uk-investigatory-powers-act-a-bad-example-for-the-world
84. Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research, 15*(9), 1277-1288. https://doi.org/10.1177%2F1049732305276687
85. Iliadis A,,and Russo F. (2016),, "Critical Data Studies: An Introduction," *Big Data and Society*, July-December 2016 https://doi.org/10.1177/2053951716674238
86. *Investigatory Powers Act 2016*. https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted
87. Investigatory Powers Commissioner's Office (IPCO). (2017). Annual Report of the Investigatory Powers Commissioner for 2017. IPCO. https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCO-Annual-Report-2017-Web-Accessible-Version-20190131.pdf
88. Investigatory Powers Commissioner's Office. (2018a). *IPCO's Advisory Notice 1/2018: Approval of Warrants, Authorisations and Notices by Judicial Commissioners*. IPCO. https://www.ipco.org.uk/publication/ipco-publication/advisory-notice-1-2018/

89. Investigatory Powers Commissioner's Office (IPCO). (2018b). Annual Report of the Investigatory Powers Commissioner for 2018. IPCO. https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCO-Annual-Report-2018-final.pdf
90. Investigatory Powers Commissioner's Office, (2018c), "IPC invitation for submissions on issues relevant to the proportionality of bulk powers" (Investigatory Powers Commissioner's Office, London,), https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC_Submissions_on_bulk_powers.pdf
91. Intelligence and Security Committee of Parliament. (2015). *Privacy and Security: A modern and transparent legal framework*. Houses of Parliament. https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf
92. Intelligence and Security Committee of Parliament. [ISC] (2016). *Report on the draft Investigatory Powers Bill*. Houses of Parliament. https://isc.independent.gov.uk/wp-content/uploads/2021/01/20160209_ISC_Rpt_IPBillweb.pdf
93. Ish-Shalom P. (2015). "Away from the heart of darkness: transparency and regulating the relationships between security experts and security sectors" in *Security Expertise: Practice, Power, Responsibility*, 1 ed., ed. Trine Villiumsen Berling and Christian Bueger (London and New York: Routhledge,
94. Ivan, C., Chiru, I., & Arcos, R. (2021). "A whole of society intelligence approach: critical reassessment of the tools and means used to counter information warfare in the digital age". *Intelligence and National Security*, 36(4), pp.495-511.
95. Jabri, V. (2006). War, Security and the Liberal State. Security Dialogue, 37(1), 47–64. doi:10.1177/0967010606064136
96. Jäger, S. and Maier, F. (2009). "Theoretical and methodological aspects in Foucauldian critical discourse analysis and dispositive analysis". In R. Wodak and M. Meyer (eds.), *Methods of Critical Discourse Analysis*, 2nd edn. London: Sage. pp. 34-61
97. Jasanoff, S. (2016). *The ethics of invention: technology and the human future*. New York: WW Norton & Company.
98. Jeffreys-Jones, R. (2017) *We Know All About You: The Story of Surveillance in Britain and America*, Oxford, UK: Oxford University Press
99. Johnson, L. K. (2017). *Spy Watching: Intelligence Accountability in the United States.* Oxford University Press.

100. Keller, R. (2013). *Doing discourse research: An introduction for social scientists*. SAGE Publications, https://dx.doi.org/10.4135/9781473957640

101. Keller, R., Hornidge, A. K., & Schünemann, W. J. (Eds.). (2018). *The Sociology of Knowledge Approach to Discourse: Investigating the Politics of Knowledge and Meaning-making*. Routledge.

102. Kind, E. (2019). *Not a Secret: Bulk Interception Practices of Intelligence Agencies*. Center for Democracy and Technology. https://cdt.org/insights/not-a-secret-bulk-interception-practices-of-intelligence-agencies/

103. Krieger, W. (2009). Oversight of Intelligence: A Comparative Approach. In G. F. Treverton & W. Agrell (Eds.), *National Intelligence Systems: Current Research and Future Prospects*. Cambridge, Cambridge University Press.

104. Kuehn, K. M. (2018). Framing mass surveillance: Analyzing New Zealand's media coverage of the early Snowden files. *Journalism, 19*(3), 402–419. https://doi.org/10.1177/1464884917699238

105. Laclau, E. & C. Mouffe (2001), *Hegemony and Socialist Strategy: Towards a Radical Democratic Politics*, London: Verso

106. Lane, K., Lindsay, D., & Vaile, D. (2016). Australian Privacy Foundation: Submission to Review of Access to Retained Data in Civil Proceedings. Australia: Australian Privacy Foundation

107. Laperruque, J., (2018), "After 'Foreign Surveillance' Law, Congress Must Demand Answers from Intelligence Community", https://www.pogo.org/analysis/2018/01/after-foreign-surveillance-law-congress-must-demand-answers-from-intelligence-community

108. Leigh, I. (2019). Intelligence law and oversight in the UK. In J.H. Dietrich and S. Sule (Eds.), *Intelligence law and policies in Europe* (pp. 535-585). Oxford: Hart Publishing.

109. Liberty (The National Council for Civil Liberties) (2016), Liberty's submission to the Terrorism Reviewer's Review of Bulk Powers, July, London, available at: https://www.libertyhumanrights.org.uk/sites/default/files/campaigns/resources/Liberty%27s%20submission%20to%20the%20Terrorism%20Reviewer%27s%20Review%20of%20Bulk%20Powers.pdf

110. Liberty. (2019). *MI5 "unlawfully" handled bulk surveillance data, liberty litigation reveals.* https://www.libertyhumanrights.org.uk/issue/mi5-unlawfully-handled-bulk-surveillance-data-liberty-litigation-reveals/

111. Lobban, I. (2013) Uncorrected transcript of public evidence before the UK's Intelligence and Security Committee Given by Sir Iain Lobban Director, Government Communication Headquarters Mr Andrew Parker Director General, Security Service Sir John Sawers Chief, Secret Intelligence Service (ISC), 7 November, https://isc.independent.gov.uk/wp-content/uploads/2021/01/20131107_ISC_uncorrected_transcript.pdf

112. Logan, S. (2017). "The needle and the damage done: Of haystacks and anxious panopticons". *Big Data & Society*. https://doi.org/10.1177/2053951717734574

113. Lomas, N. (2016). UK Surveillance Powers Bill Slammed for Privacy, Clarity and Targeting Failures. *TechCrunch*. https://techcrunch.com/2016/02/09/uk-ip-bill-slammed-for-privacy-clarity-and-targeting-failures/

114. Lubin, Asaf (2018), 'Legitimizing Foreign Mass Surveillance in the European Court of Human Rights', *JustSecurity*, https://www.justsecurity.org/59923/legitimizing-foreign-mass-surveillance-european-court-human-rights/

115. Lund Petersen K., (2019), "Three concepts of intelligence communication: Awareness, advice or co-production?", *Intelligence and National Security* 34, no. 3, 317-328, https://doi.org/10.1080/02684527.2019.1553371

116. Lyon, D. (2001) Surveillance Society: Monitoring Everyday Life (Issues in Society), Milton Keynes: Open University Press

117. Lyon D (2014) Surveillance, Snowden, and Big Data: capacities, consequences, critique, *Big Data & Society* *1*(2): https://doi.org/10.1177/2053951714541861

118. MacAskill et. al, (2013), 'GCHQ taps fibre-optic cables for secret access to world's communications', *The Guardian*, 21 Jun, available at: https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

119. Mann, Monique (2018), Privacy in Australia: Brief to UN Special Rapporteur on Right to Privacy, The Australian Privacy Foundation, available at: https://privacy.org.au/wpcontent/uploads/2018/08/Privacy-in-Australia-Brief.pdf

120. Marin, Luisa (2017), 'The deployment of drone technology in border surveillance: between techno-securitization and challenges to privacy and data protection' in Friedewald, Michael; J. Peter Burgess; Johann Čas; Rocco Bellanova; & Walter Peissl, eds,, Surveillance, Privacy and Security. Citizens' Perspectives. London: Routledge. PRIO New Security Studies

121. Marquis-Boire M, Greenwald G, Lee M, (2015), "XKEYSCORE NSA's Google for the World's Private Communications", *The Intercept*, https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/

122. Marres N, and Lezaun J., (2011) "Materials and Devices of the Public: An Introduction", *Economy and Society* 40, no. 4 489–509, https://doi.org/10.1080/03085147.2011.602293

123. Moran, J, and Walker C, (2016), 'Intelligence Powers and Accountability in the U.K.', in *Global Intelligence Oversight: Governing Security in the Twenty-First Century*, edited by Zachary K. Goldman, and Samuel J. Rascoff, pp.289-314, New York, , https://doi.org/10.1093/acprof:oso/9780190458072.003.0012

124. Müller, M. (2011). "Doing discourse analysis in critical geopolitics", *L'Espace Politique. Revue en ligne de géographie politique et de géopolitique*, (12)

125. Murray, D., & Fussey, P. (2019). 'Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data' *Israel Law Review*, 52(1), pp.31-60

126. Murray, D., and Fussey, P., (2021), "GCHQ's ethical approach to AI: an initial human rights-based response." about:Intel,, https://aboutintel.eu/qchq-ethics-ai/

127. National Academy of Sciences [NAS Report] (2015), *Bulk collection of signals intelligence: technical options Committee on Responding to Section 5(d) of Presidential Policy Directive 28*, Washington DC The National Academies Press

128. Newbery, S, and Kaunert C. (2023): "Critical Intelligence Studies: A new framework for analysis." *Intelligence and National Security* pp.1-19.

129. Ni Loideain, N. (2019), 'A Bridge too Far? The Investigatory Powers Act 2016 and Human Rights Law' in Edwards, L. (ed.), *Law, Policy and the Internet*, London, Hart Publishing

130. Omand, David (2010), *Securing the State*, London, Hurst Publishing

131. Omand, D., & Phythian, M. (2018). *Principled Spying – The Ethics of Secret Intelligence.* Oxford, Oxford University Press

132. O'Neil, P, (2007), "The curatorial turn: from practice to discourse", in *Issues in curating contemporary art and performance*, ed. Judith Rugg and Michèle Sedgwick, Bristol and Chicago: Intellect

133. Open Rights Group. (2016, February 9). ORG responds to the intelligence and security committee report into the investigatory powers bill. *Open Rights Group*. https://www.openrightsgroup.org/press-releases/intelligence-and-security-committee-report-investigatory-powers-bill/

134. Operational Case for Bulk Powers (2016), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf

135. Ortega-Alcázar, I. (2012). Visual research methods. *International Encyclopedia of Housing and Home*, (pp. 249–254), https://doi.org/10.1016/B978-0-08-047163-1.00693-7

136. Pfefferkorn, R. (2018), *Security Risks of Government Hacking*, Stanford Center for Internet and Society, Stanford

137. Phythian, M, (2008) "Intelligence Theory and Theories of International Relations: Shared World or Separate Worlds?" in *Intelligence Theory: Key Questions and Debates*, 1 ed., ed. Peter Gill, Stephen Marrin, and Mark Phythian, London and New York: Routledge.

138. Phythian, M, (2019), "Framing the Challenges and Opportunities of Intelligence Studies Research" in *Researching national security intelligence: multidisciplinary approaches* edited by Coulthart, S., Landon-Murray, M., & Van Puyvelde, D., Georgetown University Press.

139. Privacy International (2016), 'Bulk powers in the Investigatory Powers Bill: The Question of Trust Remains Unanswered', London

140. Privacy International (2017), How Bulk Interception Works, available at: https://privacyinternational.org/explainer-graphic/140/how-bulk-interception-works

141. Quinlan, M. (2007). Just Intelligence: Prolegomena to an Ethical Theory. *Intelligence and National Security*, *22*(1), 1–13. https://doi.org/10.1080/02684520701200715

142. Quinn, C., (2015), 'Surveillance, bulk data collection and intelligence. Interview with Bruce Schneier', Strife, available at: http://www.strifeblog.org/2015/06/05/surveillance-bulk-data-collection-and-intelligence-interview-with-bruce-schneier/

143. Quinn, B., and Sabbagh, D. (2019) "GCHQ aims to attract recruits with Science Museum spy exhibition." *The Guardian,* July 9, https://www.theguardian.com/uk-news/2019/jul/09/gchq-aims-to-attract-recruits-with-science-museum-spy-exhibition

144. Rein, M., and Schön D (1996), "Frame-critical policy analysis and frame-reflective policy practice," Knowledge and Policy 9, no. 1 85–104, doi: 10.1007/BF02832235

145. Renan, D. (2016). The FISC's Stealth Administrative Law. In Z. K. Goldman & S. K. Rascoff (Eds.), *Global Intelligence Oversight: Governing Security in the 21st Century* (pp. 121–140). New York: Oxford University Press.

146. Royal United Services Institute - RUSI. (2015). *A Democratic Licence to Operate: Report of the Independent Surveillance Review*. RUSI. https://rusi.org/publication/whitehall-reports/democratic-licence-operate-report-independent-surveillance-review

147. Ryk-Lakhman, Ira (2016), *The Investigatory Powers Act and International Law: Part I,* https://blogs.ucl.ac.uk/law-journal/2016/12/26/the-investigatory-powers-act-and-international-law-part-i

148. Schlanger M., (2015), "Intelligence Legalism and the National Security Agency's Civil Liberties Gap", *Harvard National Security Journal,* Vol. 6, pp.112-205

149. Schmid, A. (2004). Terrorism-the definitional problem. *Case W. Res. J. Int'l L.*, 36, pp.375-419.

150. Schneier, B. (2015), *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, W. W. Norton & Company

151. Schuster S, Melle B, Xabier L, Ton S, Ide-Kostic P, (2017), 'Mass surveillance and technological policy options: Improving security of private communications', Computer Standards & Interfaces, Volume 50, pp.76-82

152. Scott, P. (2019). "Hybrid institutions in the national security constitution: The case of the Commissioners". *Legal Studies*, 39(3), 432-454. https://doi.org/10.1017/lst.2018.44

153. Smith Ochoa, C., Gadinger, F., and Yildiz, T. (2021). "Surveillance under dispute: Conceptualising narrative legitimation politics". European Journal of International Security, 6(2), 210-232, https://doi.org/10.1017/eis.2020.23

154. Snow, D.A. (2008) Elaborating the discursive contexts of framing: Discursive fields and spaces. Studies in Symbolic Interaction 30, 3–28

155. Snow, D.A. (2013) "Discursive fields" in *The Wiley-Blackwell Encyclopedia of Social and Political Movements*, (eds D.A. Snow, D. Della Porta, B. Klandermans and D. McAdam). https://doi.org/10.1002/9780470674871.wbespm072

156. Snowden E, (2020) *Permanent Record* , New York: Picador

157. Solomon, M., (2006), "Norms of Epistemic Diversity," Episteme 3, no. 1-2 23-36, doi: 10.3366/epi.2006.3.1-2.23, 23

158. Strauss, A. and Corbin, J. (1998). *Basics of Qualitative Research*. London: Sage.

159. Ulnicane, I., Knight, W., Leach T., Carsten Stahl, B. and Winter-Gladys W, (2021) "Framing governance for a contested emerging technology: insights from AI policy", Policy and Society 40, no. 2, 158-177, doi: 10.1080/14494035.2020.1855800

160. United Kingdom Home Office (2016) "Operational Case for Bulk Powers" [Operational Case],: https://www.gov.uk/government/publications/investigatory-powers-bill-overarching-documents

161. United Kingdom Home Office (2016) *Bulk Personal Dataset Factsheet*, Document accompanying the Investigatory Powers Bill, March

162. United Kingdom Home Office (2016) *Equipment Interference Draft Code of Practice*, Document accompanying the Investigatory Powers Bill, March

163. UK Intelligence and Security Committee of Parliament (2016), Chair: The Rt. Hon. Dominic Grieve QC MP (ISC) *Report on the draft Investigatory Powers Bill*

164. UK Intelligence and Security Committee of Parliament [ISC] (2015) "Privacy and Security: A modern and transparent legal framework", London, March

165. UK Investigatory Powers Act 2016 (2016), available at: http://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf

166. UK Investigatory Powers Tribunal, (2016), *UKIPTrib 15_110-CH*, 17 October

167. UK Parliament, House of Lords, (2009) ‘’Surveillance: Citizens and the State - Constitution Committee Second Report’’ available at: https://publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1804.htm

168. UN (2007) *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, A/HRC/4/26,

169. UN (2014) *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson QC'* UN Doc A/69/397

170. Van Eijk, Nico, (2014), ‘’Mass surveillance: the Dutch state of denial’’, openDemocracy.net 16 May, available at: https://www.opendemocracy.net/can-europe-make-it/nico-van-eijk/mass-surveillance-dutch-state-of-denial

171. Vieth, K., & Wetzling, T. (2019). Data-driven Intelligence Oversight Recommendations for a System Update. Berlin, Heinrich-Böll-Stift

172. Wæver, O, (2015), “The History and Social Structure of Security Studies as a Practico-Academic Field”, in *Security Expertise: Practice, Power, Responsibility*, 1 ed., ed. Trine Villiumsen Berling and Christian Bueger, London and New York: Routledge.

173. Warrel H, and Fildes N, 2021, “Amazon strikes deal with UK spy agencies to host top-secret material.” *Financial Times*, October 25, https://www.ft.com/content/74782def-1046-4ea5-b796-0802cfb90260

174. Watt, E. (2017) *Cyberspace, Surveillance, Law and Privacy*. Doctoral thesis, University of Westminster

175. Watts Robert, and Winnett Robert (2013), ‘William Hague: British public have 'nothing to fear' from US spies’, The Telegraph, June 9, available at: https://www.telegraph.co.uk/news/politics/10108564/William-Hague-British-public-have-nothing-to-fear-from-US-spies.html

176. Wegge, N. (2017). “Intelligence Oversight and the Security of the State”. *International Journal of Intelligence and Counterintelligence*, 30(4), pp.687-700. http://dx.doi.org/10.1080/08850607.2017.1337445

177. Wetzling Thorsten, (2017), *Options for more Effective Intelligence Oversight*, Discussion Paper, SNV

178. Wetzling, T., & Vieth, K. (2018). *Upping the Ante on Bulk Surveillance An International Compendium of Good Legal Safeguards and Oversight Innovations*. Berlin, Heinrich-Böll-Stift.

179. Wong, H, (2019) "Science Museum exhibition reveals hidden history of GCHQ." Design Week, August 5, , https://www.designweek.co.uk/issues/5-11-august-2019/science-museum-gchq-exhibition/.

180. Yadron D., Granick, J. (2018), 'Government Hacking Makes Everyone Less Safe', ACLU, http://bit.ly/35RDTD8

181. Zegart, A. B. (2011). *Eyes on Spies: Congress and the United States Intelligence Community*. Washington DC, Hoover Press.

APPENDICES

App 1. key texts issued by ECtHR

Document title	Date issued	Actor (speaker)	Theme of the text	Relevant frames for the topic of bulk surveillance
Privacy International and Others v. the United Kingdom	2016	-parties' submissions (Civil Society; Executive/SIS) -ECtHR	-bulk hacking	-human rights -critical
Big Brother Watch and others v. United Kingdom (Grand Chamber Judgment)	2018	-parties' submissions (Civil Society; Executive/SIS) --ECtHR	-bulk interception communications data form service providers -intelligence sharing with foreign governments	-human rights -critical

App 2. key texts issued by the Oversight institutions and bodies / independent reviewers

Document title	Date issued	Actor (speaker)	Theme of the text	Relevant frames for the topic of bs
A question of trust—report of the Investigatory Powers Review	2015	Oversight	- assessing the legitimacy and legal grounding of bulk collection practices	-human rights -critical
Privacy and security: a modern and transparent legal framework	2015	- Oversight - Civil Society - Executive/SIS -Academia	- assessing the legitimacy and legal grounding of bulk collection practices	-justificatory -balance frame -human rights
Report on the draft Investigatory Powers Bill	2016	Oversight - Civil Society - Executive/SIS -Academia	- questioned the need for bulk equipment interference and asked for more privacy safeguards	-human rights -critical

Report of Bulk Powers Review	2016	Oversight	- assessing the necessity of bulk collection practices - presenting detailed case studies of operational scenarios provided by MI5, MI6, and GCHQ	-justificatory -human rights
OHCHR: End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland	2018	Oversight	-preliminary observations on the UK case and its progress -bulk powers and their oversight -intelligence sharing	-human rights
IPCO Annual Report 2017	2019	Oversight Civil Society	-oversight -bulk communications data -bulk personal datasets	-human rights -technocratic
IPCO Annual Report 2018	2020	Oversight Civil Society	-inspection methodology -oversight of bulk powers -surveillance legislation	-human rights -critical -technocratic
IPCO Annual Report 2019	2020	Oversight Civil Society	-inspection methodology -technology advisory panel	-human rights - technocratic
IPCO Annual Report 2020	2022	Oversight Civil Society	-inspection methodology -assessment of SIS	-human rights - technocratic

App 3. - key texts issued by Civil Society

Document title	Date issued	Actor (speaker)	Type of document	Relevant frames for the topic of bs
Reforming surveillance in the UK	2014	Civil Society	Policy paper	-critical -human rights

Two years after Snowden: Protecting human rights in an age of mass surveillance	2015	Civil Society	Report	-critical -human rights
A democratic licence to operate: Report of the Independent Surveillance Review	2015	Civil Society	Report	-justificatory -human rights
Bulk powers in the Investigatory Powers Bill: The Question of Trust Remains Unanswered'	2016	Civil Society	Report	-critical -human rights
Liberty's submission to the Terrorism Reviewer's Review of Bulk Powers	2016	Civil Society	Report	-critical -human rights
Liberty's briefing on "Report of the Bulk Powers Review"	2016	Civil Society	Report	-critical
Liberty's response to the Investigatory Powers Commissioner's informal consultation on bulk powers	2018	Civil Society	Report	-critical -human rights
Civil Society submission in Big Brother Watch v. the UK	2021	Civil Society	Legal	-critical -human rights

App 4. - key texts issued by Executive/SIS

Document title	Date issued	Actor (speaker)	Theme of the text	Relevant frames for the topic of bulk surveillance
National Security Strategy and Strategic Defence and Security Review 2015	2015	Executive/SIS	-National security -necessity of bulk collection technologies for intelligence	justificatory
Operational Case for Bulk Powers	2016	Executive/SIS	- explaining in detail the working and necessity of bulk collection technologies for intelligence and police	justificatory
Government Response to Pre-Legislative Scrutiny (Investigatory Powers Bill)	2016	Executive/SIS	-national security -oversight and safeguards	justificatory

			-Justifying the need for bulk surveillance	
Government submission to Big Brother Watch and Other v. the UK Judgment	2021	Executive/SIS	- National security threats -Justifying the necessity of bulk surveillance	justificatory
Pioneering a New National Security: The Ethics of Artificial Intelligence	2021	Executive/SIS	- attempting to establish an ethical framework to guide the future use of AI in intelligence collection	-justificatory -technocratic

App 5. - key texts issued by Academia

Document title	Date issued	Actor (speaker)	Type of document	Relevant frames for the topic of bulk surveillance
After Snowden: Rethinking the Impact of Surveillance by Zygmunt Bauman et al.	2014	Acad	Academic article	-critical
Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique by David Lyon	2014	Acad	Academic article	-critical
The (Big) Data-Security Assemblage: Knowledge and Critique by Claudia Aradau and Tobias Blanke	2015	Acad	Academic article	-critical -technology
Data gathering, surveillance and human rights: recasting the Debate by Paul Bernal	2016	Acad	Academic article	-human rights
Principled Spying: The ethics of secret intelligence by David Omand and Mark Phythian	2018	Acad SIS	Academic book	-justificatory -human rights
Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data by Daragh Murray and Pete Fussey	2019	Acad	Academic article	-human rights -critical

App 6. – The devised code system

1 Scientific knowledge	
2 targeted collection is always an alternative to bulk	9
3 bulk personal datasets	3
4 bulk acquisition	5
5 bulk EI	1
6 National security	2
7 Human rights (privacy & freedom of expression)	00
8 intertextuality	2
9 oversight and safeguards	42
9.1 improved oversight leads to more public confidence in SIS	1
9.2 need for expert oversight	1
9.3 need for independent oversight	6
9.4 enhanced judiciary	3
10 Democratic principles	8
10.1 chilling effects affecting democracy	0
10.2 need for public consent	4
10.3 rule of law	5
10.4 necessity and proportionality	34
10.5 need for transparency and openness	9
11 ECHR Art.8	8
12 security and intelligence services	7
12.1 intelligence expansion	3

12.2 intelligence sharing	2
12.3 GCHQ	3
12.4 SIS are responsible and compliant	9
13 Legal framework governing intelligence	4
13.1 dysfunctional intelligence legislation that needs change	3
14 Technology	
14.1 AI	
14.2 encryption as threat	1
14.3 big data	6
14.4 technology as threat to hr/security	9
14.5 metadata	5
14.6 technologically unfeasible	
14.7 tech advancements	2
14.8 technology as a solution to hr infringements	
15 bulk interception	8
16 bulk surveillance as threat	7
16.1 surveillance occurs at the gathering stage	
16.2 lack of effectiveness	
16.3 pervasiveness of state surveillance	3
16.4 low public trust	2
16.5 arbitrariness	4
16.6 ubiquity of data	
16.7 intrusiveness	7
16.8 Storage of bulk data is intrusive	0

16.9 secrecy and opacity	4
16.10 mass surveillance	4
16.11 Snowden revelations	8
17 bulk surveillance as solution	0
17.1 overseas threats	
17.2 efficiency resource-wise & less intrusive	4
17.3 tackling serious crime	7
17.4 assisting military operations	
17.5 counter espionage/interference	
17.6 cybersecurity	
17.7 counter terrorism	8
17.8 metadata is less intrusive	
17.9 threat discovery	4
17.10 only human examination is surveillance	
17.11 vital intelligence	3
17.12 bulk data vs targeted surveillance	
17.13 use of selectors makes it targeted	6
17.14 no possible alternatives to bulk collection methods	8
17.15 emerging threats	0
17.16 balancing security-liberty/privacy (trade-off)	