frontiers | Frontiers in Political Science

TYPE Original Research
PUBLISHED 30 May 2025
DOI 10.3389/fpos.2025.1543472

OPEN ACCESS

EDITED BY
Ben Wagner,
Delft University of Technology, Netherlands

REVIEWED BY
Jorge Constantino,
Delft University of Technology, Netherlands
Dalia Al Eisawi,
Princess Sumaya University for Technology, Jordan

*CORRESPONDENCE
Melanie Sofia Hartvigsen
melanie.hartvigsen@proton.me

RECEIVED 11 December 2024
ACCEPTED 21 April 2025
PUBLISHED 30 May 2025

CITATION
Hartvigsen MS (2025) How perceptions of raw data collection affect intelligence accountability: the Danish intelligence field. *Front. Polit. Sci.* 7:1543472. doi: 10.3389/fpos.2025.1543472

How perceptions of raw data collection affect intelligence accountability: the Danish intelligence field

Melanie Sofia Hartvigsen*

IntelHub, Center for War Studies, Department of Political Science and Public Management, Faculty of Business and Social Science, University of Southern Denmark, Odense, Denmark

The collection of raw data has become a central aspect of intelligence accountability. This study investigates the relationship between perceptions of raw data collection and intelligence accountability virtues within a coherent framework, aiming to provide a more comprehensive understanding of how intelligence accountability systems are prioritised and justified. The research combines discussions on the ethics of bulk collection of raw data and civil rights with the literature on intelligence accountability and applies this to the Danish case within an organisational fields framework. Empirically, the study draws on interviews and document analysis to examine how different actors within the Danish intelligence field understand and position themselves in relation to raw data collection. The findings demonstrate that actors adopt divergent positions on the collection of raw data, and that these positions shape their understandings of intelligence accountability and influence how they prioritise accountability systems. Furthermore, the study shows that support from political decision-makers for certain actors is decisive in determining the distribution of power within the intelligence field.

KEYWORDS

intelligence, accountability, raw data, civil society organisations, oversight, institutional logics, organisational fields, bulk collection

1 Introduction

In 2020, a spectacular case, involving the Danish Defence Intelligence Service (DDIS) and the Danish Intelligence Oversight Board (TET) emerged in the public domain, inciting a heated debate in Denmark regarding the DDIS' collection and sharing of raw data and intelligence accountability. The debate was initiated by a press release issued by the TET, which severely criticised DDIS. The TET asserted "(t)hat there is an inappropriate culture of legality within the management of DDIS and parts of the service, where the service's possible unjustified activities or inappropriate conditions are sought to be shelved, including by failing to inform the Oversight Board of matters relevant to its control" (Tilsynet med Efterretningstjenesterne [TET], 2020, p. 2 translation is my own). The primary focus of the criticism concerned the DDIS' collection and sharing of raw data and highlighted the risks of unauthorised and unjustified collection of data on Danish citizens. The press release had significant consequences for the DDIS, as five senior managers were released from duty by the Minister of Defence. Subsequently, the Ministry established a Special Commission comprising three county judges to investigate the allegations. In 2021, the Commission presented its findings, exonerating the senior managers from responsibility (Jølner et al., 2021), leaving

observers with questions about the TET's competence. Although the TET advocated for more resources and strengthened competency to effectively oversee the DDIS in connection with the press release, in 2023, the Ministry of Defence effectively denied the TET access to the raw data stored by the DDIS.[1] This decision was justified by the argument that the TET was never intended to oversee or control raw data; despite the fact that the TET had been overseeing raw data since its inception in 2014 and that several former Ministers of Defence had been aware of this practice without questioning it. In the context of intelligence, raw data is typically described as unprocessed information collected through various INT-disciplines, such as HUMIN, SIGINT, IMINT (Phythian, 2013), which is later analysed and transformed into intelligence products. As the term suggests, 'raw' denotes data that has not yet been interpreted or refined (Räsänen and Nyce, 2013). The bulk collection of raw data, collected through SIGINT, is argued to be effective for ensuring national security (Sorell, 2021) and is deemed essential for counter-terrorism efforts (Yoo, 2014). However it is not without controversy, as scholars (see for example Pulver and Medina, 2018; Friedman and Citron, 2024), legal bodies (HUDOC, 2021a; HUDOC, 2021b), and civil society organisations (Amnesty International, 2015; Transparency International, 2021) have raised concerns regarding potential violations of privacy rights. In alignment with these concerns, TET's criticism underscored the risks linked to the unjustified collection of raw data on Danish residents and stressed the importance of controlling such data (Tilsynet med Efterretningstjenesterne [TET], 2020).[2] Nevertheless, the potential implications of raw data collection and the importance of control measures were interpreted differently by the Minister of Defence, who stated that "as it is per definition not possible to determine whether the raw data includes information about individuals residing in Denmark, it is stipulated in the DDIS Act that the TET are not permitted to control the DDIS' collection and sharing of raw data."[3] Consequently, the Minister's divergent perspective on the nature of raw data ultimately influenced the TET's mandate to oversee DDIS.

This incident did not occur in a vacuum. Civil society organisations (CSOs) expressed frustration and outrage over both the incident and its outcomes, raising concerns about the risks of uncontrolled mass surveillance and the sharing of Danish citizens' data with third parties (Bech-Nielsen, 2023). As a result, the CSOs reached conclusions that diverged from those of the Ministry, particularly regarding the nature of raw data collection and the risks it poses. The case had profound consequences for most parties involved. The DDIS losts its top management, and its relationship with foreign services may have been damaged (Kaarsbo, 2021). The TET underwent reform, was denied access to raw data, stripped from its ability to communicate fully independently with the public, and the composition of the Board has been changed.[4] Political decision-makers involved faced allegations of incompetence and overreach of power (Eller and Tofte, 2023), and finally, the public was left with a pile of unanswered questions about the state of the Rule of Law and fundamental civil rights within their democracy.

The bulk collection of raw data has become central to the discourse on intelligence oversight and accountability. This debate has highlighted divergent interpretations of raw data collection, particularly concerning potential violations of civil rights, which have significant implications for the understanding and scope of intelligence accountability. Such discussions are not unprecedented. Public and scholarly debates about the implications of bulk collection,[5] raw data and the right to privacy have exploded in recent years, particularly after the Snowden revelations in 2013. Opponents of bulk collection of raw data emphasise the privacy concerns associated with the loss of control over data merely through its collection. In contrast, governments and intelligence agencies often argue that privacy is not compromised as long as the raw data is not accessed (Macnish, 2018).

Raw data, the fuel that powers the services' engine, and its collection is also a significant focus for intelligence accountability measures and legislative frameworks. Within the literature on intelligence accountability, data is frequently discussed in terms of personal data protection issues (see for example Leigh, 2012; Aden, 2018; Jansson, 2018). These discussions focus on the adequacy of legislation and formal oversight mechanisms, stemming from the perception of raw data as possessing subjective value. In this sense, all collected data, including raw data, should be subject to accountability measures carried out by authorised oversight bodies. However, studies of intelligence practices indicate that intelligence officers understand data as objective and interpretation-free bits and pieces of information collected and selected for analysis (Räsänen and Nyce, 2013; Rønn, 2022). The Danish case exemplifies these differing perspectives, which may ultimately affect the structuring and formalisation of accountability. To gain a comprehensive understanding of intelligence accountability, it is necessary to examine perceptions of raw data collection and intelligence accountability within a coherent framework. Accountability is a fundamental element in conferring legitimacy to authorities (Yauri-Miranda, 2021) and involves 'the obligation to explain and justify conduct' (Bovens, 2007, p. 450). Consequently, accountability pertains to justifiable conduct within a specific field or situation, and is inherently subjective. This study addresses accountability as the virtues of actors, rendering it a normative concept contingent upon a specific actor and context (Bovens, 2010). In the Danish intelligence context, particularly concerning DDIS, formal accountability measures primarily relate to the collection, storage, and processing of data, as the external oversight of DDIS is narrowly focused on ensuring compliance with Danish

1 The Ministry of Defence conducted an internal analysis and drew this conclusion. The analysis is classified, but an explanation of the conclusions took place during a parliamentary hearing (Forsvarsministeriet [Ministry of Defence], 2023).

2 The Danish intelligence oversight system in regard to DDIS primarily consists of TET, which monitors whether DDIS processes information about natural and legal persons in accordance with Danish law, the Parliamentary Committee on the Intelligence services, which operates under absolute confidentiality, and the executive.

3 Said during a parliamentary hearing (Forsvarsministeriet [Ministry of Defence], 2023, p. 3).

4 Amendments to the law were introduced on the 11th of June, 2024 (Justitsministeriet [Ministry of Justice], 2024). For a discussion on the implications of the bill, see for example Hartvigsen et al. (2024).

5 I use the term *bulk collection* to refer to the gathering of vast amounts of communications signals information. While this practice is often described as *mass surveillance*, the definition of that term remains contested. Therefore, in this article, I adopt the less normative and more descriptive term *bulk collection*.

legal provisions regarding the processing of information about natural and legal persons. By identifying understandings of raw data collection, we can infer actors' accountability virtues, namely, the desirable behaviour of government organisations and officials concerning when and how the collection and processing of raw data is perceived as justifiable and what accountability mechanisms are deemed relevant and important in this regard. Expressed perceptions of raw data collection thus provide critical insights into how various intelligence actors comprehend accountability and why conflicts regarding justifiable conduct may be inevitable. This case presents us with at least four important questions: (1) How do actors position themselves in terms of their perceptions of raw data collection? (2) How do these positions inform actors' perceptions of intelligence accountability virtues? (3) Which accountability understanding dominates the intelligence field and what are its societal implications? (4) What does this mean to future scholarly debates on intelligence accountability?

This paper aims to integrate discussions on the ethics of bulk data collection and civil rights with the literature on intelligence accountability and to apply this synthesis to the Danish case within an *organisational fields* framework. By operationalising the organisational field framework as an analytic tool, it becomes possible to identify the perceptions of raw data collection, how they inform accountability virtues and priorities, thereby identifying the dominating perceptions. This analytical framework facilitates three contributions: first, it elucidates the connections between perceptions of raw data collection and intelligence accountability and how they exist in a dynamic engagement between actors within the intelligence field and the political domain. Second, it offers an empirical example from one of the most digitalised societies in the world (Department of Economic and Social Affairs, 2020), showcasing the societal consequences of contested perceptions of raw data collection and their implications for intelligence accountability. Finally, it contributes to the intelligence accountability literature by challenging the prevalent assumption of turf wars between intelligence services and overseers, suggesting that accountability virtues are shaped by perceptions of raw data collection as a significant factor in conflicts among actors, rather than a resistance to the concept of accountability itself.

The remainder of this article is organised as follows: The next section outlines the theoretical and methodological frameworks employed in this study. The subsequent analysis focuses on examining the institutional logics of the three actors, which elucidates the connections between the perception of raw data and intelligence accountability virtues. The three actors under consideration are the DDIS, the TET and a consortium of CSOs. Finally, the findings will be discussed in terms of their societal and scholarly implications, followed by a conclusion.

2 Theoretical framework and methodological approach

This study explores perceptions of raw data collection and how they inform accountability virtues. The theoretical section addresses these two topics separately. The ethical approaches (control account and access account) for the collection of raw data are based on the literature on ethics and surveillance, whereas the approaches to intelligence accountability are based on the intelligence accountability literature as well as on public administration literature. Subsequently, the organisational field framework is elaborated as the analytical framework of this study.

2.1 Bulk collection and privacy: two ethical positions

There is no commonly accepted definition of the term *data*; however, within information system disciplines, data are commonly regarded as factual information that serves as the foundation for reasoning and discussion. That is, data are considered the raw material from which information is derived (as pointed out and criticised by Räsänen and Nyce, 2013). This idea has been challenged based on the argument that data is cultural, not natural, and needs to be generated, protected, and interpreted (Gitelman and Jackson, 2013). Moreover, the increasingly complex challenge of distinguishing between digital and real identities, as these are increasingly woven together with the growing digitalisation of societies (Søe and Mai, 2022), reflects the importance of how society understands data, the collection of data, and the use of data. Hence, the collection and processing of citizen data is not merely a matter of the right to control personal digital data, but also the right to "influence the construction of one's identity" (Søe and Mai, 2022, pp. 491–492). Along the same lines, human rights organisations, such as Amnesty International (2015) and Transparency International (2021), have advocated for greater attention to the problems of bulk collection, pointing to data as the enabler of creating detailed profiles of individual identities, hence as a potential violator of privacy rights.

> *It is the responsibility of the state to ensure that citizens are not subjected to arbitrary surveillance by authorities, intelligence services, and companies that can create a highly detailed picture of an individual's life by collecting sensitive personal data online* (Amnesty International, 2014 translation is my own).

In the context of national security concerns, it is frequently contended that the correct balance between security and civil liberties must be struck (see for example Born and Johnson, 2005; Leigh, 2012). This suggests that, to enhance national security, the bulk collection of data should be accepted as a method to identify threats before they materialise, which may, however, compromise civil liberties such as the right to privacy (Yoo, 2014; Sorell, 2021).

However, there is a distinction between the mere collection of data and the access to data. In philosophical literature, the issue of bulk collection and privacy has been discussed from two positions in particular. One position, the control account, posits that when one loses control over information (for example, when it is collected), it constitutes a loss of privacy (Inness, 1996). In this sense, privacy means that people have control over areas of their lives and that you lose that control as soon as you give it away (voluntarily or involuntarily), since you are no longer in charge of future dissemination of the information. Following this logic, the bulk collection of data of intelligence services necessarily constitutes a violation of privacy regardless of whether the data is accessed or not.

The other position, the access account, argues that a loss of privacy only occurs when the data is accessed. According to Macnish (2018), bulk collection of data is not a matter of privacy, as long as it is not

accessed; hence, in terms of privacy rights, bulk collection of data does not constitute a violation *per se*. However, other important issues are associated with the practice, such as a loss of security (people may feel vulnerable regardless of whether the collected data is accessed or not) and the *risk* that the data may be accessed. In other words, access or no access, the issues of bulk collection of data are related to whether people *understand* bulk collection as a threat to their privacy rights and the fact that their privacy rights may be violated in the future. Macnish further argues that such consequences may be even more severe on a societal scale than actual violations of privacy rights.

The distinction between these two positions is instrumental in elucidating the various understandings of raw data collection and their implications for the accountability virtues of actors. In the subsequent section, I will account for the intelligence accountability discussion and outline three relevant approaches to accountability.

2.2 Virtues of intelligence accountability

Accountability is broadly understood as the connector between legitimacy and state power (Bochel et al., 2015; Yauri-Miranda, 2021). In this sense, it serves as a core pillar for keeping powerholders in check and informing those governed about those who govern. Hence, accountability itself has value (Bovens, 2007). Within this broader understanding, it is important to distinguish between accountability mechanisms and virtues. Mechanisms are institutional arrangements and structures that govern public actors' behaviour, and virtues are perceived as positive qualities of accountable behaviour of organisations and individuals (Bovens et al., 2014). In this sense, accountability mechanisms provide legitimacy to public governance through regulatory frameworks and institutionalised structures that regulate public actors' behaviour through a relationship between an actor being accountable towards a forum and a forum that can pose questions and pass judgement (Bovens, 2010). The Intelligence Studies literature tends to adopt this approach, emphasising the extent to which accountability mechanisms are capable of maintaining accountability by scrutinising formal oversight mechanisms and legal frameworks (Hartvigsen, 2024). Accordingly, the literature tends to perceive intelligence accountability as leading to turf wars between an agent who does not want to be held accountable and a forum struggling to keep the actor accountable (Manjikian, 2016). However, we cannot understand the nature of accountability in a given context solely by focusing on the laws governing intelligence services and formally established intelligence oversight mechanisms, as argued in recent literature (Gill, 2020; Yauri-Miranda, 2021; Leon-Reyes, 2022; Kniep et al., 2023; Hartvigsen, 2024). Intelligence, like any other social phenomenon, is embedded in perceptions, practices, and power struggles (Ben Jaffel et al., 2020; Klein Goldewijk, 2021). This is where the idea of accountability as a virtue takes on importance.

The functionality of accountability mechanisms is enabled by virtues of accountable behaviour, which is closely linked to responsiveness, a sense of responsibility, and a commitment to transparent, fair, compliant, and equitable conduct (Considine, 2002; Koppell, 2005; Bovens et al., 2014). Accountability virtues are the conduct that flourishes within an organisation beyond the scope of external rules and regulations, and they reflect social constructions that are dependent on the institutional and political context as well as the nature of the respective actor (Bovens, 2010). In other words, virtues depend on the set of values of a given organisation. Accountability virtues give legitimacy to public organisations and officials, and in this manner, mechanisms and virtues are mutually complementary—one does not work without the other, and the accountability virtues of those actors involved in intelligene accountability practices are therefore crucial to understanding the nature of intelligence accountability in a given context. This comprises not only perceptions of intelligence services and formal oversight bodies but also actors such as CSOs, media, and scholars (Hillebrand, 2012; Dobson, 2019; Kniep et al., 2023; Yauri-Miranda, 2023). Since the aim of this paper is to show how understandings of raw data collection inform perceptions of accountability, accountability virtues are the focus of analysis.

Accountability exists at many levels and with various focuses. Hence, to try and understand actors' accountability virtues, it is useful to turn to predefined categories of accountability. I use the categories developed by Romzek and Dubnick (1987), as they are useful for understanding the desired and emphasised relationships among actors (Ejersbo and Greve, 2016). The three relevant categories are as follows:[6]

- Bureaucratic accountability is based on a logic of a relationship between a superior and a subordinate. It is an internal accountability system with a high degree of control and in which rules must be followed, including politically formulated objectives (Romzek and Dubnick, 1987; Ejersbo and Greve, 2016).
- A legal accountability system is based on a relationship between two autonomous parties in which one, mandated by law, oversees the other. In this sense, the accountability holder is external and there is a high degree of control (Romzek and Dubnick, 1987).
- In the political accountability understanding, the accountability holder is a key stakeholder with a low degree of control but with the ability to impose democratic pressure on government organisations. Such stakeholders include the public, CSOs and political decision-makers. The emphasis in this understanding of accountability is on openness, freedom of information and responsiveness, and the primary question is who the government organisation represents (Romzek and Dubnick, 1987).

These categories are described as accountability systems or standards, but it is important to note that I do not assess whether the *actual* intelligence accountability system (mechanisms) falls within either of the categories; I only use the categories to understand the *perceived* and *prioritised* accountability virtues of actors, meaning which accountability system does the actors orient themselves towards in their understanding of accountability and which accountability system is perceived as the most important in relation to raw data collection.

6 In Romzek and Dubnick's (1987) account there are four categories. The last one is professional accountability. However, this category is less relevant to the study of intelligence accountability, as the contemporary accountability thesis of rules and regulations does not fit well with placing the accountability responsibility solely in the hands of individual employees. Moreover, the analysis shows very limited emphasis of professional accountability.

2.3 Organisational fields as an analytical framework

To expose the inherent perceptions of raw data and how they inform intelligence accountability virtues, I employ the analytical framework from New Institutionalism (March and Olsen, 2013). This framework is centred on the concepts of institutional logics and organisational fields, which are instrumental in guiding the analysis. Organisational fields are characterised by the interactions among field actors, their structure, their logics, and the political environment (Scott, 1994). The study posits that the various organisations involved, both directly and indirectly, in intelligence accountability can be considered part of the same organisational field.[7] An organisational field, as delineated by DiMaggio (1983), consists of actors (organisations) that produce similar services or products, with the actors and their activities constituting the field. DiMaggio's work utilised the metaphor of the *battlefield* to illustrate the concept of organisational fields, emphasising the aspects of power and competition as drivers for institutional change. Consequently, these fields may not be stable, but are instead dynamic and constantly evolving.

The fundamental premise of this study is that interactions in an organisational field typically align with the field's dominant institutional logic, which shapes its development (Reay and Hinings, 2005). Reay and Hinings assert that institutional logics are the principles that shape the actions of field actors, that is, the belief systems of such actors and their related practices. The presence of competing institutional logics within a field implies that conflicts may occur as actors struggle to establish dominance. Stability in the field can only be achieved when one institutional logic is recognised as dominant (Hinings et al., 2003). This suggests that conflicting institutional logics can contribute to explaining policy stability or uncertainty, with change and development occurring only when the logics combine or unify. Identifying the various institutional logics operating within a field can help to elucidate how that field may (or may not) continue to develop, considering that the organisational field of intelligence encompasses various actors engaged with intelligence accountability. From this perspective, accountability is a particular form of organisational practice, informed by inherent values and beliefs. Moreover, in accordance with several recent arguments in Intelligence Studies, this *accountability field* consists of not only intelligence services and their formal overseers (mandated oversight bodies) but also informal overseers (see for example Van Puyvelde, 2013; Kniep et al., 2023; Yauri-Miranda, 2023). Consequently, the actors considered in this study comprise intelligence services, formal oversight bodies, and CSOs.

Institutional logics is defined by Thornton and Ocasio (1999) as belief systems that shape the understanding and actions of field actors over time. Institutional logics consist of values, beliefs, and institutional rules embedded in the practices of organisations. Values are relatively stable principles of significant importance for prioritisation and guidance of behaviour (De Groot and Thogersen, 2012; Krasny, 2020). In this study, these values are found in the concepts of accountability and security. Beliefs focus on specific objects, and are more specific than values. They refer to an acceptance that something is true regardless of whether this acceptance is based on facts (De Groot and Thogersen, 2012; Krasny, 2020). In this study, beliefs refer to the ethical considerations of field actors regarding raw data collection and rights, as exhibited by their core values and goals. Institutional rules are concrete practices that support the values and beliefs. In this analysis, the practices related to intelligence accountability priorities and raw data are analysed to elucidate attempts to emphasise organisational values and beliefs. Together, these elements constitute virtues of accountability.

2.4 Methods and ethics

The study employs a pattern-inducing methodology by collecting empirical data on the topic and identifying the logics associated with raw data collection and accountability. This was achieved through textual coding and analysis, demonstrating how beliefs are shaped by the specific logics of the organisations (Friedland and Alford, 1991; Reay and Jones, 2016). Textual elements were grouped into categories depicting how reality (raw data collection and accountability virtues) was presented (Phillips and Schrøder, 2005) in relation to the two ethical positions on raw data and privacy issues (Macnish, 2018) and the three accountability systems (Romzek and Dubnick, 1987). Furthermore, the organisational field was situated within the current political context to elucidate the power dynamics among actors in the field, thereby explaining change or stasis (Hinings et al., 2003).

The research drew upon a diverse array of sources of textual data, encompassing official publications, reports, public statements to the news media, and public consultation letters. These sources provided detailed insights into organisations' perspectives on raw data collection, associated concerns, opportunities, and accountability virtues, revealing the underlying logics of their beliefs. To enhance empirical validity, the textual analysis was complemented by in-depth qualitative interviews with representatives from DDIS, TET, and CSOs. This triangulation approach is a well-established method in Intelligence Studies to address the limitations of relying solely on interviews or publicly available data, which can present a misleading picture owing to secrecy (Van Puyvelde, 2018; Díaz-Fernández, 2023). Sixteen interviews were conducted: four with DDIS representatives, four with TET board members and secretariat staff, and eight with representatives from seven Danish CSOs. All interviewees from DDIS and TET were manager-level staff or board members, meaning that the perceptions derived from the interviews are exclusively expressed by the top management of the organisations. In this regard, the conclusions of this study cannot be assumed to reflect the perspectives of all organisational levels. However, as key carriers of their organisation's institutional logics, managers hold authority over critical aspects of organisational life and play a central role in articulating these logics to external audiences (Lounsbury et al., 2021). Moreover, interviewing lower-level staff in the DDIS or TET was not an option. Intelligence organisations typically conceal their organisational structures and personnel identities, with only top management publicly known (Díaz-Fernández, 2023); Denmark is no exception. Consequently, the interviewees were made available to me at the management level. Given the study's theoretical framework and interviewees' access to and knowledge of accountability practices and

7 See Ben Jaffel (2020) and Bigo (2019) for examples of operationalising the field concept in intelligence studies.

bulk data collection, this was considered appropriate for addressing the research question. The CSOs were identified by scrutinising public statements to media outlets, screening of public consultation letters to bills regarding intelligence issues, and through informal conversations with individuals close to the field. The scope of organisations includes labour unions, NGOs, and interest groups. Similar to the interviews conducted with the DDIS and TET, I interviewed individuals in leading positions or experts on the subject of intelligence accountability and raw data collection. These interviews are particularly valuable for identifying institutional logics, as language's expressive power serves as a crucial resource for accounts (Hammersley and Atkinson, 1995). The conclusions drawn from these interviews should be understood as snapshots of a specific moment in time. Conducting similar interviews at different points might have yielded different results, as institutional logics – and, by extension, the virtues of accountability and perceptions of raw data collection – are shaped by institutional and political contexts that evolve over time. The aim of this paper is not to generalise about particular understandings within specific organisations, but rather to demonstrate how perceptions of raw data collection can shape conceptions of intelligence accountability, potentially giving rise to conflicts over what constitutes justifiable conduct.

Through an interpretive analysis of perceptions of raw data collection, perceived and prioritised accountability virtues were identified. Subsequently, the significance of political factors in field conflicts was examined. To ascertain the logics of political decision-makers, I scrutinised textual data from media sources (where politicians in government have voiced their views) and parliamentary hearing transcripts on the topic. Understanding the intelligence field necessitates the consideration of political actors, as they establish the boundaries and possibilities for intelligence actors. The predominant (politically backed) logics in the intelligence field was identified by juxtaposing the logics of field-level actors with those of political decision-makers. This allowed me to explain the lack of substantial progress in this field. All the translations from Danish are my own.

To uphold the principles of research ethics, information was sent to organisational participants outlining the study's objectives, methodology, participating organisational actors, data processing, anticipated outcomes, the full interview guide, information about procedures for lodging complaints, and information about the ability to revoke consent in accordance with the Danish Code of Conduct for Research Integrity (Ministry of Higher Education and Science, 2014). All participants signed an informed written consent statement, and all participants remains anonymous.[8] A research ethics approval was not obtained for this study, because ethical approval prior to initiating research projects in Denmark is mandatory only for certain types of health research projects and projects involving laboratory animals. However, the present project received a statement from the Research Ethics Committee at the University of Southern Denmark, confirming that the project obeys Danish law (case no. 24/55575). Moreover, as the data collection included personal data, permission to commence data collection, storage, and processing was granted by the University of Southern Denmark Legal Services (notification no. 11.935).

3 Analysis

In the following analysis, I will flesh out the belief systems of the DDIS, TET, and CSOs, identifying their beliefs regarding raw data collection and how they inform actors' perceptions and priorities concerning intelligence accountability and associated practices.

3.1 DDIS: raw data and more data in the name of national security—trust us, we have got this

The DDIS, the Danish foreign intelligence service, was established in 1967, but the organisation was not placed on a statutory footing until 2013. Prior to this, oversight was mainly confined to executive control (Andersen et al., 2022). As the work of the DDIS has mostly been a black box to the public since its creation, public information about the service has been scarce. However, since 2016, the DDIS has regularly issued the publication Indblik [Insight], which provides the public with a peek inside the service.

The DDIS frames its core task as supporting decision-making concerning foreign and security policies (Forsvarets Efterretningstjeneste [DDIS], 2019, 2021, 2023). Furthermore, the service equals its efforts to the national security of Denmark:

> *The DDIS is the foreign intelligence service of Denmark, and it works – in secret and in the open – to protect Denmark and Danish interests in a changing world. Our knowledge and efforts – Denmark's security* (Forsvarets Efterretningstjeneste [DDIS], 2019, p. 8).

Along the same lines, the interviewees from the DDIS emphasised the role of the DDIS as securing Denmark against foreign threats, or as specifically framed by one intelligence official, the DDIS is a system-preserving organisation which must ensure the free society,[9] which showcases an institutional logic embedded within a state security logic that is specifically oriented towards safeguarding the nation-state and national interests as the core value and goal in accordance with *raison d'état* (Hartvigsen et al., 2024).

Within the organisation, raw data collection is perceived as a vital tool necessary for the performance of the core goal, as emphasised in the 2023 edition of Indblik:

> *For many years, the DDIS has been a high-tech and data-driven workplace. But in recent years, the importance of technology and particularly the way we handle data have become absolutely decisive for our work* (Forsvarets Efterretningstjeneste [DDIS], 2023 p. 7).

It is highlighted that the service thrives on information, continuously needs to keep up with technical developments, and

8 Anonymity is often a necessary condition when studying intelligence organisations. Furthermore, this study focuses on the organisation rather than the individual, rendering the identity of specific interviewees less significant in this context.

9 DDIS intelligence official at management level. Interview conducted in fall 2023.

"draws on all of it when the situation demands it" (Forsvarets Efterretningstjeneste [DDIS], 2023, p. 11). Raw data is the foundation of objective analyses and assessments that provide the basis for political decision-making. Thus, raw data collection is undeniably tied to the value and goal of safeguarding national security.

The prevailing belief regarding the characteristics of the collected data within the DDIS is that it is indeed *raw*. Moreover, the belief that collected data is raw, that it is in need of preparation, suggests that in order to be of any use, it needs human processing and interpretation (Søe, 2024), as emphasised in this quote:

> *The DDIS gathers large amounts of data, which rarely proves useful in its raw state. The data developers ensure that the data is aligned and systematised so that the analysts can easily find the relevant data* (Forsvarets Efterretningstjeneste [DDIS], 2019, p. 33).

This perception suggests an overall ideal of objectivity and raw data as unaffected by humans, while at the same time underscoring the need for the availability and accessibility of data. Furthermore, the focus in terms of the sensitivity of raw data is mainly on the post-collection processes, which means access to the data:

> *We collect large amounts of raw data from electronic communications daily, which our analysts can search to identify the specific data needed to build an intelligence image. There is significant focus on the procedures for searching through raw data, and for this reason, we conduct an almost exhaustive internal review of all searches related to Denmark* (Forsvarets Efterretningstjeneste [DDIS], 2021, p. 13).

The belief that raw data is in need of preparation to be useful and the extensive focus on access procedures suggests an organisational acceptance of the collection of raw data as vital for the organisational goal and as unproblematic until accessed. In other words, it is perceived as harmless prior to human preparation and interpretation, and the risk of future access with the intent of misuse receives little attention, as also emphasised by one former intelligence official interviewed in this study:

> *Collected material is merely data in a vast lake. It is so large, with so many entry points, that the only reasonable way to conduct oversight is to focus on what data has been used. If the data is untouched, it does not matter at all – it just needs to be there. There are capacities to access it if you have a court order.*[10]

This naturally leads to the question of intelligence accountability, as the collection of raw data is not believed to be problematic *per se*, whereas internal control mechanisms and guidelines regarding access ensure compliance with the law. In its publications, DDIS places considerable emphasis on outlining the compliance of its internal control and oversight measures with applicable legal provisions (Forsvarets Efterretningstjeneste [DDIS], 2019, 2021, 2023). The Service describes that there is a high level of education and awareness of the rules among employees and that the efforts are supported by a large number of internal procedures and self-checks. Such emphasis on and prioritising of internal accountability mechanisms largely resemble the *bureaucratic accountability* practice, which emphasises an internal accountability system with a high degree of internal control.

The reclusive nature of the DDIS does not mean that it is not subject to external control or oversight. The intelligence officials interviewed, as well as the publications, highlight the role of the TET in holding DDIS legally accountable as well as their political accountability obligations. These, however, take a subordinate position compared to the internal bureaucratic accountability measures. TET and legal accountability are mainly seen as an external control of the DDIS's own control but also as a potential challenge to the organisation's expertise and effectiveness.[11] Political accountability mostly consists of the Indblik publications. The series is thought to provide accessibility and dialogue by outlining DDIS' role, tasks, and organisation. The Indblik reports can be interpreted as an organisational practice with the aim of providing more transparency and openness towards the general public, thereby eventually contributing to the political accountability obligations of the DDIS.

> *We publish Indblik in order – as far as our special task allows – to give the public a comprehensive picture of who the DDIS is and what tasks we solve* (Forsvarets Efterretningstjeneste [DDIS], 2023 p. 7).

However, this is obviously a very controlled and one-way accountability practice, that is a practice with the purpose of creating a sense of awareness, understanding, and trust[12], as well as serving the purpose of justifying methods of bulk collection of raw data and the need for technological development. In a recent publication, the DDIS Head of Law and Management Support stated:

> *Although the DDIS works in secrecy, the Service and especially our field of work and knowledge are subject to great public attention. This entails a need to communicate, because if the DDIS does not communicate, a vacuum arises which others try to fill. Likewise, it is absolutely crucial for the public's trust in the DDIS that we are as transparent as possible* (Forsvarets Efterretningstjeneste [DDIS], 2023 pp. 43–44).

Hence, the organisational practice of publishing the Indblik series serves as a means to support organisational values and goals, as well as showcase bureaucratic accountability efforts.

In summary, the core value of the DDIS rests on the *raison d'état* concept, in which the bulk collection of raw data is perceived as a vital tool and is believed to pose no serious concerns prior to access. Accountability virtues align with the bureaucratic accountability understanding, in which internal control mechanisms are prioritised and mainly focus on access to raw data

10 Former DDIS intelligence official at management level. Interview conducted in fall 2023.

11 DDIS intelligence officials at management level. Interviews conducted in fall 2023.

12 For an outline of intelligence communication types, see Petersen (2019).

rather than collection, whereas external (legal and political) accountability measures are problematised or limited. The values and associated beliefs are further promoted in the Indblik series with the aim of informing the public and justifying practices that effectively provide the DDIS with a voice in the intelligence field that can be difficult to contest for external actors.

3.2 TET: raw data collection may jeopardise legal rights, and we are the safeguard against misuse (until the Minister says otherwise)

The TET came into existence on 1 January 2014 and is an independent oversight board consisting of five board members chaired by a High Court judge. A secretariat consisting of eight to ten employees assists the TET with the oversight task, which is limited to the part of the Danish services' work that involves the data of natural and legal persons in Denmark. Moreover, the TET has no mandate to issue sanctions or orders against the services but can merely express their opinions. It is up to the Minister whether they chose to follow the TET's recommendations (Koch, 2013). Since its inception, the TET has continuously voiced concerns regarding personal data collection and processing procedures within the services; nevertheless, several times, the Ministry of Justice has shown little willingness to accommodate these concerns (Andersen et al., 2022).

In alignment with the DDIS, the TET sees its core goal as protecting Denmark, but with a very different threat in mind: the internal threat that the very existence of intelligence services poses due to their secrecy and extensive mandate (Hartvigsen et al., 2024). The focus is on protecting Denmark's status as a nation governed by democratic principles and Rule of Law. This is emphasised by the interviewees from both the Board and the Secretariat[13] and is also stated in the 2022 annual report:

> *To carry out its important societal function, the DDIS is granted, by law, very broad powers and capabilities to gather data. To ensure the legal rights of individual citizens and businesses in Denmark, these extensive powers are counterbalanced by rules stating that the service may not direct its collection capabilities against individuals residing in Denmark without a court order* (Tilsynet med Efterretningstjenesterne [TET], 2023, p. 2).

In this way, security becomes a matter of *protecting rights*, with a special focus on the security of data collection and processing. In other words, the main value of the TET is the Rule of Law, as pointed out by one board member during the interviews, and the organisation perceives itself as the body legitimising the existence of the DDIS. That is, without the TET, the DDIS would have no legitimacy as a state organisation in a democratic society. This logic is also stated in the annual reports:

> *The oversight activities of the TET contribute to the legitimisation of the DDIS' operations by enhancing public confidence that the service's activities comply with the law* (Tilsynet med Efterretningstjenesterne [TET], 2024, p. 3).

Whereas the DDIS expressed beliefs that raw data was objective and harmless prior to human preparation and interpretation, with little attention to the inherent risks of the mere collection of raw data, the TET perceives raw data in different ways. The press release issued by the TET in 2020 was partly based on a disagreement between the DDIS and TET regarding the collection and processing of raw data. The TET did not believe that the DDIS handled raw data with the integrity required to secure citizens' rights (Fastrup et al., 2020). The importance of this was underscored by the Chair of the TET in his forewords in the 2021 Annual Report:

> *When the DDIS collects raw data, it is of significant importance that this data is handled in a manner that ensures that the integrity of the information is maintained even after collection. If this is not the case, it could jeopardise the legal rights of individuals, as the DDIS may not be able to comply with the deadlines set by a judge or the legally mandated timeframe for data deletion* (Tilsynet med Efterretningstjenesterne [TET], 2022, p. 6).

Thus, the TET does not oppose the collection of raw data, but strongly emphasises the risks it entails, particularly concerning potential future illegitimate access and processing. Hence, their beliefs about the collection of raw data align with the issues raised by Macnish (2018), who argues that the collection of raw data is not a violation of privacy rights (the access account); nevertheless, raw data must be subject to time stamping and deletion rules to decrease the risk of future violations of privacy rights.

Accordingly, the virtues of accountability within the TET seem to rest on the conceptualisation of *legal accountability systems*, that is, a relationship between two autonomous parties in which one oversees the other mandated by law. This also means that their interpretation of the alleged threat or risk associated with raw data is guided by law. However, this does not mean that if the law (or rather the interpretation of the law) changes, so will the organisational beliefs even though the organisation's practice will change. During an interview, one board member said that the TET does not have a policy, since the organisation's only task is to assess the legality of the services' conduct. Hence, there is also an ideal of objectivity in the TET, but this objectivity is not directed towards raw data and the interpretation of raw data, but rather towards the correct interpretation and implementation of the law. The Danish laws that govern intelligence services and mandate the TET are rather vague (Koch, 2023) leaving room for interpretation, which means that the ideal of objectivity is challenging to adhere to in practice.

This point is further highlighted by the events following the 2020 press release. The TET deemed it necessary for the public to be aware of critical conditions within the DDIS and, therefore, used the press release to inform (Tilsynet med Efterretningstjenesterne [TET], 2020), but potentially also to call for assistance (Hartvigsen et al., 2024). Since the establishment of the TET, the organisation has continuously expressed criticism of

13 Interviews with Board Members and employees at the Secretariat. The interviews were conducted in spring 2023.

some practices within the DDIS[14], but little political attention has been directed towards the issue. In this light, the 2020 press release can be understood as an attempt to influence the intelligence field. Following the Special Commission's acquittal of DDIS' responsibility—based on the interpretation that TET was not mandated to oversee raw data—TET suspended its oversight of DDIS' raw data collection until the government resolved the jurisdictional disagreement. In 2023, the Ministry of Defence issued a decision on the matter in alignment with the Special Commission, stating that the law mandating the TET was not to be interpreted as giving the TET mandate to oversee raw data (Forsvarsministeriet [Ministry of Defence], 2023). Following this, the Board adopted the new practice.

Although TET's practice adhered to the interpretation of the regulation by the Ministry of Defence, the TET's 2022 Annual Report suggests that the TET maintained its position on the regulation of raw data pointing to case law by the European Court of Human Rights (ECtHR):

> *…a restriction of the oversight of the DDIS in accordance with the Commission's interpretation would be contrary to the case law of the European Court of Human Rights in Big Brother Watch and Others v. The United Kingdom and Centrum för Rättvisa v. Sweden* (Tilsynet med Efterretningstjenesterne [TET], 2023, p. 28).

The statement is followed by an account of the Ministry's decision and ends with "the TET organises its oversight accordingly" (Tilsynet med Efterretningstjenesterne [TET], 2023, p. 28). It seems that the TET's beliefs regarding raw data hinge on the risk that the collection and processing of raw data may endanger citizens' rights and lean on the ECtHR case law to support its views. Although their accountability practices may have changed to comply with the interpretation by the Ministry of Defence regarding raw data, the statement in the 2022 Annual Report suggests that their beliefs regarding raw data collection and accountability virtues have not changed.

In summary, the core value of TET is the Rule of Law, and its goal is to ensure citizens' rights. The collection and processing of raw data are believed to pose a risk of violating privacy rights, whether or not the data has been accessed. Accountability virtues adhere to the legal accountability system in which external oversight is prioritised and seen as vital for the legitimacy of the DDIS, and which is informed by the legal interpretation of raw data and privacy rights by the ECtHR. In an attempt to promote these values and beliefs, the TET issued the 2020 press release, which underscored the importance of legal accountability regarding raw data, but it was heavily undermined by the Special Commission and later the Ministry of Defence, which forced the TET to alter their practice. However, in this case, the new practice does not seem to align with prevailing beliefs in the TET of virtuous accountability behaviour. The effort to advance the institutional logics of TET within the intelligence field was clearly unsuccessful and undermined.

3.3 CSOs: data is power, and we want to be left alone—but no one seems to care about what we think

Denmark has a strong civil society tradition, and civil society has influenced state development, as well as norms of citizenship and civil rights (Damgaard, 2003). Hence, civil movements and CSOs in the country have influenced societal progress (Reuter et al., 2014). Concerning intelligence issues, CSOs generally perceived the Danish services with doubt and distrust throughout the last half of the 20th century (Andersen et al., 2022). This was particularly due to the domestic intelligence service's (the Danish Security and Intelligence Service) persistent practice of registering Danish citizens solely on the grounds of legal political activity, although legal political activity is protected by the Danish Constitution. In addition, entire organisations, specifically a labour union for IT professionals, were put under surveillance in the 80s on the grounds of members' allegedly left-wing political orientations (Schmidt, 2009). After 9/11, the services gained a more visible role in Danish society (Andersen, 2016), yet contemporary public levels of trust in the agencies remain an open question.

CSOs have different goals depending on whether they are labour unions, human rights organisations, interest groups, and so on. Nevertheless, they have one common value as a collective umbrella for the interests they represent: the promotion of the democratic discussion. Such discussion includes pluralism and contestation so as not to be limited or restricted by certain world views or truths, as highlighted by interviewed representatives from several of the organisations.[15] This suggests that the common logic regarding security is that it is agonistic: security is political, and therefore it must be subject to and accepting of conflict between different visions of what security entails (Tulumello, 2021).

This is emphasised by many organisations in terms of arbitrary bulk collection of raw data, privacy rights, and civil rights in general. The issue is not only the handling and processing of raw data, but also its collection. In a collective open letter to the Danish parliamentarians prior to a vote on a law regarding the logging of telecommunications data, eleven Danish CSOs expressed their concerns:

> *We believe it is unacceptable that we should all be subject to suspicion and surveillance. A fundamental aspect of living in a free country is the ability to move freely and call whomever we chose without the state knowing about it* (Lemberh-Petersen et al., 2021).

In this way, these organisations challenge the access account approach held by both the DDIS and the TET (while keeping in mind that the TET perceives the future risks and societal implications posed by raw data collection in a more urgent manner than the DDIS) by pushing a different belief regarding the collection of raw data.

14 In several annual reports, the TET criticised the DDIS for unjustified searches in raw data and unjustified collection of data concerning individuals residing in Denmark (see for example Hiis, 2020; Tilsynet med Efterretningstjenesterne [TET], 2022, 2023, 2024).

15 Interviewees from four of the seven CSOs were explicit about this matter. Interviews conducted during spring 2024.

Amnesty International further underlines the belief that the collection of raw data constitutes a violation of fundamental rights:

> *A general and indiscriminate logging of the entire population constitutes a significant and serious violation of the right to respect for privacy, the protection of personal data, as well as freedom of expression and information. It exceeds what is strictly necessary or proportional for the purposes of crime prevention or the protection of national security and is therefore in conflict with international human rights standards* (Amnesty International, 2021).

There are, of course, variations in whether the organisations consider the collection of raw data a violation of privacy rights or a violation of citizens' fundamental rights in general, or whether they focus on the risks of violating privacy rights. In a public statement, the labour union PROSA points to the general problem of the bulk collection of raw data in terms of general democratic values, as well as to the risks of future violations.

> *There is nothing wrong with surveillance – as long as it is targeted and based on concrete suspicion. This is foundational for the Rule of Law. However, arbitrary mass surveillance of all citizens is a dangerous path, one we must do everything to prevent, as it goes directly against the values of our open society, which is built on trust and freedom. Big Brother technology and the cross-referencing of vast amounts of data about every single citizen can be misused – especially when we do not know how future governments will handle it* (Bertelsen, 2019).

Similar arguments were posed by the Danish Institute for Human Rights (Institut for Menneskerettigheder, 2022). The perception of raw data collection is based on both the control and access account. For some CSOs, collection in itself constitutes a violation of privacy, while others, who fall within the access account, heavily problematise the bulk collection of raw data, as they go against fundamental democratic values and also pose risks of future violations of privacy rights. The perceived severity of the risks is based on the belief that data is power. As one interviewee pointed out "data is power and those with access to data can influence society."[16] The idea is further elaborated by one employee from the Danish Institute of Human Rights:

> *The fight to protect our personal data is crucial because it concerns the human right to privacy. It is about safeguarding people's private sphere, typically against a state that is more powerful than the individual. Just as the state does not have the right to forcibly vaccinate you or enter your home without cause, it also cannot simply collect and use all kinds of information about you* (cited in Kølln, 2019).

Thus, the question of bulk collection of raw data is believed to be inherently political. Pluralism and contestation of the collection of raw data beliefs are also central to priorities regarding intelligence accountability among CSOs. The general perception of intelligence accountability in Denmark is that it is too secretive, and this has been the centre of the debate among CSOs. Already in 2013, prior to the parliamentary vote on the establishment of the TET, Amnesty International pointed out that the proposed oversight structure would restrict parliamentary and public debate on intelligence matters (Amnesty International, 2013). This perception was further pushed in the public debate following the TET's press release and the recent debate prior to a reform of the intelligence oversight system.[17] In a public consultation letter to the bill, the interest group Association for Legal Policy (Retspolitisk Forening in Danish) stated:

> *The Association for Legal Policy cannot recommend the proposed bill be adopted in its current form. It would only cement the unsustainable and democracy-weakening secrecy within the system, which, in these times of military rearmament marked by highly one-sided official worldviews and enemy images, is expected to become even more pronounced.* (Retspolitisk Forening, 2024).

The Association criticises the one-sided perspective regarding intelligence accountability, and other organisations have called for more public debates concerning intelligence accountability and oversight.[18] Evidently, intelligence accountability is perceived and framed as inherently political, which makes the public, CSOs, and parliamentarians from opposition parties stakeholders entitled to a voice in intelligence accountability and in the matter of how services collect and process raw data. In this sense, the accountability virtues of CSOs are based on the idea of a political emphasis on democratic dialogue, discussion, and contestation. This is also evident in their attempts to influence and challenge the traditional logics of the intelligence field. To support the values and beliefs regarding raw data, privacy rights and intelligence accountability, the main practices entail public consultation letters, engagement in public debates and attempts to spark debate.[19] However, these attempts to influence the institutional logics in the intelligence field are deemed to have little effect by actors. Three reasons are highlighted in this regard. First, the organisations experience a general indifference towards bulk collection of raw data by the general public (Kampmann, 2010; interviewee from PROSA). Second, there is a general perception that public consultation letters lead to no changes in proposed bills, as the drafts have already been politically agreed upon before the public hearings, as highlighted by several interviewees. Third, political willingness is limited, as pointed out by interviewees from Transparency International and an IT interest group, and stated by the Association of Legal Policy i 2012.

> *The fact is, unfortunately, that the way things are structured in Denmark requires a favourable signal from the services before anything can happen. Otherwise, the responsible ministers for the services wouldn't dare to do anything other than reject the criticism* (Elmquist, 2012).

16 Interviewee from an IT labour union. Interview conducted in winter 2023.

17 See for example Bertelsen (2020), Krog (2020), and Transparency International Denmark (2020).

18 See for example, the statement of the chair of Transparency International Denmark (cited in Bech-Nielsen, 2023).

19 Practices highlighted by CSOs interviewees. Interviews conducted during spring 2024.

In summary, the core collective value of CSOs is the upholding of democratic discussions and pluralism. Thus, the collection and processing of raw data is a political question, as it may directly violate democratic core principles and pose risks of future violations of privacy rights. In this sense, the data is directly related to power. Accordingly, prioritised accountability practices are framed as centred on political accountability, in which the public, CSOs, and parliamentarians are key stakeholders, which require democratic discussion and dialogue. The practices adopted to promote democratic discussions are mainly public consultation letters and engagement in public debate and dialogue. However, these practices are perceived to have little effect on the dominant logic in the intelligence field due to experienced political unwillingness, public indifference, and structural restraints.

4 Discussion: contestation of the dominating logic in the intelligence field fails to drive meaningful progress—is that a problem?

The analysis suggests that institutional beliefs regarding the collection of raw data vary among actors in the intelligence field and also inform their accountability virtues in different ways. The DDIS adopts the access account, which emphasises that privacy is only violated when the data is accessed, and, therefore, prioritises the bureaucratic processes focusing on how data is accessed and used in an attempt to ensure that the data collected is only used for legitimate purposes. The TET has a more nuanced approach to the collection of raw data: it emphasises the associated risks of violating privacy rights on the basis of international rules and legal norms in that regard. This belief informs their accountability virtues (which are also given by their legal mandate) in the sense that they believe that the oversight of raw data is necessary to ensure that future violations of privacy rights will not occur. Lastly, the CSOs believe that the collection and possession of raw data equals power and is therefore a political matter subject to contestation. Accordingly, this belief informs their accountability virtues, which focus on concerns over loss of privacy, unequal power balances, and on working to achieve transparency about surveillance programmes and bulk collection of data; these are virtues of political accountability, which prioritise public debates and public expectations.

The framework of organisational fields suggests that the presence of competing logics within a field may cause conflict among actors, as they struggle to establish their own logics as the dominant (Hinings et al., 2003). The analysis showed that competing logics exist in the intelligence field. These competing logics have contributed to escalating the conflict among actors, which has been simmering since 2014 and erupted in 2020 with the TET's press release and started the biggest Danish intelligence scandal in recent times. Hence, it is reasonable to say that the field has been characterised by uncertainty and conflict rather than stability. Accordingly, actors' efforts to push their own values and goals in the field have taken place through various means, as previously explained. Nevertheless, a general tendency has been shown in terms of the success (or lack thereof) of such efforts from the TET and CSOs. Attempts to influence the status quo have been met with rejection or minor attention from the executive and lawmakers, which brings the importance of the political into the struggles among actors in the intelligence field.

First, the TET's press release can be understood as an attempt to influence the intelligence field and challenge the institutional logic of the *raison d'état* held by the DDIS. The attempt was eventually met with an intelligence reform, which stripped the TET from its power of full independence to communicate with the public. Second, the effort of the TET to get the Minister of Defence to deal with the issue of raw data resulted in the TET being denied oversight of raw data and forced to alter their practice. Third, the efforts of CSOs to raise concerns in relation to bills and hence to further their own values and goals in the legal frameworks governing the intelligence field are generally experienced as gaining little attention from lawmakers, since laws are generally already agreed upon before public hearings. This point has also been argued in a study on the limited impact of public consultations in Denmark (Pedersen, 2021). Lastly, CSOs' efforts to raise public debate and awareness to put pressure on political decision makers are generally experienced as being met with little interest. Consequently, the practices of the TET and CSOs to further their own institutional logics have little impact on the intelligence field.

In general, the executive supports the beliefs of the DDIS in terms of perceptions of raw data collection, and hence, accountability virtues regarding prioritised accountability systems. When the TET ceased control with raw data until receiving clarity from the Ministry of Defence, the Ministry emphasised that the DDIS itself was obliged to ensure the legality of collection of raw data (quoted in Quass, 2022), that is, the bureaucratic accountability system was prioritised.

This framing of raw data by the Minister mirrors the access account which is also emphasised by the DDIS, without reference to the associated risks of future violations or the societal implications of citizens feeling surveilled. This indicates that the political decision makers fall in line with the institutional logics of the DDIS, which effectively situates the intelligence service in a rather powerful position in the field without much more effort than justifying its cause (*raison d'état*). In this sense, the institutional logic held by the DDIS must be assumed to be the dominant and most powerful logic because of what seems to be near-unwavering support from the political decision makers and the political shutdown of contestations regarding perceptions of raw data collection and intelligence accountability virtues.

Moreover, it is evident that the dominating institutional logic of raw data collection and its impact on privacy rights in particular and fundamental rights in general determine which intelligence accountability virtues are prioritised in society. In this context, the dominating logic faces no serious threats from other logics. Hence, bureaucratic accountability within the DDIS is maintained as the main accountability mechanism, which means that the virtues of accountability centre on the organisational integrity of the DDIS. It goes without saying that the internal processes of control are vital for adequate intelligence accountability, yet they cannot stand alone and must be complemented by strong external oversight mechanisms, as established in the intelligence accountability literature (see for example Born and Johnson, 2005; Born and Leigh, 2005; Gill, 2020). Without proper checks and balances, the services remain a democratic problem, and the risks of abuse and violations of citizens' rights remain an uncertain and open question. This ought to be a concern in any democratic

society that seriously considers its democratic values and principles.

In addition, the services' raw data collection must be subject to contestation and public debate. Otherwise, this may have several implications. First, the population may experience growing uncertainty and insecurity owing to fear related to bulk collection practices. The risks of societal consequences have been well established in the literature, which points to limitations on individuals' autonomy and choices as well as to changes in democracy itself (see for example Peissl, 2003; Maras, 2012; Bauman et al., 2014; Parsons, 2015). In the Danish context, however, there has been no widespread objection to the increased bulk collection of data, as pointed out by some CSOs. However, this does not imply that there are no concerns. A 2019 survey found that only one in five thought it acceptable for authorities to collect citizens' data without informing them (Jørgensen, 2019). And another survey from 2021 shows that 34 percent of respondents "are to a large or some extent concerned that public authorities are collecting data that they do not want the authorities to know about" (Larsen, 2021, p. 1) and that they have altered their behaviour due to concerns about surveillance.

Another serious societal implication of the limited debate about the collection of raw data is that parliamentarians may vote in favour of legislation which they do not fully understand. This seemed to be the case in 2013, when the Danish parliament adopted the legal framework for the DDIS, which enabled the service to collect raw data and disseminate it to third parties. It was later revealed that several parliamentarians were unaware of the law's implications, as the issue of raw data collection and dissemination had not been thoroughly discussed (Wolfhagen and Stræde, 2014).

With regard to the scholarly debate, which has mainly centred on the legal aspects of accountability and the formal structures of the oversight system, this study's analysis shows that to understand the nature of accountability in a given context, we also need to understand the political beliefs regarding raw data collection in relation to the beliefs of the actors in the intelligence field, how they inform virtues of accountability intelligence, and whether these are subject to contestation. The general scholarly focus on legal accountability in the intelligence field leads to unproportionate efforts towards the development of comprehensive legal frameworks and appropriate structures of formal intelligence oversight mechanisms and maintains a narrative of intelligence services not wanting to be held accountable while neglecting the aspects of accountability virtues, that is, how actors perceive and practice accountability. Accountability is inherently political, and actors provide accountability with meanings that align with their interests. Hence, accountability cannot be fully understood from a functional perspective, and we need to study each case to understand its general tendencies and specificities. Moreover, because of the rapidly developing technological abilities of the services, and since the bulk collection of raw data increasingly constitutes a core pillar of the services' work, attention towards and discussion of perceptions of raw data collection are vital for intelligence accountability matters, as they may inform how states decide to structure their accountability measures. Otherwise, there is a risk that scholarly discussions and progress on intelligence accountability may stagnate.

5 Conclusion

In conclusion, this study has demonstrated that actors within the intelligence field adopt diverging positions toward the collection of raw data and that these positions shape their understanding of accountability virtues and priorities. The DDIS's logic, centred on the access account, dominates the intelligence field, with significant support from political authorities who reinforce its bureaucratic accountability as a virtue and priority. In contrast, the efforts of TET and CSOs to introduce alternative logics focused on concerns regarding future violation of privacy and fundamental rights, as well as a prioritisation of legal and political accountability, have been largely marginalised, and their contestations have received limited political support or public attention.

Furthermore, the analysis highlights that the competing logics not only risk advancing conflict among the actors but also underscore the lack of a holistic approach to intelligence accountability, which may have serious consequences for society, including civic uncertainty and insecurity, political lack of understanding of the legislation which they pass, and organisational and reputational damage for the intelligence services.

In closing, I propose that future scholarly discussions broaden their scope beyond legal and formal oversight structures by considering the normative dimensions of intelligence accountability as articulated by a diverse array of stakeholders, including the intelligence services, oversight bodies, CSOs, the media, political decision makers and opposition parties in parliament. The findings of this study calls for a more profound investigation into the political beliefs that influence intelligence accountability systems, the perceptions surrounding raw data collection, and the societal implications of bulk collection of raw data. Absent of such critical engagement, academic discourse risks stagnation, thereby neglecting crucial aspects of intelligence accountability in an era characterised by rapidly advancing surveillance technologies.

Data Availability Statement

The datasets presented in this article are not readily available. The restrictions that apply to the data set are: (1) Anonymisation of interview participants. (2) Participants' prior approval of published quotes in the material restricts public access to the full dataset because unpublished quotes have not been approved by participants for public disclosure. (3) The dataset may contain material that is potentially subject to confidentiality obligations. Access to the dataset cannot be granted for the reasons outlined above.

Ethics Statement

Ethical review and approval was not required for the study on human participants in accordance with the local legislation and institutional requirements. The participants provided their written informed consent to participate in this study.

Author contributions

MH: Conceptualisation, Data curation, Formal analysis, Investigation, Methodology, Project administration, Resources, Writing – original draft, Writing – review & editing.

Funding

The author declares that financial support was received for the research and/or publication of this article. This study received funding from the Carlsberg Foundation, Semper Ardens: Accelerate grant.

Acknowledgments

I am very thankful for valuable comments on a previous version of the article from Kira Vrist Rønn and Sille O. Søe. In addition, I would like to thank the organisers and participants at the workshop 'Accountability and the use of technologies in intelligence & security sectors' for their valuable comments and discussions regarding the results of this paper as well as the subject in general. Finally, I wish to thank both reviewers for their thoughtful and constructive comments, which have significantly contributed to improving this paper.

Conflict of interest

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author declares that no Gen AI was used in the creation of this manuscript.

Publisher's note

References

Aden, H. (2018). Information sharing, secrecy and trust among law enforcement and secret service institutions in the European Union. *West Eur. Polit.* 41, 981–1002. doi: 10.1080/01402382.2018.1475613

Amnesty International Om forslagene til Folketingets Kontroludvalg med Efterretningstjenesterne, PET-tilsynet og om den manglende retlige regulering af brugen af civile agenter m.v., jf. Morten Storm-sagen [On the proposals to the Danish Parliament's Intelligence Services Control Committee, DSIS oversight, and the lack of legal regulation of the use of civilian agents, etc., cf. the Morten Storm case]. (2013). Available at: https://amnesty.dk/wp-content/uploads/media/1528/h__ringssvar_-_pet_kontrol_220113.pdf (Accessed September 24, 2024).

Amnesty International (2014) Staten skal sikre borgernes netsikkerhed [The state must ensure the citizens' cybersecurity], Amnesty International. Available online at: https://amnesty.dk/staten-skal-sikre-borgernes-netsikkerhed/ (Accessed October 18, 2023).

Amnesty International (2015) Does Your Country Share Your Data with the USA?, Amnesty International. Available online at: https://www.amnesty.org/en/latest/campaigns/2015/06/does-your-country-share-your-data-with-the-usa/ (Accessed January 10, 2024).

Amnesty International Amnesty Internationals bemærkninger til høring over udkast til forslag til lov om ændring af retsplejeloven og lov om elektroniske kommunikationsnet og -tjenester (revision af reglerne om registrereting og opbevaring af oplysninger om teletrafik (logning) m.v.) [Amnesty International's comments on the consultation regarding the draft proposal for a law amending the Administration of Justice Act and the Act on Electronic Communications Networks and Services (revision of the rules on the registration and retention of information on telecommunications traffic (logging), etc.)]' (2021). Available online at: https://amnesty.dk/wp-content/uploads/2021/10/Hoeringssvar-logning-2021.pdf (Accessed 24 September 2024).

Andersen, L. E. (2016) 'Denmark: From State Security to Security State. The Invention of Preventive Security', in GraaffB. de, J. M. Nyce and C. Locke (eds) The Handbook of European Intelligence Cultures. London: Rowman & Littlefield, pp. 95–108.

Andersen, S. J., Hansen, M. E., and Davies, P. H. J. (2022). Oversight and governance of the Danish intelligence community. *Intellig. Natl. Sec.* 37, 241–261. doi: 10.1080/02684527.2021.1976919

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., et al. (2014). After Snowden: Rethinking the Impact of Surveillance. *Int. Political Sociol.* 8, 121–144. doi: 10.1111/ips.12048

Bech-Nielsen, P. C. (2023) 'Regeringen lukker af for størstedelen af tilsynet med Forsvarets Efterretningstjeneste [The government is shutting down most of the oversight of the Danish Defense Intelligence Service]', *Radar*, 19 January. Available online at: https://radar.dk/artikel/regeringen-lukker-af-stoerstedelen-af-tilsynet-med-forsvarets-efterretningstjeneste (Accessed May 23, 2024).

Ben Jaffel, H. (2020). Britain's European connection in counter-terrorism intelligence cooperation: everyday practices of police liaison officers. *Intellig. Natl. Sec.* 35, 1007–1025. doi: 10.1080/02684527.2020.1778857

Ben Jaffel, H., Hoffmann, A., Kearns, O., and Larsson, S. (2020). Collective discussion: toward critical approaches to intelligence as a social phenomenon. *Int. Political Sociol.* 14, 323–344. doi: 10.1093/ips/olaa015

Bertelsen, N. (2019) *Vilkårlig masseovervågning er et vildspor, vi må forhindre [Arbitrary mass surveillance is a wrong path we must prevent]*, *PROSA*. Available online at: https://www.prosa.dk/artikel/vilkaarlig-masseovervaagning-er-et-vildspor-vi-maa-forhindre/ (Accessed September 24, 2024).

Bertelsen, N. (2020) 'Prosa til politikerne: I har forsømt at gribe ind trods flere faretegn i Forsvarets Efterretningstjeneste [Prosa to the politicians: You have failed to act despite multiple warning signs in the Danish Defense Intelligence Service]', *Altinget.dk*. Available online at: https://www.altinget.dk/forsvar/artikel/prosa-til-politikerne-i-har-forsoemt-at-gribe-ind-trods-flere-faretegn-i-forsvarets-efterretningstjeneste (Accessed September 24, 2024).

Bigo, D. (2019). Shared secrecy in a digital age and a transnational world. *Intellig. Natl. Sec.* 34, 379–394. doi: 10.1080/02684527.2019.1553703

Bochel, H., Defty, A., and Kirkpatrick, J. (2015). "New Mechanisms of Independent Accountability": Select Committees and Parliamentary Scrutiny of the Intelligence Services. *Parliam. Aff.* 68, 314–331. doi: 10.1093/pa/gst032

Born, H., and Johnson, L. K. (2005). "Balancing Operational Efficiency and Democratic Legitimacy" in Who' Watching the Spies? Establishing Intelligence Service Accountability. eds. H. Born, L. K. Johnson and I. Leigh. *1st* ed (Washington, DC: Potomac Books), 225–240.

Born, H., and Leigh, I. (2005). Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies. Oslo: Geneva Centre for Democratic Control of Armed Forces.

Bovens, M. (2007). Analysing and Assessing Accountability: a Conceptual Framework. *Eur. Law J.* 13, 447–468. doi: 10.1111/j.1468-0386.2007.00378.x

Bovens, M. (2010). Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism. *West Eur. Polit.* 33, 946–967. doi: 10.1080/01402382.2010.486119

Bovens, M., Goodin, R. E., and Schillemans, T. (2014). "Public Accountability" in The Oxford Handbook of Public Accountability. eds. M. Bovens, R. E. Goodin and T. Schillemans (Oxford: Oxford University Press), 1–20.

Considine, M. (2002). The End of the Line? Accountable Governance in the Age of Networks, Partnerships, and Joined-Up Services. *Governance* 15, 21–40. doi: 10.1111/1468-0491.00178

Damgaard, E. (2003). "Denmark: Delegation and Accountability in Minority Situations" in Delegation and Accountability in Parliamentary Democracies. eds. K. Strøm, W. C. Müller and T. Bergman. *1st* ed (Oxford: Oxford University Press), 281–300.

de Groot, J., and Thøgersen, J. (2012) 'Values and pro-environmental behaviour', in L. Steg, A. van den Berg and J. de Groot (eds.) Environmental psychology: An introduction. Wiley-Blackwell, pp. 141–152.

Department of Economic and Social Affairs (2020) UN Press Release: COVID-19 Pushing More Government Activities Online Despite persistent Digital Divide, Annual E-Government Survey Finds. Available online at: https://publicadministration.un.org/Portals/1/E-Government%20Survey%202020%20Press%20Releases.pdf (Accessed August 23, 2024).

Díaz-Fernández, A. M. (2023). "Talking with Spies: From Naïve to Distrustful Researcher" in Fieldwork Experiences in Criminology and Security Studies: Methods, Ethics, and Emotions. eds. A. M. Díaz-Fernández, C. Del-Real and L. Molnar (Cham: Springer), 3–22.

DiMaggio, P. J. (1983). "State expansion and organizational fields" in Organizational Theory and Public Policy. eds. T. H. Hall and R. E. Quinn (SAGE: Beverly Hills), 147–161.

Dobson, M. J. (2019). The last forum of accountability? State secrecy, intelligence and freedom of information in the United Kingdom. *Br. J. Polit. Int. Rel.* 21, 312–329. doi: 10.1177/1369148118806125

Ejersbo, N., and Greve, C. (2016). "Digital era governance reform and accountability: the case of Denmark" in The Routledge Handbook to Accountability and Welfare State Reforms in Europe. eds. T. Christensen and P. Lægreid. *1st* ed (London: Routledge), 267–279.

Eller, E., and Tofte, L. R. (2023) 'Kritikken vælter ned over regeringen efter droppede sager: "Rystende inkompetence" [Criticism pours over the government after dropped cases: 'Shocking incompetence']', *Danmarks Radio [Danish Broadcasting Corporation]*. Available online at: https://www.dr.dk/nyheder/indland/moerklagt/kritikken-vaelter-ned-over-regeringen-efter-droppede-sager-rystende (Accessed January 10, 2024).

Elmquist, B. (2012) Vejen til effektiv kontrol med PET og FE [The path to effective oversight of DSIS and DDIS], Retspolitik.dk. Available at: https://www.retspolitik.dk/vejentil-eff.ektiv-kontrol-med-pet-og-fe/ (Accessed 17 October 2023).

Fastrup, N., Moltke, H., Ilsøe, T. M., and Quass, L. (2020) FE-skandale omhandler tophemmeligt spionagesamarbejde med USA [DDIS scandal concerns top-secret espionage collaboration with the USA], Danmarks Radio [Danish Broadcasting Corporation]. Available online at: https://www.dr.dk/nyheder/indland/fe-skandale-omhandler-tophemmeligt-spionagesamarbejde-med-usa (Accessed September 23, 2024).

Forsvarets Efterretningstjeneste [DDIS] (2019). Indblik: Beretning 2017–2018 [Insight: Report 2017–2018]. Copenhagen: Forsvarets Efterretningstjeneste [DDIS].

Forsvarets Efterretningstjeneste [DDIS] (2021). Indblik: Beretning 2019–2020 [Insight: Report 2019–2020]. Copenhagen: Forsvarets Efterretningstjeneste [DDIS].

Forsvarsministeriet [Ministry of Defence] (2023). Besvarelse af samrådsspørgsmål B om Forsvarsministeriets besvarelsen til Tilsynet med Efterretningstjenesterne om behandling af rådata (afholdes den 21. marts 2023 kl. 14) [Response to consultation question B regarding the Ministry of Defense's reply to the Danish Intelligence Oversight Board on the handling of raw data (to be held on March 21, 2023, at 2:00 PM)]'. Available online at: https://www.ft.dk/samling/20222/almdel/fou/spm/58/svar/1944574/2683733.pdf (Accessed August 26, 2024).

Forsvarets Efterretningstjeneste [DDIS] (2023). Indblik: Beretning 2021–2022 [Insight: Report 2021–2022]. Copenhagen: Forsvarets Efterretningstjeneste [DDIS].

Friedland, R., and Alford, R. R. (1991). "Bringing Society Back In: Symbols, Practices, and Institutional Contradictions" in The New Institutionalism in Organizational Analysis. eds. W. W. Powell and P. J. DiMaggio (Chicago: University of Chicago Press), 232–267.

Friedman, B., and Citron, D. K. (2024). Indiscriminate Data Surveillance. *Virginia Law Review,* 110, 1351–1438. doi: 10.2139/ssrn.4738981

Gill, P. (2020). Of intelligence oversight and the challenge of surveillance corporatism. *Intellig. Natl. Sec.* 35, 970–989. doi: 10.1080/02684527.2020.1783875

Gitelman, L., and Jackson, V. (2013). 'Raw data' is an oxymoron. Cambridge, MA: The MIT Press.

Hammersley, M., and Atkinson, P. (1995). Ethnography: Principles in Practice. *2nd* Edn. London: Routledge.

Hartvigsen, M. S. (2024). Towards Intelligence Accountability as a virtue. *Intellig. Natl. Sec.* 39, 119–139. doi: 10.1080/02684527.2023.2255446

Hartvigsen, M. S., Hartmann, M. R. K., and Diderichsen, A. (2024). "Intelligence Oversight as an Institutional Battlefield: The Danish Experience" in Intelligence Practices in High-Trust Societies: Scandinavian Exceptionalism? eds. K. V. Rønnet al. *1st* ed (London: Routledge New Intelligence Studies), 89–104.

Hartvigsen, M. S., Koch, P. B., and Rønn, K. V. (2024) 'Eksperter er dybt bekymrede: Uafhængigheden svækkes for tilsyn med efterretningstjenesterne [Experts are deeply concerned: Independence is being weakened for oversight of the intelligence services]', *Radar*. Available online at: https://radar.dk/holdning/eksperter-er-dybt-bekymrede-uafhaengigheden-svaekkes-tilsyn-med-efterretningstjenesterne (Accessed January 10, 2024).

Hiis, T. S. (2020) Dokumentation: Tilsynet har kritiseret Forsvarets Efterretningstjeneste siden 2015 [Documentation: The oversight has criticized the Defense Intelligence Service since 2015]. Available online at: https://www.altinget.dk/artikel/dokumentation-tilsynet-har-kritiseret-forsvarets-efterretningstjeneste-siden-2015 (Accessed August 26, 2024).

Hillebrand, C. (2012). The Role of News Media in Intelligence Oversight. *Intellig. Natl. Sec.* 27, 689–706. doi: 10.1080/02684527.2012.708521

Hinings, C. R., Reay, T., and Suddaby, R. (2003) 'Dynamics of Change in Organizational Fields', in M. S. Poole and VenA. Van de (eds) Handbook of Organizational Change and Innovation. Oxford: Oxford University Press, pp. 304–323.

HUDOC Case of Big Brother Watch and Others v. The United Kingdom (2021a). Available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-210077%22]} (Accessed November 11, 2024).

HUDOC Case of Centrum för Rättvisa v. Sweden (2021b). Available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-183863%22]} (Accessed: 11 November 2024).

Inness, J. C. (1996). "Beyond Isolation: A Control-Based Account of Privacy" in Privacy, Intimacy, and Isolation. ed. J. C. Inness. *1st* ed (New York: Oxford University Press), 41–55.

Institut for Menneskerettigheder (2022). Tilsyn med efterretningstjensterne [Oversight of the Intelligence Services]. Overbliksnotat [Overview note]. Copenhagen: Institut for Menneskerettigheder.

Jansson, J. (2018). Building resilience, demolishing accountability? The role of Europol in counter-terrorism. *Polic. Soc.* 28, 432–447. doi: 10.1080/10439463.2016.1191485

Jølner, T., Beck, H. J. N., and Danielsen, J. H. (2021) Sammenfatning af FE-kommissionens konklusioner [Summary of the DDIS Commission's Conclusions]. Commission Report Summary. FE-Kommissionen [DDIS Commission]. Available online at: https://feuk.dk/wp-content/uploads/sites/2/2021/12/Sammenfatning-af-FE-kommissionens-konklusioner.pdf (Accessed March 18, 2022).

Jørgensen, R. F. (2019). "Danskernes syn på overvågning [Danes' view on surveillance]" in Usikker modernitet - Danskernes værdier fra 1981 til 2017 [Uncertain Modernity - Danes' Values from 1981 to 2017]. ed. M. Frederiksen. *1st* ed (Copenhagen: Hans Reitzels Forlag), 135–183.

Justitsministeriet [Ministry of Justice] (2024) Forslag til Lov om ændring af lov om Politiets Efterretningstjeneste (PET), lov om etablering af et udvalg om forsvarets og politiets efterretningstjenester og lov om beskyttelse af whistleblowere (Styrkelse af tilsynet med efterretningstjenesterne) [Proposal for an Act to Amend the Act on the Danish Security and Intelligence Service (DSIS), the Act on the Establishment of a Committee on the DDIS and DSIS, and the Act on the Protection of Whistleblowers (Strengthening Oversight of the Intelligence Services)], LOV nr 666 af 11/06/2024. Available online at: https://www.retsinformation.dk/eli/lta/2024/666 (Accessed January 10, 2024).

Kaarsbo, J. (2021) Tidligere chef i FE: Lækagesagen er danmarkshistoriens mest skadelige [Former manager in DDIS: The leakage case is the most damaging in Danish history]. Available online at: https://www.altinget.dk/artikel/tidligere-chef-i-fe-laekagesagen-er-danmarkshistoriens-mest-skadelige (Accessed January 10, 2024).

Kampmann, M. (2010) Danskere er ligeglade med at blive registreret [Danes don't care about being registered]. Available online at: https://www.retspolitik.dk/danskere-er-ligeglade-med-at-blive-registreret/ (Accessed October 17, 2023).

Klein Goldewijk, B. (2021). Why still critical? Critical intelligence studies positioned in scholarship on security, war, and international relations. *Intellig. Natl. Sec.* 36, 476–494. doi: 10.1080/02684527.2021.1893071

Kniep, R., Ewert, L., Reyes, B. L., Tréguer, F., Cluskey, E. M., and Aradau, C. (2023). Towards democratic intelligence oversight: Limits, practices, struggles. *Rev. Int. Stud.* 50, 209–229. doi: 10.1017/S0260210523000013

Koch, P. B. (2013). Fra Wamberg til PET-tilsyn – en analyse af den nye danske kontrol med efterretningstjenesterne [From Wamberg to oversight with DSIS – an analysis of the new Danish control over the intelligence services]. *Nordisk Tidsskrift Kriminalvidenskab* 100:70126. doi: 10.7146/ntfk.v100i1.70126

Koch, P. B. (2023). Retsgrundlag for efterretningstjenester i en ny tid [Legal Basis for Intelligence Services in a New Era]. *Juristen* 1, 11–19.

Kølln, T. (2019) "Det er vammelt, når man bare indsamler enorme mængder data om borgerne uden grund" ["It is grotesque when you simply collect enormous amounts of data about citizens without reason"]. Available online at: https://dm.dk/akademikerbladet/aktuelt/2019/januar/det-er-vammelt-naar-man-bare-indsamler-enorme-maengder-data-om-borgerne-uden-grund/ (Accessed September 4, 2024).

Koppell, J. G. (2005). Pathologies of Accountability: ICANN and the Challenge of "Multiple Accountabilities Disorder". *Public Adm. Rev.* 65, 94–108. doi: 10.1111/j.1540-6210.2005.00434.x

Krasny, M. E. (2020). "Values, Beliefs, and Attitudes" in Advancing Environmental Education Practice (Ithaca: Cornell University Press), 101–116.

Krog, A. (2020) 'Advarsel: Undersøgelse af FE kan ende i blindgyde [Warning: Investigation of DDIS could end in a dead end]'. Available online at: https://www.

altinget.dk/forsvar/artikel/advarsel-undersoegelse-af-fe-kan-ende-i-blindgyde?toke=33fc13ebd377436e8f8c4e470b1935d7 (Accessed October 17, 2023).

Larsen, M. (2021). Undersøgelse: Sådan påvirker overvågning på internettet danskerne [Study: This is how internet surveillance affects Danes]. Copenhagen: Dansk IT [Danish IT].

Leigh, I. (2012). Rebalancing Rights and National Security: Reforming UK Intelligence Oversight a Decade after 9/11. *Intellig. Natl. Sec.* 27, 722–738. doi: 10.1080/02684527.2012.708525

Lemberh-Petersen, M., Petersen, T. D., Olsen, B. K., Guild, M., Hvilshøj, R., Gregersen, CD., et al. (2021) 'Åbent brev: Stop overvågningen af os alle sammen [Open letter: Stop the surveillance of all of us]'. Available online at: https://amnesty.dk/aabent-brev-stop-overvaagningen-af-os-alle-sammen/ (Accessed September 24, 2024).

Leon-Reyes, B. (2022). "Towards a Reflexive Study of Intelligence Accountability" in Problematising Intelligence Studies Towards A New Research Agenda. eds. H. Ben Jaffel and S. Larsson. *1st* ed (London: Routledge), 30–47.

Lounsbury, M., Steele, C. W. J., Wang, M. S., and Toubiana, M. (2021). New Directions in the Study of Institutional Logics: From Tools to Phenomena. *Annu. Rev. Sociol.* 47, 261–280. doi: 10.1146/annurev-soc-090320-111734

Macnish, K. (2018). Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World. *J. Appl. Philos.* 35, 417–432. doi: 10.1111/japp.12219

Manjikian, M. (2016). Two types of intelligence community accountability: turf wars and identity narratives. *Intellig. Natl. Sec.* 31, 686–698. doi: 10.1080/02684527.2015.1077627

Maras, M.-H. (2012). The social consequences of a mass surveillance measure: What happens when we become the "others"? *Int. J. Law Crime Just.* 40, 65–81. doi: 10.1016/j.ijlcj.2011.08.002

March, J. G., and Olsen, J. P. (2013). "8 Elaborating the "New Institutionalism"" in The Oxford Handbook of Political Science. ed. R. E. Goodin (Oxford: Oxford University Press), 159–175.

Ministry of Higher Education and Science 'The Danish Code of Conduct for Research Integrity' (2014). Available online at: https://ufm.dk/en/publications/2014/files-2014-1/the-danish-code-of-conduct-for-research-integrity.pdf (Accessed June 11, 2024).

Parsons, C. (2015). Beyond Privacy: Articulating the Broader Harms of Pervasive Mass Surveillance. *Media Commun.* 3, 1–11. doi: 10.17645/mac.v3i3.263

Pedersen, M. J. (2021). Making Better Regulation: How Efficient is Consultation? *Scand. J. Public Admin.* 25, 43–57. doi: 10.58235/sjpa.v25i1.7129

Peissl, W. (2003). Surveillance and Security: A Dodgy Relationship [1]. *J. Conting. Crisis Manag.* 11, 19–24. doi: 10.1111/1468-5973.1101004

Petersen, K. L. (2019). Three concepts of intelligence communication: awareness, advice or co-production? *Intellig. Natl. Sec.* 34, 317–328. doi: 10.1080/02684527.2019.1553371

Phillips, L., and Schrøder, K. (2005). "Diskursanalytisk tekstanalyse [Discourse Analytical Text Analysis]" in Kvalitative metoder i et interaktionistisk perspektiv: Interview, observationer og dokumenter [Qualitative Methods in an Interactionist Perspective: Interviews, Observations, and Documents]. eds. M. Järvinen and N. Mik-Meyer. *1st* ed (Copenhagen: Hans Reitzels Forlag), 275–302.

Phythian, M. (Ed.) (2013). Understanding the Intelligence Cycle. Abingdon, UK: Routledge.

Pulver, A., and Medina, R. M. (2018). A review of security and privacy concerns in digital intelligence collection. *Intellig. Natl. Sec.* 33, 241–256. doi: 10.1080/02684527.2017.1342929

Quass, L. (2022) 'Tilsyn har indstillet kontrol med Forsvarets Efterretningstjenestes aflytning af kabler [Oversight body has halted monitoring the DDIS' wiretapping of cables]', *Danmarks Radio [Danish Broadcasting Corporation]*. Available online at: https://www.dr.dk/nyheder/indland/tilsyn-har-indstillet-kontrol-med-forsvarets-efterretningstjenestes-aflytning-af (Accessed September 27, 2024).

Räsänen, M., and Nyce, J. M. (2013). The Raw is Cooked: Data in Intelligence Practice. *Sci. Technol. Hum. Values* 38, 655–677. doi: 10.1177/0162243913480049

Reay, T., and Hinings, C. R. (Bob). (2005). The recomposition of an organizational field: health care in Alberta. *Organ. Stud.* 26, 351–384. doi: 10.1177/0170840605050872

Reay, T., and Jones, C. (2016). Qualitatively capturing institutional logics. *Strateg. Organ.* 14, 441–454. doi: 10.1177/1476127015589981

Retspolitisk Forening Høring over udkast til forslag til lov om ændring af lov om Politiets Efterretningstjeneste (PET), lov om etablering af et udvalg om forsvarets og politiets efterretningstjenester og lov om beskyttelse af whistleblowere (Styrkelse af tilsynet med efterretningstjenesterne) [Consultation on the draft proposal for an amendment to the Act on the Danish Security and Intelligence Service (DSIS), the Act on the Establishment of a Committee on DDIS and DSIS, and the Act on the Protection of Whistleblowers (Strengthening oversight of the intelligence services)]. (2024). Available online at: https://www.retspolitik.dk/wp-content/uploads/2024/04/Hoeringssvar-styrkelse-af-tilsynet-med-efterretningstjenesterne-marts24.pdf (Accessed September 24, 2024).

Reuter, M., Wijkström, F., and Meyer, M. (2014). "Who Calls the Shots? The Real Normative Power of Civil Society" in Modernizing Democracy. eds. M. Freise and T. Hallmann (Springer New York: New York, NY), 71–82.

Romzek, B. S., and Dubnick, M. J. (1987). Accountability in the Public Sector: Lessons from the Challenger Tragedy. *Public Adm. Rev.* 47, 227–238. doi: 10.2307/975901

Rønn, K. V. (2022). The multifaceted norm of objectivity in intelligence practices. *Intellig. Natl. Sec.* 37, 820–834. doi: 10.1080/02684527.2022.2076331

Schmidt, R. (2009) PET-Kommissionens Beretning: PET's Overvågning af Arbejdsmarkedet 1954–1989 [DSIS Commission Report: DSIS' Surveillance of the Labor Market 1954–1989]. Bind 8 [Volume 8]. PET-Kommissionen [DSIS Commission. Available online at: https://leksikon.org/images/pet_bind8.pdf (Accessed September 24, 2024).

Scott, R. W. (1994). "Conceptualizing Organizational Fields: Linking Organizations and Societal Systems" in Systems Rationality and Partial Interests. eds. H.-U. Derlien, U. Gerhardt and F. W. Scharpf (Baden-Baden: Nomos Verlagsgesselschaft), 203–221.

Søe, S. O. (2024). "Metaphors We Hide Behind: What Metaphors of Data, Information, and Technology Can Tell Us About Scandinavian Intelligence Practices" in Intelligence Practices in High-Trust Societies: Scandinavian Exceptionalism? ed. K. V. Rønn. *1st* ed (Routledge), London, 15.

Søe, S. O., and Mai, J.-E. (2022). Data identity: privacy and the construction of self. *Synthese* 200:492. doi: 10.1007/s11229-022-03968-5

Sorell, T. (2021). "Privacy, bulk collection and operational utility" in National Security Intelligence and Ethics. eds. S. Miller, M. Regan and P. F. Walsh. *1st* ed (London: Routledge), 141–155.

Thornton, P. H., and Ocasio, W. (1999). Institutional Logics and the Historical Contingency of Power in Organizations: Executive Succession in the Higher Education Publishing Industry, 1958– 1990. *Am. J. Sociol.* 105, 801–843. doi: 10.1086/210361

Tilsynet med Efterretningstjenesterne [TET] (2020) Pressemeddelelse [Press Release], August. Available online at: https://www.tet.dk/wp-content/uploads/2020/08/PRESSEMEDDELELSE.pdf (Accessed March 18, 2022).

Tilsynet med Efterretningstjenesterne [TET] (2022). "Årsredegørelse 2021: Forsvarets Efterretningstjeneste [Annual Report 2021: Danish Defence Intelligence Service]" in Annual Report (Copenhagen: Tilsynet med Efterretningstjenesterne [TET]).

Tilsynet med Efterretningstjenesterne [TET] (2023). "Årsredegørelse 2022: Forsvarets Efterretningstjeneste [Annual Report 2022: Danish Defence Intelligence Service]" in Annual Report 2022 (Copenhagen: Tilsynet med Efterretningstjenesterne [TET]).

Tilsynet med Efterretningstjenesterne [TET] (2024). "Årsredegørelse 2023: Forsvarets Efterretningstjeneste [Annual Report 2023: Danish Defence Intelligence Service]" in Annual Report 2023 (Copenhagen: Tilsynet med Efterretningstjenesterne [TET]).

Transparency International (2021) *The Spy Who Lives in My Phone*, *Transparency International: The global coalition against corruption*. Available online at: https://www.transparency.org/en/blog/pegasus-project-spy-who-lives-my-phone (Accessed January 10, 2024).

Transparency International Denmark (2020) *Sagen om FE: Ubetryggende kontrolspil fra Justitsministeriet [The DDIS case: Unsettling games of control from the Ministry of Justice]*, *Transparency International Denmark*. Available online at: https://transparency.dk/sagen-om-fe-ubetryggende-kontrolspil-fra-justitsministeriet/ (Accessed October 17, 2023).

Tulumello, S. (2021). Agonistic security: Transcending (de/re)constructive divides in critical security studies. *Secur. Dialogue* 52, 325–342. doi: 10.1177/0967010620945081

Van Puyvelde, D. (2013). Intelligence Accountability and the Role of Public Interest Groups in the United States. *Intellig. Natl. Sec.* 28, 139–158. doi: 10.1080/02684527.2012.735078

Van Puyvelde, D. (2018). Qualitative Research Interviews and the Study of National Security Intelligence. *Int. Stud. Perspect.* 19, 375–391. doi: 10.1093/isp/eky001

Wolfhagen, R., and Stræde, M. K. (2014) 'Partier vidste ikke, hvad Forsvarets Efterretningstjeneste fik lov til [Parties did not know what the DDIS was allowed to do]', *Information*. Available online at: https://www.information.dk/indland/2014/06/partier-vidste-forsvarets-efterretningstjeneste-fik-lov (Accessed September 27, 2024).

Yauri-Miranda, J. R. (2021). Principles to Assess Accountability: A Study of Intelligence Agencies in Spain and Brazil. *Int. J. Intellig. Counter Intellig.* 34, 583–613. doi: 10.1080/08850607.2020.1809954

Yauri-Miranda, J. R. (2023). The Role of the Media and Civil Society in Intelligence Accountability: The Cases of Spain and Brazil. *J. Intellig. Conflict Warfare* 5, 23–58. doi: 10.21810/jicw.v5i3.5061

Yoo, J. C. (2014). The legality of the National Security Agency's bulk data surveillance programs. *Harvard J. Law Public Policy* 37, 901–930.