UiT The Arctic University of Norway

Faculty of Humanities, Social Sciences and Education

Tilrettelagt innhenting – necessary to ensure national security, or an unreasonable incursion into Norwegian's privacy?

A discourse analysis on the implications of bulk interception on national security and individual's privacy.

Sebastian Leonard Rangel-Halvorssen

Master's thesis in Peace and Conflict Transformation SVF-3901 May 2023

Acknowledgements

I would first like to thank my supervisor, professor Gunhild Hoogensen Gjørv, for all of her support and guidance. I have enjoyed all the interesting conversations and it has been a pleasure having Gunhild as a supervisor. I would also like to thank the Centre for Peace Studies and staff for providing me with much advice and support throughout the program. They have all made sure that it has been some of the most interesting years of my life.

I would like to express my appreciation towards my classmates and friends, for the exciting discussions, academic support, and overall great experiences both on and off campus. I am look forward to the future and what it has in store for us.

Finally, I would like to express my gratitude to my family and girlfriend, for all of their support in completing the program and this thesis. I could not have done it without them.

Abstract

The introduction of bulk interception (in Norwegian: “tilrettelagt innhenting”) into the Norwegian intelligence service’s toolbox represents both a continuation of the long-standing security-liberty debate, and a significant development in Norwegian security policy. This development puts Norwegian democracy in a new and difficult situation to navigate, in order to achieve a proper balance of values.

This thesis focuses on the possible implications of bulk interception on both Norway’s national security, and individual Norwegians privacy. The original security-liberty debate has been somewhat reconfigured to now being considered a security-*privacy* debate due to advent of new technological developments, in which we share much more personal data than before, in addition to digital tools to collect and analyze the data these technologies generate. The result has been a situation which puts pressure particularly on privacy, but also provides opportunities with regards to security.

A discourse analysis has been performed to achieve the objectives of this thesis, as the public debate regarding bulk interception has generated plenty of written material. One of the key findings is that proponents argue that there are several other allied countries that already have a system for bulk interception, which speaks to its value, and that the threat environment makes the system a necessity for security. On the other hand, critics argue that there is limited documented value, it is a form of “mass surveillance”, and that the system is a violation of the right to privacy. However, the key conclusion to be drawn is that the democratic control mechanisms play the crucial role in achieving a proper balancing and therefore must have the resources and expertise to perform that role.

Keywords: Norway, security, liberty, privacy, bulk interception, democracy, technology, intelligence

Table of Contents

List of tables

1 Introduction

A classic issue all societies encounter during their development is how to balance security and liberty. This issue is particular for democracies, and it traces its origins back to Thomas Hobbes. In his seminal work, the Leviathan, Hobbes explains how free men came together to establish a sovereign who could provide them with protection from the dangers of the natural condition (Skaug, 2022, s. 7). In exchange, the sovereign would be given the right to rule, and the subjects would submit to his will. Hobbes provides an absolutist account in which all of the subject's rights will be exchanged for security. This exchange is incompatible with the values of a liberal democracy. Furthermore, this balance is a continuous challenge, and today it is impacted by the development of new technologies. To take two examples, the advent of the smart phone and social media have both created a situation where we share significantly more information about ourselves with several different actors. Although there are many instances in which this sharing of information is useful to our everyday lives, it has also created issues for our privacy. This is not only due to social media or the smart phone, but also because of the development of technologies that can collect and analyze this information, which in turn can be leveraged for a multitude of purposes. For companies, the objective is to reach and influence a larger group of people and turn them into customers for profit. For governments, the objective is security and crime prevention, among other things. It is no surprise that law enforcement and security is among the primary concerns for the state. Social media and the internet in general have created an environment in which criminals can operate with less risk of being caught. The emergence of hybrid threats, cyber-attacks, fake news, and the online spread of terrorist ideology has further complicated the maintenance of security, both for the individual and the state. It has created a grey zone which has proved quite difficult to handle by traditional methods.

A key method in which government agencies provide security is through surveillance. The development of new technological tools for these agencies to conduct surveillance and tackle the challenges found in this grey zone has in some ways created a completely new situation which has actualized the age-old security-liberty debate. However, the access to previously more private information, has changed the debates configuration, into a more security-*privacy* focused debate.

With these developments as a backdrop, a broad majority of the Norwegian parliament, Stortinget, approved a new law for the Norwegian intelligence service (NIS) in the summer of 2020 (Døvik, 2020). The law is intended to update the intelligence service's

legal framework to ensure that the service is better equipped to secure Norway's sovereignty, territorial integrity, democracy, and other national security interests, and in particular, to be in accordance with recent human rights developments (Innst. 357 L (2019–2020)). The most significant and controversial part of the law is found in chapter seven, which introduced the legal basis for NIS to collect and store large amounts of electronic communications, mainly metadata, which crosses the Norwegian boarder – so called "tilrettelagt innhenting". To ensure that readers unfamiliar with the Norwegian term, or who cannot read Norwegian, will be able to comprehend the contents of this thesis, "tilrettelagt innhenting" will be substituted with the term *bulk interception*. The reason for choosing bulk interception as the substitute term will be explained in the analysis chapter.

Metadata is information about who, when and where someone is communicating with someone else (Døvik, 2020). The main reason bulk interception is so controversial is due to the fact that most of Norwegians domestic communication is conducted through different digital services. These digital services are provided by private commercial Communication Service Providers (CSP), who usually have their servers placed abroad. The new law places a requirement on those CSPs to facilitate the collection. This entails that even if someone in Norway is communicating with someone else in Norway through one of those digital services, their metadata will be collected by the system. In addition, the intelligence service is not authorized to conduct intelligence activities about individuals in Norway, which adds another layer of complexity as the data will be stored by NIS.

For these reasons, critics argue that the bulk interception system is a form of "digital mass surveillance" and a huge violation of the individual's right to privacy (Døvik, 2020). However, there is no doubt that there exists a public consensus that Norway is under increasing pressure from hybrid threats, in particular within the cyber domain. The Norwegian Intelligence Service (2022, s. 19), the Norwegian Police Security Service (2022, s. 6), and National Security Authority (2022, s. 9) all highlight cyber threats within their public threat assessments. Bulk interception is presented as a tool which will allow us to counteract these threats. This raises questions regarding the viability of this claim, and whether or not the increase in security is worth the impact on privacy, which is the focus of this thesis.

1.1 Background, relevance and intended contribution

My interest in security policy has developed over the course of many years. Gradually I discovered that it was more than just a "hobby" and I eventually decided to pursue a degree

which allowed me to explore this topic further. As I searched for more knowledge, I came across an article which addressed the introduction of bulk interception in Norway. This is now about five years ago. Throughout these years I regularly read articles which discussed this topic and from there, privacy became an area of interest. My privacy online was suddenly something I was taking very seriously. I switched internet browsers and search engines, installed different add-ons, a password manager and began searching for a VPN.

The idea of writing my master thesis about privacy and security began to form some time before I applied to my current master program, and when my studies started, I had already begun to collect articles about bulk interception as it combines both of my interests, at the same time. In addition, it is an expansion of the Norwegian Intelligence Service's powers, which requires scrutiny and accountability. Not only by politicians, or privacy experts, but from an outside and bottom-up perspective as well. It's a significant development in that regard, and it could only be the start of further expansion. Therefore, it is important to conduct research on these developments in a Norwegian context is important to further expand our knowledge and understanding. I hope that my research can serve as a platform for further research on these topics.

Furthermore, democratic development is central to the field of peace and conflict studies. The balancing between security and liberty has its place within this process and it is strongly connected to the concepts of negative and positive peace coined by Galtung in his article "Violence, peace, and peace research" (1969). Galtung introduced the separation of peace into two different concepts to allow for a better analysis of the dynamics of peace. Galtung connects violence and peace by first dividing violence into personal (direct) and structural (indirect). An absence of personal violence is considered as negative peace, and an absence of structural violence as positive peace (Galtung, 1969, s. 183). The reason for the use of the term negative peace to imply an absence of personal violence is because it does not result in a positive condition. However, an absence of structural violence leads to social justice, which is understood as a positive condition e.g., positive peace. Therefore, peace theory is also connected to development theory and not only conflict theory (Galtung, 1969, s. 183).

Thus, bulk interception has its relevance within the realm of positive peace. Peace and democracy are not a state which is present or absent, rather it exists at different degrees and stages. How different societal developments affect peace and democratic conditions is an important area of study. This thesis is relevant to peace and conflict studies within this area. It explores how the introduction of bulk interception affects the trade-off between security and

liberty/privacy, within a Norwegian context. In addition, it explores the relationship between Norwegian state and its citizens, and how it will positively or negatively affect democracy and peace in Norway.

By exploring these complex and interrelated issues, this study aims to contribute to the existing and expanding body of research within the fields of democratic development, privacy, and intelligence collection. Specifically, it aims to contribute to the very limited body of research on the implications of bulk interception on Norwegian society. Lastly, this study aims to contribute to a knowledge-based discussion about how new technological developments will impact and challenge democratic values, such as liberty and privacy, security, and state-citizen relationships.

1.2 Research problem, objectives, and questions

The discourse surrounding bulk interception in Norway has existed for a long time. However, the absence of a bulk interception system has made research on its impact within a Norwegian context very limited. Furthermore, this system has been present in contexts of similar nature to the Norwegian context. Especially US and UK contexts are highly relevant and researched. They will provide information applicable to the Norwegian context. Despite some obvious similarities, the Norwegian context has significant differences compared to both the US and UK contexts, in particular with the public's relationships to security, privacy, intelligence agencies, and the government, and therefore warrants research focusing specifically on the Norwegian case. It is not sufficient, nor advisable, to draw direct conclusions of bulk interception's implications from the US and UK, and onto Norway. For these reasons, it is very important to address these issues early in its infancy, to lay the foundation for future research when more empirical data will be available.

To address the research problem outlined above, this thesis will seek to accomplish three objectives. First, this thesis will examine and highlight the implications of bulk interception on individual Norwegians' privacy and the Norway's national security. Second, it will assess these implications in light of the security-liberty trade-off. Third, it will serve as an initial study in which future research and debate can build upon.

To accomplish the research objectives, this thesis will aim to answer three research questions. First, to what extent does bulk interception contribute to increase Norway's national security? Second, to what degree are Norwegian citizens´ privacy affected by bulk

interception? Third, what are the possible long-term implications of this bulk interception system on the dynamics of Norwegian society?

1.3 Structure of the thesis

Chapter 1 introduces the reader to the issues addressed within this thesis. It presents how new technological developments challenge democracy and difficulties with how to address these challenges. In addition, it provides some background information about the motivation for the choice of topic, the relevance of bulk interception to the field of peace and conflict studies, and its intended contribution. Lastly, the research problem, objectives and questions are presented.

Chapter 2 covers the literature review which presents a collection of articles which represents relevant developments within the topics of privacy, liberty, security, and intelligence collection. This section will provide context for the rest of the thesis. It presents how liberty, security and privacy is interconnected, proposed legislation of intelligence collection, the dissonance of the claim that intelligence can adhere to only overseas collection, social media's role, encryption and back-doors, foreigners privacy protection, commercial Communication Service Providers' (CSP) roles in electronic surveillance, and the technological development of surveillance.

Chapter 3 presents the theoretical framework which will guide the analysis. It begins with a brief description of the emergence of the security-liberty trade-off theory. Furthermore, it expands on the trade-off and describes the difficulties it represents in terms of methods of measurement. The connection between liberty and privacy is explored and with it, the derivation of the security-privacy trade-off is presented.

Chapter 4 focuses on the methodological framework of the thesis. This section starts with presenting the role anti-realism and constructivism plays within discourse analysis. The methods of data collection and the analytical framework is described. It also includes a description of how trustworthiness and authenticity should be used as the reliability criteria in which a study of this kind should be evaluated. Lastly, it covers reflexivity and ethical considerations.

Chapter 5 presents the research findings. It organizes the texts into two sections: proponents and critics. The *in-favor* section consists of all the selected texts which supports or have a positive position towards the introduction of bulk interception. The *critics* section consists of the texts who are critical or negative towards bulk interception.

Chapter 6 provide the analysis of the findings. It is also divided into a proponent and critics section and extracts the key themes within each section. Furthermore, it highlights key arguments, their possible intention, and how it attempts to convince. The four analytical tools presented in the methods chapter will be the guide to analyze the findings.

The discussion and conclusion will be found in chapter 7. It will discuss the analysis in light of the theoretical framework and answer the research questions. Then the implications, limitations, and recommendations for future research will conclude this thesis.

2 Review of relevant literature

The literature review serves as a starting point for conducting research within most fields of study. The purpose is to identify current knowledge within a topic, which concepts and theories are relevant, and if there are any unanswered questions that needs to be addressed (Bryman, 2012, s. 98). As stated, the issue of balancing security, liberty and privacy has a long history and has become further actualized due to the advent of new technology, such as social media. The following literature review will provide a limited overview of central issues from recent publications and developments within this topic. It will provide the context in which bulk interception is placed within this area of study.

The ongoing debate of the struggle to achieve both national security and privacy is a continuation of the continuing discussion on the trade-off between liberty and security. Henrik Skaug makes this case in his article "The ethics of trading privacy for security" (2022, ss. 1-2). Today's digital age allows for modern technology to obtain information about individuals for many different reasons, usually due to its aid in preventing terrorist attacks, cyberattacks, espionage, and other highly destructive acts. Naturally, this line of argument makes clear that to increase security, some privacy must be sacrificed, not unlike the security-liberty trade-off – in other words, reduced privacy is the price individuals pay for security in today's world. Furthermore, depending on the conception on liberty, the function of privacy differs (Skaug, 2022, s. 5).

Social contract theory is one theory which links the complex and interdependent relationship between security, liberty, and privacy (Skaug, 2022, s. 7). By nature, individuals have absolute liberty, but engage in a social contract to exchange liberty or privacy for security to a certain level. However, if the trade continues beyond a certain level, it could lead to the erosion of liberty. Furthermore, Skaug highlights criticism towards the "trade-off" as being a false choice, and he makes an example that an increase in security by reducing liberty

can lead to blocking of legitimate opposition to the government, which in turn could lead to civil unrest (Skaug, 2022, s. 9) Viewing it as a trade-off implies a linear relationship and masks the complexity of the relationship it has to other values. Instead, Skaug proposes that it is necessary to take a holistic approach when examining the issue.

To build on Skaug's focus on technologies role in complicating this trade-off, we turn our attention to Tajdar Jawaid, who in his article on the trade-off between privacy and national security, examines how the technological development has changed intelligence agencies' ability to conduct surveillance operations (2020). Jawaid highlights five technologies which enables mass-surveillance and the possible system for checks and balances to protect privacy and avoid misuse (Jawaid, 2020, ss. 5-6). The technologies are the internet and digital communication; encryption; video surveillance combined with biometrics such as facial recognition technology; big-data analytics, machine-learning and artificial intelligence; and data storage centers. The scale of the technological capabilities for surveillance has grown significantly compared to the development of privacy protection, and to avoid misuse, Jawaid proposes oversight and development of laws which regulates the use of these technologies and balances the trade-off.

Although not mentioned specifically by Jawaid, social media occupies a central position in the technological developments. People regularly share personal information on social media platforms, which has completely transformed the amount of data available to individuals, companies, and governments. Should this information be regarded as public, and therefore available for intelligence agencies to collect, or should it be covered by privacy laws? Kira Vrist Rønn and Sille Obelitz Søe (2019, ss. 362-363) examined this issue and point at the public outcry after the Cambridge Analytica scandal shows that people in general are not comfortable with their information being collected and that it was a breach of their privacy. However, the potential benefits of using social media in intelligence gathering has been deemed large, with very little cost, making it very attractive for these agencies. It is therefore no wonder that there is a clash between the privacy interests of citizens, and information interest of intelligence agencies.

Social media is placed in the space in between private and public, and the question then becomes when agencies can exploit this information (Rønn & Søe, 2019, s. 363). The morality of utilizing social media intelligence (SOCMINT) depends on whether it is targeted or not, which certainly raises questions regarding what criteria justifies targeted collection (Rønn & Søe, 2019, s. 373). However, Rønn and Søe (2019, s. 373) argue that untargeted intelligence collection is not justified. Furthermore, bulk interception of information from

social media could negatively affect the way social media is utilized today, which can have wider negative consequences for society in general and democracy in particular (Rønn & Søe, 2019, s. 374).

In addition to social media's crucial role, the Snowden leaks in 2013, can certainly be considered to have exacerbated privacy concerns, as it revealed to some extent the scope of US, UK, and the Five Eyes surveillance capabilities (Watt, 2017, s. 773). An attempt to address this issue was made by the Council of Europe's Committee on Legal Affairs and Human Rights. The committee proposed the Intelligence Codex; a multilateral treaty which would regulate cyber surveillance and intelligence gathering domestically and abroad (Watt, 2017, s. 774).

Eliza Watt (2017, s. 790) argues in her article that mass foreign surveillance is unlawful under international human rights law. However, there are shortfalls within the ICCPR art.17 and ECHR art. 8 that needs to be addressed. The development of greater legislative surveillance powers in European states, such as the UK Investigatory Powers Act 2016, increases the problem without a solution in sight.

Aaron Pulver and Richard M. Medina (2018, s. 242) takes a similar approach as Watt and investigated some of the alleged surveillance programs which have been covered by several news stories in recent years. They attempt to gain insight into the possible capabilities of US intelligence agencies. In addition, they look at different US laws related to privacy and the publics opinion on these issues. In their investigation, they find that the US government has been in crisis mode since 9/11 and the introduction of the Patriot Act has given US citizens the impression that privacy laws can be adapted to allow further intrusion (Pulver & Medina, 2018, ss. 251-252). Furthermore, they find that threats to privacy from intelligence activities rise with an increase in threats towards citizen's safety.

They also ask if US privacy laws should better reflect that US surveillance is a threat to foreigner's privacy (Pulver & Medina, 2018, s. 252). Lastly, they highlight that NSA's bulk and targeted surveillance programs are not effective in stopping terrorist attacks. It therefore warrants questioning if these programs should be continued.

Asaf Lubin takes a different approach from that of Pulver and Medina, and argues that there is a dissonance between how citizens view mass digital surveillance depending on whether it is directed domestically or abroad, which further complicates the matter (2018, ss. 505-506). If it is directed domestically, then it is generally met with stark opposition, but if it is directed abroad, then it is generally supported. The role of foreign intelligence services is to conduct intelligence activities towards foreigners, and for these surveillance programs to

achieve domestic support, the argument is often that the program is directed at foreigners, and therefore is of no concern to national citizens (Lubin, 2018, s. 508). According to human rights activists, this differentiation is against the universal right to privacy. However, Lubin (2018, s. 509) argues that it is possible to justify this differentiation, in a limited sense, due to practical limitations in the way surveillance of foreigners is conducted.

Lubin further argues that certain distinctions are legitimate, such as political-jurisprudential limitations, technological disparities, and divergence in potential harm, and an acceptance of this by human rights defenders will allow for a discussion on how to create tailored human rights standards for foreign surveillance activities. Furthermore, in establishing these standards it is important to avoid a situation in which these rights can be broken abroad in the name of protecting them at home, or that removing control mechanisms can lead to agencies to employ the "revolving door" (allowing a foreign agency to spy on the states citizens and then exchanging the information to avoid control mechanisms) (Lubin, 2018, s. 537). Lubin (2018, ss. 538-550) makes eight suggestions for a potential new human rights framework: i) legitimate grounds for the distinction; ii) the Territoriality Presumption; iii) locations with "Quasi Territorial Qualities"; iv) the Principle of Legality; v) the Weber six; vi) Oversight and Transparency; vii) Notifications and Remedies; and viii) Intelligence Sharing.

Lubin's suggested framework is but one attempt to come up with principles for a new human rights framework. Simone Cooper (2018) made use of an alternative framework in her analysis of two pieces of legislature in New Zealand, specifically the Telecommunications (Interception Capability and Security) Act 2013 (TICSA) and the Intelligence and Security Act 2017 (ISA). Cooper assessed whether they comply with the International Principles on the Application of Human Rights to Communications Surveillance. Cooper found that the laws were initially framed as ensuring security and respecting human rights, democracy, accountability, and the rule of law, however, it was on the contrary in violation of the Necessary and Proportionate Principles (Cooper, 2018, s. 119). Hence, specifically highlighting that the legality principle is not upheld, as the TICSA and ISA is neither accessible, predictable nor ensure freedom from arbitrary interference. The measures the laws provide do not need to be necessary or proportionate.

There are few obligations for due process, and no requirement to inform of the number of individuals under surveillance. Lastly, Cooper highlights the obligation put on network providers which undermines the security and privacy of a communications system, and the

conclusion is that non-compliance with the principles goes against New Zealand's commitment to human rights, freedom, and democracy (2018, s. 119).

Legal measures to "rebalance" the skewing towards security is one way to address these issues and has naturally received a lot of attention from researchers. Another way is through technical measures, such as encryption. Digital communication, and thereby privacy, is protected through encryption. There are many events in the last couple of years that have renewed the debate on whether governments should have a backdoor to circumvent encryption. This is what Jeroen Veen and Sergei Boeke looked at and they found that government's argument in favor of a back-door, or similar access methods, is usually a variation of their inability to access terrorists' and criminals' mobile devices due to encryption (2020, s. 36). Privacy advocates have three main arguments against such access. First, governments might use this capability not only for terrorists and specific criminals, but all kinds of crimes. Second, if one government gets access, then every government would want access, even those that have questionable human rights records. Lastly, these keys will become targets of hackers who could acquire the same capabilities (Veen & Boeke, 2020, s. 38).

In short, proponents of strong encryption argues that the whole encryption system will become useless if a backdoor is introduced. Different countries have made different decisions regarding encryption, where the Netherlands decided against taking legal measures to restrict the strength of encryption, a position not shared by France and the UK (Veen & Boeke, 2020, s. 39).

Technical measures, and the providers of technology, deserve more attention from researchers. In the build up to the US Congress' renewal of the FISA Amendments Act in 2017, Mieke Eoyang examined the role of the telecommunications industry in electronic surveillance (2017). According to Eoyang the interests of these companies are often left out of the surveillance-privacy debate, despite being the enablers of electronic communication and surveillance (2017, s. 259). Private companies must conduct their own balancing act as they want to contribute to national security, but also must meet the demands of current and potential customers.

To ensure that the CSPs' interests are addressed, Eoyang makes three suggestions. Firstly, the collection of data from the companies without their knowledge must be stopped, and they will be notified of the data the agency requests and transfer it in accordance with a FISC order (Eoyang, 2017, ss. 275-277). Secondly, bulk interception should be replaced by

targeted collection as to ease foreign customers concerns (Eoyang, 2017, ss. 277-280). Lastly, establish a forum to discuss and create norms for electronic surveillance among allies (Eoyang, 2017, ss. 280-281).

This collection of literature shows the vastness of issues at play at the same time. However, all of them center around an underlying security-liberty trade-off which has been developed into a security-privacy debate. Furthermore, surveillance through new technologies has become the most efficient, effective, and economically viable way to achieve security, and therefore privacy comes into play as it is often framed as a hindrance. This is where bulk interception becomes relevant, as it is a way to circumvent this hindrance, at the intersection between legal and technical measures. To achieve a better understanding of this literature collection the interplay between surveillance, privacy, security, and liberty, it is necessary to establish the theoretical framework it is built upon. This will be presented in the following chapter.

3 Theoretical framework

To better understand the vast literature outlined in the previous chapter, and prior to beginning the analysis, it is fundamental to establish the theoretical framework in which it is built upon. Therefore, the framework will be established piece by piece. It will begin with establishing the concept of *security* and how it should be understood in the proceeding analysis and discussion. Then, the attention will turn towards *liberty*, in which negative and positive liberty will be presented, in addition to republican and liberty understood as independence. From there, privacy's role within liberty will be explored, to understand their connection. To make the framework complete, the way in which privacy can function as a "currency" which can be exchanged for security is presented. This is crucial to understand in order to grasp why privacy has become the prominent area of concern. Lastly, the reasoning behind the framework's relevance to the research problem and the limitations of it will be explained.

3.1 Security

Security is a concept which can encompass a multitude of understandings, depending on the context. However, the subject matter of this thesis provides an indication of which type of security is most relevant. It has its roots in Hobbes's conceptualization of the establishment of a sovereign. In the state of nature, before there was any government, individuals had

absolute liberty, which lead to significant problems for three reasons (Skaug, 2022, s. 7). First, several important goods are scarce which leads to competition. Second, there is uncertainty regarding the intentions of others and therefore fear of what they might do. Third, people have desire for others to value them as highly as they value themselves. However, because this will generally not be true, it will together with the other two factors create conflict. The state of nature with absolute liberty is plagued by fear and danger. Therefore, we trade our absolute liberty for security by establishing a sovereign who will provide protection from these dangers.

According to Hobbes, the primary duty of the state is therefore to protect its citizens from danger and harm, in other words to provide collective security. Although Hobbes' account is more focused on the internal dangers, it is possible to transfer this duty to also include protection from external threats. As states became nation-states, national security has become the main conceptualization of collective security, and it has been operationalized through law by most nations. The Norwegian definition of national security is found in "sikkerhetsloven" (2019, ss. §1-5) and states (author's translation):

> "In this act, the following terms shall have the following meanings:
>
> 1. national security interests: Norway's sovereignty, territorial integrity and democratic system of government, and general political security interests related to
>   a) the activities, security, and freedom of action of the highest state bodies
>   b) defense, security, and contingency preparedness
>   c) relations with other states and international organizations
>   d) economic stability and freedom of action
>   e) fundamental societal functions and the basic security of the population"

This definition provides a more specific and elaborate understanding of national security from a Norwegian perspective. Despite security being operationalized by law, a method of measuring how secure the nation is, remains a difficult task. This in turn cause difficulties with determining the extent the introduction of a new security measure, such as bulk interception, will impact overall security. The political theorist Jon Elster suggested to use the risk of harm as a metric for security (Posner & Vermeule, 2007, s. 38). A high-risk context would be one with less security, and one with low risk would be of higher security – the relationship between the input and output is inverse. This certainly aids in evaluating new security measures; however, it is still a subjective matter.

3.2 Liberty

As with security, liberty poses challenges of definition, and there are several different "types" of liberty, depending on what is emphasized. The political theorist Isiah Berlin (Skaug, 2022, s. 4) conceptualized two different types of liberty, which also function as a base in which a method of measurement could be established. The two different "types" are *negative* and *positive liberty*.

Negative liberty is defined as an individual's ability to act without obstruction or interference by other people (Skaug, 2022, s. 4). This understanding of liberty can be considered the most basic approach or fundamental understanding of liberty. In addition, it is perhaps the "easier" definition in which to build a metric upon. The degree of interference is one example.

Positive liberty builds on negative liberty, by including an emphasis on self-development and internal obstacles, in addition to the removal of external obstructions (Skaug, 2022, s. 4). The options and alternatives that are available to an individual and if the individual can make use of them. This definition is much broader and turns the attention towards individual's autonomy and ability. The difference between negative and positive liberty can be summed up as: negative liberty is what an individual is free *from*, while positive liberty is also what an individual is free *to do*.

A third type of liberty is worth including. *Republican liberty* is concerned with liberty as non-domination (Skaug, 2022, s. 4). It is considered an intermediate position between negative and positive liberty. It emphasizes non-interference, by advocating for protection of individuals from *potential* interference. Someone's ability to obstruct an individual's actions creates a state of domination, despite that someone not exercising their ability.

Lastly, there is *liberty as independence* (Skaug, 2022, s. 4). This definition of liberty is situated between negative and republican liberty. It agrees with republican liberty in that individuals must be protected from potential interference but disagrees with the emphasis on protection from arbitrary interference. Any nonarbitrary reduction of liberty must be considered liberty reducing within this understanding. It is a non-moralized conception of liberty, similarly to negative liberty.

For liberty, Elster acknowledges that defining a metric is much more difficult and suggests that it should be assumed to be possible to measure it and therefore just skip it (Posner & Vermeule, 2007, s. 39). Although it is not difficult to agree with Elster's statement, this is a rather simplified approach, and leaves much to be desired. One, several, or a mix of these definitions, can function as a base for the creation of indicators which can measure how

liberal a specific nation is. However, similar challenges exists between security and liberty, such as which understanding of liberty should be prioritized? What kind of indicators should be included? From a societal point of view, the aim is to optimize by finding the point which maximizes the welfare for the population. However, without a surefire method to measure security and liberty, the two concepts remain difficult to balance.

3.3 Privacy and its function within liberty

Privacy can be defined as "the rights to be let alone, secrecy, personhood, intimacy, limited access to the self, and control over personal information*"* (Skaug, 2022, s. 2). It consists of some form of voluntary and temporary withdrawal from public attention. Furthermore, it can range from minimal to absolute depending on the individual's own preference.

Depending on whether negative or positive liberty is prioritized, privacy can either be considered distinct or a precondition for liberty (Skaug, 2022, s. 5). The key point of negative liberty is the absence of obstruction of individuals actions, and if obstruction is occurring, then it reduces liberty. However, if governments or private commercial companies are not obstructing individuals' actions, but is surveilling or conducting other breaches of privacy, then it is not viewed as negatively affecting liberty (Skaug, 2022, s. 5). The reasoning being that the individual is still free to continue acting however they see fit, despite being observed. This ignores the changes in behavior that occur when people are observed, including self-censorship and conformity, which is a form of interference. Whether the surveillance is covert or overt further complicates the situation. Covert surveillance might not cause any interference to individual's actions as they are unaware of the observation, and self-censorship might not occur.

On the other hand, within positive liberty, self-mastery occupies a key position and views privacy as precondition for developing an individual capacity for self-determination and self-development, which leads to an individual's ability to pursue the available options (Skaug, 2022, ss. 5-6). Privacy sets the individual apart from its social setting and allows for a safe space in which people can develop and acquire the skills necessary to be considered free. From a positive liberty perspective, a breach of privacy, in the form of surveillance, either covert or overt, would negatively affect this development only if it becomes too comprehensive. A recording of an individual's movements would not be problematic, but detailed knowledge of someone's biological data would be viewed as problematic.

Within republican liberty and liberty as independence, privacy is considered the safeguard against domination and maintenance of independence (Skaug, 2022, s. 6). Privacy performs as a safeguard in three ways. Firstly, it allows individuals to hide certain parts of their lives which makes it difficult for others to exercise physical control over them. Secondly, it allows individuals to hide psychological parts of their lives which makes it difficult for others to exercise psychological control over them. Lastly, it prevents the collection of personal data which limits the amount of personal data being stolen and exploited by others. Furthermore, this understanding of privacy is not limited to only individual's physical lives but extends to their online lives.

Privacy's role as a precondition for self-development and self-determination, safeguard against domination, and as a tool for maintaining independence, set's the conditions for it to be exchangeable with security. This is due to the reduction of privacy measures, either partly, or completely, naturally reduces its ability to perform its function.

3.4 Trading privacy for security

How, then, can privacy be traded for security? Replacing liberty with privacy in this trade-off is dependent on which security measure is considered. If the security measure directly impacts privacy's role within liberty, it can be said to have "replaced" liberty. Tiberiu Dragu (2011, s. 66) addresses the security rationale for reducing privacy and makes clear how privacy can be traded for increased security. Dragu divides the logic into two main arguments. The first argument states that agencies responsible for counter-terrorism experience privacy protections, such as restrictions on interception of communication, data retention and data mining, as constraining their efforts to prevent terrorist attacks. By allowing counter-terrorist agencies to breach the privacy protections, they will be better equipped to prevent potential attacks. To build on this, Skaug (2022, s. 3) explains that the information that is collected can be extensive personal data which can be analyzed to determine different patterns of behavior that can predict which individuals have extremist convictions and could be inclined join an terrorist group. In addition, the collection of personal data and interception of communication could also expose the planning of an attack and the members of a terrorist cell. By inversing the first argument we can also see that by increasing privacy protections counter-terrorism agencies will experience further restrictions and hence security will be reduced.

Dragu's second argument claims that a reduction in privacy protection creates a more dangerous environment for terrorists to plan and conduct their attacks (Dragu, 2011, s. 66).

Strong privacy protection allows for potential terrorists to communicate and grow covertly, and the freedoms and openness are taken advantage of. These arguments are to a large degree transferable to preventing other possible threats to national security, such as espionage and cyber-attacks.

Replacing liberty with privacy is not contingent on whether the security measure only impacts privacy, as liberty consists of interconnected rights and freedoms which naturally will lead to several being affected at the same time. However, privacy must be considered the right mostly affected in order to replace liberty as a whole.

3.5 Relevance and limitations

The choice and relevance of this theoretical framework is based on three main reasons. First, the actors that participate in the public discourse regarding the introduction of bulk interception in Norway can generally be grouped into two camps which oppose each other. One camp if in favor of introducing bulk interception into the Norwegian intelligence services' toolbox. The other camp is against it. The arguments are made in such a way that a trade-off is implied. Second, the actors in favor generally make their arguments based on national security-related concerns. The actors against make their arguments based on privacy-related concerns. Lastly, as security, liberty and privacy are abstract concepts which are experienced subjectively, it is necessary to evaluate how different actors perceive this legislative change within a framework that address these concepts directly. If it was possible to mathematically calculate the impact of targeted interception on security, liberty and privacy, the discussion could be conducted in a more objective fashion. However, since that is not possible, it is the subjective experiences that must lay the foundation for the discussion, and which must be analyzed to extract the possible implications of it.

The theoretical framework does contain some limitations that it is important to keep in mind when applying it to the findings. Dragu created a game-theoretic model of the interaction between an antiterrorist agency and a terrorist organization and analyzed changes in the probability of a terrorist attack with changes in privacy protections (2011, s. 64). Two implications were derived from the model. First, when accounting for strategic interactions, reducing privacy did not necessarily increase security, which entails that the two is not "naturally" in conflict, as often assumed. Second, the agency will always want less privacy, despite that it may lead to reduction in security. The agency with a disproportionate ability to influence policy making complicates the balancing in a way the trade-off does not account

for. Furthermore, Skaug finds that the use of "balance" or "trade-off" assumes a simple linear relationship which is false, and that security, liberty and privacy share a more complex relationship, depending on which liberty is applied (2022, ss. 8-9). This is due to that in some instances, trading privacy for security, liberty is increased as the enjoyment of other liberties require security. Another way is to view the reduction of privacy to increase security as having no effect on liberty. A view in accordance with negative liberty. However, for the reasons state above, the more complex relationship between these values is not considered in this thesis.

4 Methodological framework

To analyze the implications of bulk interception on Norwegian national security, Norwegians individual privacy and possible consequences, I have performed a discourse analysis. The source material consists mainly of relevant news articles, government documents, opinion pieces, and hearings responses, by policymakers, experts, and interest groups. A qualitative methodology was appropriate for this subject as I am investigating abstract concepts with subjective experiences. This required an inductive research technique that allowed theory to function as an analytical lens to evaluate the implications of bulk interception.

There is no universal approach to discourse analysis. However, one approach that has been widely used by social scientists is characterized by two different features at the epistemological and ontological level, namely anti-realism, and constructivism (Bryman, 2012, ss. 528-529). Anti-realism denies any claims of an object reality that a researcher can discover and therefore no researcher can acquire privileged knowledge of an aspect of the social world. However, some analysts take a position that is closer to a realist position (Bryman, 2012, s. 539). Constructivism emphasizes that versions of reality is constructed by actors within a specific social context by their renditions of it. This makes discourse a meaningful device as people seek to achieve objectives through talk or writing. The interesting aspects are the technics employed and discourse analysis is therefore focused on action (Bryman, 2012, s. 529).

The reason discourse analysis is an appropriate method to investigate the implications of bulk interception is found in philosopher Michel Foucault's thoughts in which he considered discourse as the ways we depict an object frames our comprehension of it (Bryman, 2012, s. 528). Discourse forms a version of the object, and that version eventually

constitutes it. This has implications for how the object or issue is addressed. It creates the framework and justification for, as an example, power distribution within a specific area of concern. The public debate on bulk interception has in essence been a "battle" for the public's perception of it. Therefore, it provides an indication of the public's comprehension of bulk interception and how their actions are affected by it. This has led to the production of plenty of written material. A discourse analysis allows for meaning and evaluations to be extracted from this material to answer the research questions and determine how bulk interception is comprehended and constituted.

4.1 Data collection

Discourse analysis does not have a definite method of data collection; however, the research problem is usually used to guide the collection (Tonkiss, 2017, s. 483). The relevance of the source is the determinant for its inclusion, while the number of texts is considered less important. To obtain relevant texts, I used my research problem as a guide and made use of the Google Search Engine. There I would type in different key words and sentences in Norwegian, such as "bulk interception", "new intelligence law Norway" and "critical to bulk interception" to narrow my search to relevant sources. In addition, The UiT Arctic University of Norway's Oria service was used to find relevant academic material. The snowball method is a form of convenience sampling in which the researcher makes contact with a small group of informants and then use them to establish contact with other informants (Bryman, 2012, s. 202). This method is useful to obtain relevant sources and when a random sampling is not feasible. However, it will not provide a representative sample of the population. This method is mostly used within qualitative research due to generalization being less important than within quantitative research (Bryman, 2012, s. 203). The method can be used to sample other types of sources as well, such as texts. I employed the snowball method as relevant sources often contained links and references to other articles which addressed similar and different point of views.

Furthermore, discourse analysis is generally based on textual data, more so than conversation analysis (Tonkiss, 2017, s. 483). Therefore, the data collected is texts and mostly secondary, and they have been collected from different organizations such as government institutions and agencies, academia, think tanks, special interest groups and media outlets. These organizations provide a wide variety of texts which include white papers and policy documents, committee reports, parliamentary discussion summaries, hearing responses,

legislative texts, press releases, journal articles, newspaper articles, and opinion pieces. All of these texts have to varying degree been included in the source material.

As the research problem under investigation is within a Norwegian context the texts are mostly written in Norwegian. Since this thesis is written in English, this poses challenges with regards to the translation of the arguments used within a text. In the process of translation, meaning can be lost, and the argument is therefore weakened. On the other hand, meaning can be added and the argument could become strengthened. To mitigate these challenges, I have strived to make as direct translations as possible and avoid including terms which could either add or remove meaning. Whenever a text includes Norwegian words which have no direct or precise word in English, the Norwegian word will be used. A description of the word, together with a possible English word, will be found in the analysis chapter.

Another main challenge is that all source material originating from the Norwegian government will be edited to exclude any information considered sensitive and classified. On the one hand, this allows the actors in favor to argue from a position of privileged information which either strengthens their point of view or protects them from more elaborate scrutiny. It also limits how specific their argumentation can become, as part of the argument cannot be made public. On the other hand, it limits the arguments that can be made against, as the "full picture" is not available.

Lastly, the number of sources is a challenge as the issue has been discussed to varying degree since 2016. The relevance criteria ensured that the data did not include texts which were irrelevant, which in turn aided in the volume of material remaining manageable. The following criteria was also utilized to avoid an overwhelming amount of data whilst still having a comprehensive database: the text contributed to answering the research questions; the source did not only provide the same arguments, in other words, new and different arguments where presented; a relative balance in the texts positions; and the document's probable purpose. In addition, some sources that seemed relevant in the beginning where later excluded due to not taking a position towards bulk interception, but focused on other areas of the new intelligence law. Some opinion pieces were a response to a previous opinion piece; however, it was not taken into account due to it not being relevant to their positions. Most of the sources acknowledged the opposite's motivation, but it was left out of the summaries as this acknowledgement does not contribute to their argumentation, but rather reflects an awareness of their positions.

4.2 Data analysis

As with data collection, discourse analysis has no clear analytical framework and resists codifying the practice. It is viewed more as skill that must be acquired through "learning-by-doing" (Bryman, 2012, s. 530). However, the uncovering of interpretive repertoires is central, which Potter and Wetherell refers to as the overall rhetorical effect of a text. It provides a framework to consider the text's inconsistencies, internal workings, and small strategies of meaning – in other words, the ways of speaking about and understanding a topic that organizes the meaning of a text (Tonkiss, 2017, s. 485). Furthermore, it is not necessary to analyze every sentence of a text. To be selective and extract the sections that provide the best sources of data, is much more appropriate. One must be aware of selecting sections which only supports one point of view, and ignoring opposite or contradicting arguments, as they provide for a comprehensive analysis. In addition, it is important that any conclusions are supported by the data. Discourse analysis is an interpretative process, and therefore does not contain any clear framework. Despite this, and based on Foucault's suggestions, a text can be analyzed based on four different areas: by identifying key themes and arguments; searching for association and variation; exploring characterization and agency; and focusing on emphasis and silences (Tonkiss, 2017, ss. 485-486).

By identifying key themes, terms, and arguments the aim is to bring forward significant keywords, phrases, and images the author has used to construct their argument. This involves working through the texts and comparing and contrasting how different themes emerge. The number of times a certain keyword could be counted to show its significance, and especially if it is frequently associated with another keyword (Tonkiss, 2017, s. 486). This is also referred to as interpretive repertoires, which are the ways of speaking and modes of understanding within a text (Tonkiss, 2017, s. 487). These can vary and be context dependent, as the belief and action of a writer takes place within templates that guide and influence them (Bryman, 2012, s. 533).

To search for patterns of association and variation involves establishing the relationship between different aspects within the text. Connections could be made between different actors or groups of people and a particularly polarizing political issue, such as refugees and crime (Tonkiss, 2017, s. 487). The links that are created can also work to favor a group, by associating it with something positive. Variations can materialize in a text by attempts at reconciling conflicting perspectives, or address uncertainty, which exposes the internal inconsistencies of the writer's argumentation. It includes being aware of the exclusion of alternative accounts.

Characterization and agency are strongly connected to patterns of association as it entails exploring how different social actors are described and positioned in the text (Tonkiss, 2017, s. 488). The way in which specific values, problems or qualities are linked to a general or specific group. Personalization or depersonalization are other techniques of characterization. The author's standpoint could potentially be of interest as well. Also, whether the text is attempting to draw authority by writing from an objective or subjective point of view, depending on the context. The way agency is presented in the text, which actor is passive or active in creating the problems and solutions, is an important aspect to review (Tonkiss, 2017, s. 489). Both can be positive and negative, depending on the context in appears in, and the possible effect it has on the reader.

By focusing on emphasis and silences, the objective is to bring attention to the aspects that are highlighted and neglected in a text (Tonkiss, 2017, s. 490). To manage this, the reader must first understand and capture the position the text is supporting. Second, the reader must look for what is not included, or purposely omitted, keeping in mind the text is written with a specific purpose. This can help to expose the purpose and author's position within the discourse which makes it easier to draw connections between texts and contrast them to others. However, it is important to avoid attempting to making the data claim something that it does not support.

4.3 Trustworthiness and authenticity

Validity and reliability are criteria usually used to evaluate the quality of a quantitative study. The transferring of these criteria onto qualitative research poses challenges, due to measurement being a major component of quantitative research, which is not the case in qualitative research. This has led to the development of related but different criteria to assess qualitative research. Guba and Lincoln suggested two alternative criteria for qualitative studies: trustworthiness and authenticity (Bryman, 2012, s. 390).

Trustworthiness consists of four sub-criteria which each capture an equivalent criterion in qualitative research. The first criteria is credibility, and it is related to internal validity. Since there are multiple accounts of reality, the source's credibility of an account is possible to establish. This can be achieved by good practice of the method, respondent validation, and triangulation. For this study, good practice and triangulation will be in employed as respondent validation is not feasible.

The second criteria is transferability and is the production of a thick description, in other words, a rich description of the phenomenon (Bryman, 2012, ss. 391-392). This will provide a database others can use to judge the transferability. Transferability parallels external validity. This study's objective is providing a thick description, and this is taken into account.

The third criteria is dependability and entails ensuring that the entire research process is on record and possible to establish (Bryman, 2012, s. 392). It will allow others to conduct an "audit" and determine the degree of dependability. This criteria parallel's reliability.

The fourth criteria is confirmability. It parallels objectivity and is used to evaluate whether the researcher has acted in good faith by not allowing personal opinions shape the research (Bryman, 2012, ss. 392-393).

Authenticity is concerned with the political impact of the research and consists of five sub-criteria (Bryman, 2012, s. 393). This criterion will be particularly important to this study as it is investigating a controversial topic within the public discourse, despite their relative lack on influence. In addition, it ensures that the researcher is mindful of possible implications. *Fairness* focuses on whether the research achieves a fair representation of the different viewpoints. *Ontological authenticity* concerns whether the thesis is adding knowledge of the social context. *Educative authenticity* evaluates the degree to which the study allows participants to increase their understanding of different perspectives. *Catalytic authenticity* focuses on if the investigation allowed participants to act to change their circumstances. Lastly, *tactical authenticity* evaluates whether the research has empowered participants to take necessary steps for active engagement.

4.4 Reflexivity and Ethical considerations

Reflexivity is a term which has multiple meanings within social sciences, and is also considered a difficult concept to establish, especially with consideration to the "superiority" of a reflexive position compared to an unreflexive one (Bryman, 2012, ss. 393-394). However, in this context, reflexivity is referred to as the researcher being reflective about the implications of their methods, values, bias, and decisions on their study. It entails a sensitivity to the researcher's cultural, political, and social context (Bryman, 2012, s. 393). The knowledge that is produced will always reflect the researcher's location in time and space.

Therefore, the context of the researcher of this study is particularly important. The researcher is a Norwegian citizen and is conducting the research within Norway. Inevitable, this will to some degree influence how the researcher approaches the research, as the

researcher is under the jurisdiction of the new intelligence law. The objectivity of the researcher could therefore be considered less objective compared to a researcher from a different country and conducting research on this topic from abroad. On the other hand, to reach a comprehensive analysis of the topic, different perspectives which complement and criticize each other can only be considered a positive development. In this light, this study must be considered as a small part of, hopefully, a future broad knowledge production on the subject of bulk interception, in a Norwegian context.

Furthermore, the researcher's motivations and prior knowledge of this topic will certainly affect the conduction of the study, as opinions of the topic can have been formed prior. Section 1.0 "Motivation" already address the motivation behind the choice of topic. Complete objectivity is therefore not possible and could be argued as not necessarily something to aim for, however, the researcher will strive to ensure that neither participant of the discourse receives preferential treatment in the analysis, and to live up to the criteria of trustworthiness and authenticity.

To consider the possible ethical implications of research is important as it ensures that the researcher reflects on the potential social consequences of one's studies. There are four ethical principles that is central to social research: do no harm to participants; obtain informed consent; avoid invasions of privacy and deception as far as possible (Bryman, 2012, s. 135). All of these principles are less relevant to this thesis as the researcher will not interact directly with any individuals who have participated in the discourse, nor make use of information that is not publicly available. However, it is important to keep these principles in mind as the research progresses and take time to consider if any actions violate any of these principles. Furthermore, the potential political and social implications must be considered. Bulk interception is a controversial topic, and this study could be misused to support a perspective it has no basis for. Therefore, it is important that the findings, analysis, discussion, and conclusion are supported by the data, and that the data is traceable to the original source.

5 Findings

Now that the methodology has been covered, the attention is turned towards the findings of the research. The texts are organized into a grid with three headings to provide an orderly overview of each included text. *Type* describes the kind of document which is included. *Title/author* presents the title and/or author (specifically relevant for the hearings responses as they did not have a title). In order to extract meaning, the *main arguments* have

been written as a summary. This will allow the reader to get a brief impression of each text's argumentation and serve as a reference work for the analysis. Furthermore, the texts are divided into two sections, with color coding (green and red), which signifies their position vis-à-vis bulk interception. The *in-favor* category is first, and naturally takes a position positive towards bulk interception. The *critical* section is second and have a negative view of bulk interception.

In-favor		
Type	Title/author	Main arguments
Speech	Forsvarsministerens innlegg ved presentasjonen av forslag til ny etterretningstjenestelov	Communication through cross-border fiberoptic cables, owned by companies, has fundamentally changed the conduct of foreign intelligence. Extraction of relevant data in real-time is not possible. Therefore, all metadata that crosses the border must be collected and stored, and then relevant data is extracted. Content data will not be stored. Oslo District Court must approve search of the dataset and can stop ongoing collection upon petition from EOS-committee. Expert panels and experience from other states confirm the need for bulk interception. Data will only be used for intelligence purposes. There is control before, during and after collection. Surplus data can only be dispensed in cases of emergency (Bakke-Jensen, 2020)
News article	E-sjefen: – Det blir fest i Russland og Kina hvis Norge dropper datalagring	Intelligence pressure against Norway is increasing and NIS doesn't have the tools to counteract the activity. It will be a party in spy agencies in Russia and China if Norway doesn't implement bulk interception. Norway mentioned in ISIS propaganda as good transit state because there is no control. NIS is not interested in Norwegian traffic. Content data will only be made available by a court's approval, and everything will be traceable. We should appreciate that the process is open, because in many

		other countries these tools are used without informing the public (NTB, 2019).
News article	IKT-Norge og E-tjenesten: Cybertruslene gjør at vi må tenke nytt om personvern	Bulk interception will enable NIS to discover the large volume and targets of malicious activity, and then help Norwegian businesses to stop it. The activity will become worse, so we might have to allow other invasive tools. It is important to not become stuck in "ideological trenches" about privacy and freedom of expression without a proper debate which accounts for changes in the context. NIS does not want to breach privacy more than necessary, but at the same time protect us from foreign threats. We don't live in an ideal world (Seglsten, 2022)
Opinion piece	Vi kan ikke ha et analogt forsvar i en digital verden	Large volume of digital threat activity. Today Norway is dependent on information from allies with similar systems to protect ourselves and therefore we should have an independent ability to protect our digital domain. Bulk interception has gone through a thorough democratic process. TI is not "mass surveillance", but rather "mass storage" (Gram, 2022).
Opinion piece	Uten sikkerhet er ikke friheten og rettssikkerheten fullstendig	Democracies acknowledge their primary duty as security guarantor for its citizens. Secret intelligence is fundamental to national security. To overcome our advisories, it is necessary to have access to personal communication. It involves accepting this ethical risk, which a democracy can regulate through law. Intelligence on terrorism and cyber-attacks comes from large datasets which allows for identifying the communication patterns of potential threats. This is good intelligence, not "mass surveillance". In the UK, digital intelligence, together with traditional methods, have prevented 15 terror attacks within the last 18 months (Omand, 2020).

Opinion piece	Tilrettelagt innhenting styrker vår sikkerhet	Bulk interception has gone through a democratic process**.** It establishes a national ability which ensures that Norway no longer remain exposed to the most advanced cyber threats, nor dependent on receiving information from states with equivalent systems to protect ourselves. We are already late with this system compared to the rest of Europe. NIS is only interested in intelligence relevant data. Unfortunately, not technically possible to filter irrelevant information beforehand. Therefore, there will be strict control mechanisms and due process guarantees. TI will safeguard against the threat actors that wants to undermine our democratic values, freedoms, and rights (Skogen, 2021).
Opinion piece	Digitalt grenseforsvar – samfunnets behov for sikkerhet bør ikke vike for personvernet	Digitalization and the potential for low-intensity hybrid conflicts showcase the need for new tools and laws to secure society. Bulk interception can help mitigate these threats. These new security measures require a balancing act we have never faced. We should listen to NIS when they say that we don't have the tools to protect ourselves in the digital domain. The best privacy laws do not protect our digital society from cyber threats. Bulk interception could contribute to protect Norwegian businesses which is a prerequisite for both total defense and NATO art.5. Privacy may be the price to pay to ensure our collective security (Førsund & Utne, 2019).
Opinion piece	Å rope «ulv-ulv»	Cyber-attacks from states and terrorists are the biggest threats. Datatilsynet is cyring "wolf wolf" based on wrong assumptions. Correct information is necessary to prevent a cooling effect. Sweden has had bulk interception since 2008, and there is nothing that indicates that they are communicating differently than Norwegians. To find and target foreign threat actors, it is a technological necessity

		to store, not surveille, cross border communication. Yes, there will be data of Norwegians in the metadata storage that we won't be able to remove in advance, but it is surplus data which NIS' employees won't have access to. It will be deleted automatically after 18 months. Access is controlled by the courts, and EOS-committee will oversee that the approval is followed. Norway can no longer remain vulnerable and "blind". Allies and partners already have similar systems in place, and most of them have fewer control mechanisms in place than us. No known alternative solutions. EMD acknowledge the necessity for such a system. Datatilsynet doubts the courts, EOS-committee and Stortingets ability and will to prevent *formålsutglidning* – I don't. The law doesn't open for a "back-door." Surplus data will not be used to support police duties, except in instances where it can prevent a serious criminal offence. Foreign intelligence is legitimate, necessary, and complex (Lunde, 2019).
News article	E-sjefen: Frykter dataangrep mot stortingsvalget	NIS won't be able to discover and prevent terror planning and other threats without bulk interception. If it is not implemented politicians must take responsibility for the shortcomings of NIS. Disinformation campaigns is a primary concern, especially towards elections. Cyber-attacks considered acts of war; society put in "check mate" without digital boarder control. I understand that it is a choice between the plague or cholera, but important to demonstrate that the control mechanisms work. This is not mass surveillance. NIS will not focus on fighting crime, only foreign intelligence. Other states have this kind of system, and we could ask for information from them, but then there is no Norwegian court approval, and

		unlikely that we will be prioritized. We will also have to explain why we are requesting certain information, and they will take copies, which means we will not have national control of the data. The surveillance pressure towards Norwegians may decrease, because we want to be as surgical as possible (Johnsen, 2017).
Opinion piece	Nei, det blir ikke masseovervåking av norske borgere	Bulk interception is not mass surveillance. It is mass storage of metadata that crosses the border. Norwegian communication will be filtered out (as much as possible). Search requires court approval, and the content will not be stored. The purpose is for foreign intelligence, not surveillance of citizens, which is a fundamental prerequisite. Bulk interception will have several security mechanisms and it is within EU court rulings. We have agreed to strengthen EOS-committee and courts. Difficult balance but believe we have found a good solution. Good intelligence important for defense and security. Today, we are dependent on allies for this kind of information. A national system will strengthen domestic intelligence ability. In addition, we will be more able to discover and counteract foreign threats (Gram, 2022).
Opinion piece	Ny e-lov gir bedre beskyttelse mot digitale angrep	Access to the data is strictly regulated: NIS can only search for metadata and store content data by court approval. Independent control before, during and after. Only for foreign intelligence. Surplus data can only be shared when there is a threat of life, health or freedom, not ordinary cases. Difficult to balance security and privacy concerns, but it is necessary to collect the data to protect Norway. Foreign intelligence is fundamental to Norwegian defense and security (Bakke-Jensen, 2020).
Opinion piece	Ja, vi har nytte av å lagre metadata	There is a need for bulk interception of metadata, and there is no alternative which is less invasive and

		that can fulfill the need. Experts and experience from other states supports this view. British report claims that 50% of British intelligence on terror and 95% on cyberattacks, comes from bulk interception. Comparable countries have this system because it is valuable. Bulk interception is a prerequisite for more targeted methods. There is independent control before, during and after (Skogen, 2020).
Committee report	Digitalt grenseforsvar (DGF) Lysne II-utvalget	The biggest threat to national security is from cyberattacks and terrorism, and NIS have minimal tools to prevent them. There is no essential difference between collection through open sources, satellite and fiberoptic cables with regards to human rights. Bulk interception allows for independent intelligence production and can increase Norway's access to other relevant data if traded. Bulk interception is just another component of the total picture. Other comparable states collect data in bulk. Furthermore, Norway has a duty to prevent that Norway is used as a transit country for cyberattacks, fight terrorism, proliferation, and more. There are several consequences by not having a system for bulk interception: threats won't be discovered and stopped; lower quality intelligence to decision-makers; reduced standing among allies; increased activity from NIS, PST and NSM to make up the gap as best possible, which demands more resources, and some methods may be even more invasive (Lysne, Grytting, Jarbekk, Lunde, & Reusch, 2016, ss. 28-32).
Hearing response	Justis- og beredskapsdepartamentet	Hybrid threats warrant the implementation of bulk interception. Relevant information to decision-makers requires bulk interception and to solve NIS' fundamental tasks. Important to collect information independently to ensure sovereignty. Sharing surplus data that can prevent other serious crimes,

		such as murder, or child abuse, and should be allowed (Justis- og beredskapsdepartement, 2019, ss. 2-3).
Hearing response	Nasjonal sikkerhetsmyndighet (NSM)	Current threat assessment warrants a system for bulk interception. Relevant and timely information is central to safeguard the nation. No viable alternative to bulk interception. It will be complementary to NSM's VDI-system and therefore relevant information obtained through bulk interception should be shared with NSM (Nasjonal sikkerhetsmyndighet, 2019).
Hearing response	NUPI – Norsk utenrikspolitisk institutt	Important to have an independent national capability to gather data through bulk interception. Omitting bulk interception will send a signal to allies/others that Norway takes cybersecurity lightly, which will make cooperation difficult, and lead to less access to their data. Data is an "international commodity" and all of Norwegians data is already collected by other intelligence agencies and commercial actors. The debate is more about who and how data can be collected – whether NIS should be allowed to take part in this activity which is already being conducted. Because the law is "technology neutral" EOS must be strengthened with necessary resources (Norsk utenrikspolitisk institutt, 2019).
Hearing response	Politiets sikkerhetstjeneste (PST)	The threat situation, and the need for national control of cross-border communication, makes bulk interception necessary. Information collected through bulk about terror incidents should be exempted from the ban on information sharing and be used as evidence in a court of law (Politiets sikkerhetstjeneste, 2019, s. 9).
Judicial analysis	Rettslig analyse:	The European Court of Human Rights found that the Swedish system for bulk interception was in violation of the right to privacy, due to weak legal

	Etterretningstjenesteloven kapittel 7 og 8 i lys av dommer fra Den europeiske menneskerettsdomstolen og EU-domstolen	basis for sharing information and weaknesses related to post-inspection (Forsvarsdepartementet, 2022, s. 5). In the UK case, ECHR found that the system was in violation of the right to privacy, due to inadequate guarantees against arbitrariness and abuse (Forsvarsdepartementet, 2022, s. 6). Furthermore, ECHR recognizes state's need for bulk interception, and that there are no adequate alternative solutions (Forsvarsdepartementet, 2022, s. 7). The conclusion is that Norway's system complies with the requirements of the ECHR (Forsvarsdepartementet, 2022, s. 19). In separate British, French, and Belgian cases requiring communication service providers to store or transfer data to security services for reasons of national security, the EU court found that all cases were in violation of privacy rights. These rulings are not directly binding for Norway (Forsvarsdepartementet, 2022, s. 20). However, Norway is bound by EU's Data Privacy Directive, which is currently under review and is set to be replaced. The timeframe for this is unclear, and it should therefore not be a hindrance to implement the system, as CSP's transfer of data for national security reasons is recommended to not be part of the new directive. Furthermore, the criteria for bulk interception, which is threats to national security, should be further specified in §7-3. A review should be conducted for this reason, and therefore §7-3 should be postponed, but it is not a hindrance for the rest of chapter 7 and 8 to come into effect (Forsvarsdepartementet, 2022, s. 36).

Table 1: Arguments in favor of bulk interception

Critical		
Type	Title/Author	Main arguments
Opinion piece	Opprop mot Tilrettelagt Innhenting	The bulk interception system is a violation of human rights and the Constitution. Targeted methods are adequate to perform NIS' tasks. It is mass surveillance, and there is a huge potential for abuse. Metadata reveals a lot more information than what is perceived. The benefits of the system are questionable, and it can cause a cooling effect. It will allow for a backdoor to circumvent encryption. It weakens the affected companies' ability to compete in the market (Arvesen, Bakke, Brodwall, & Lysaa, 2020).
Editorial	Aftenposten mener: E-tjeneste i juridisk gråsone	NIS will be operating in a legal grey zone with the bulk interception system. Privacy must be the main focus of the law. The public's trust is essential to the secret services, and therefore it is important to ensure there is no grey zones (Aftenposten, 2016).
Opinion piece	Lysne-utvalget har feilet i oppgaven sin – det finnes allerede et digitalt grenseforsvar i Norge	The VDI system is already performing the task of protecting our digital infrastructure. Instead of mass surveillance of the population the government can surveille important institutions, critical infrastructure, and companies. Bulk interception could destroy privacy. The government should rather expand and improve VDI, than implement a system for mass surveillance (Jørgenrud, 2017).
Opinion piece	Digital masseovervåking	Bulk interception is digital mass surveillance. The intelligence service will face a dilemma by having information about a domestic threat they are not supposed to know about. The system will increase the government's knowledge of individuals which will shift power from the individual to the state. This may also cause a cooling effect. The law does not comply with ECHR's surveillance requirements. Allowing NIS to perform machine tests and analysis will ensure that the court's involvement is too late (Coll & Nielsen, 2022).

Opinion piece	Etterretning, etterrettelighet og moderne lovgiving	The amount of data collected, combined with machine processing, will be too large to actually be useful. There is a huge potential for abuse. The government should begin with designing the control mechanisms before developing a system for collection to ensure adequate security (Andersen, 2019).
Opinion piece	Et oppgjør med den nye E-tjenesteloven	There is limited documented value of bulk interception. The protection of journalist's sources is reduced. There may be a cooling effect and plenty of ethical issues. It may be a steppingstone for future expansion of surveillance (Hoff, 2020).
Opinion piece	Nytten av masseovervåkning er ikke godt nok dokumentert	There is limited documented value of bulk interception. Bulk interception is mass surveillance. On the other hand, the negative effects of state surveillance are well documented (Simen, 2020).
Opinion piece	Etterretningssjef med utestemme	The law contains many unclear aspects. If everyone that is critical to the system just haven't understood how it works, then that is a major problem. Trust in the intelligence service may erode. It is easy to draws parallels to the Data Storage Directive (Thon, 2019).
Press release	Etterretningslov: Støtter forslaget. Tar dissens om omfattende overvåking	The bulk interception system is too invasive. There is a real fear of "formålsutglidning", and it may cause a cooling effect. It is a violation of the right to privacy (Haugsvær, 2020).
Opinion piece	Masseovervåkning uten sidestykke	The system is certainly mass surveillance. The court's approval will just be a formality. Meta-data reveals a lot of information. The issue is not lack of trust in our government, but rather that the storage facility can be hacked, and data can be stolen, which could lead to reduced trust in the government. The control mechanisms must be enhanced**,** and it should include a "suicide"-button (Haugsbø & Harkestad, 2022).
Opinion piece	Tilrettelagt innhenting og etterlevelse av EØS-rettslige forpliktelser	The system is not in accordance with ECHR requirements. The main difference is whether Communication Service Provider is storing the data or NIS is storing the data. If the CSP's are storing the data,

		then it is a better solution. Stopping anti-democratic attacks should not take the form of anti-democracy (Juliussen, 2021).
Committee report	Digitalt grenseforsvar (DGF) Lysne II-utvalget	The bulk interception system requires access to Norwegian citizen's communication which is irrelevant to NIS. CSP will have to be the "middleman" (Lysne, Grytting, Jarbekk, Lunde, & Reusch, 2016, s. 33). There is a risk of "formålsutglidning", and there could cause a cooling effect. It does reduce privacy and protection of communication. There is also the risk of abuse (Lysne, Grytting, Jarbekk, Lunde, & Reusch, 2016, ss. 33-35)**.**
Hearing response	Nasjonal kommunikasjons-myndighet	It is very important to have a proper control mechanism (Nasjonal kommunikasjonsmyndighet, 2019, ss. 3-4). The duty to facilitation is so invasive towards communication and privacy rights that there must be explicit requirements to when and how the duty comes into play, and the decision-process is traceable. Important to not include that encryption is reduced more than necessary. Nkom should be notified about the installation of equipment to ensure that Nkom can fulfil their tasks (Nasjonal kommunikasjonsmyndighet, 2019, s. 6).
Hearing response	Norges institusjon for menneskerettigheter	Bulk interception is a violation of privacy. The limits of the purpose of the system must be specified further. Important to further limit the opportunity to use bulk interception towards people in Norway. Sharing data from the system for police purposes must be further specified. The duty to facilitate and choice of CPS' must reflect that NIS only have access to the CPS (ergo further specified, and not as open) see §5-4. "Reason to investigate" (§5-1 and 2) must be specified further. Court control should come at an earlier stage, particularly when the duty to facilitate is invoked, and it should have a time limit to ensure continued evaluation. Must be independent (from NIS) and proper competence available to the courts. Must state clearly that the courts

		have access to all relevant information. There should always be a lawyer present §8-5. To ensure a qualitative proper judicial review, NIM believes it is important that criteria are established such as delimits the scope of the petitions, particularly the search terms, some which might be prohibited. EOS committee control should be improved in terms of working method and ability to make binding decisions, such as cancelation of ongoing search or deleting data (Norges institusjon for menneskerettigheter, 2019).
Hearing response	Amnesty International	Bulk interception is a serious intervention of privacy. Not documented well enough the effectiveness of it. It could lead to a cooling effect. There should be court control, which entails increasing the courts competence. Sharing intelligence with other states' intelligence services could contribute to human rights violations, and it could increase with bulk interception (Amnesty International, 2019).
Hearing response	Tekna - Teknisk-naturvitenskapelig forening	It is questionable whether the benefits outweigh the costs of bulk interception. We are worried about lack of competence within the control mechanisms, the security risks, and the potential negative effects for Norwegian web-based services. There is also the negative effect on privacy, and potentially a cooling effect, purpose slippage, and reduced trust in government. EOS-committee must be strengthened if the law is passed (Tekna - Teknisk-naturvitenskapelig forening, 2019).
Hearing response	Datatilsynet	The system is mass surveillance, and it is too big of a violation of privacy. It endangers our democracy. There is potential for a cooling effect. It becomes a shift in power from citizens to the state. There is potential for "formålsutglidning". The law does not comply with ECHR requirements. There are several unclear formulations. Furthermore, it is not proportional. Lack of effective control. Privacy should be built into the law.

		The filtration system will not be able to remove adequate amounts of Norwegians data (Datatilsynet, 2019).

Table 2: Arguments against bulk interception

6 Analysis

Following presentation of the results, but before beginning the analysis, this section will provide a translation and definition of the term "formålsutglidning" and explain how *bulk interception* became the term for "tilrettelagt innhenting" in English. Then, the key findings will be introduced followed by a presentation of the in-depth analysis. The analysis will be guided by the four analytical tools presented in the methodology chapter and offer different perspectives on the impact, purpose, strength, and weaknesses of the argumentation. Furthermore, this chapter will be divided into a *in favor* and *critical* section, in accordance with the presentation of the results.

6.1 Translation and definitions

The term "formålsutglidning" is used several times by different texts, most notably by the ones critical to bulk interception. It refers to the use of information for other purposes than originally intended (Teknologirådet, 2007). It is used as a fear that bulk interception may be used for other purposes than foreign intelligence. This is understood to be a gradual development, and not a sudden change. An alternative English term could be "multi-purpose", in that critics fear that bulk interception will become a multi-purpose tool. However, it does not convey the full meaning as it does not include that it will be gradual. This is why the original Norwegian term has been included directly.

The most central term to this thesis and to the discussion in general is the Norwegian term: "tilrettelagt innhenting". Throughout this thesis, it has been replaced by *bulk interception*. The reason for this is due to its similarity to the United Kingdom Investigatory Powers Act 2016. To begin to understand the term it is reasonable to begin with the Norwegian definition of it. The Norwegian definition of bulk interception is found in chapter seven of the intelligence law, and it states that for the purpose of intelligence production, the intelligence service can collect and store electronic information that crosses the Norwegian border in bulk (Etterretningstjenesteloven, 2021). It is primarily metadata that will be collected. Furthermore, it places a duty to facilitate the collection on Communication Service

Providers (CSP). In addition, it allows for the targeted collection and storage of content data, so long as it is in accordance with court rulings. The Investigatory Powers Act (IPA) has divided these powers into two separate ones. Their bulk interception power allows for the collection of a volume communications from people outside the UK for the purpose of foreign intelligence and uncovering threats to the UK (Home Office, 2015, s. 1). The duty to facilitate and the ability to perform targeted collection is found in the targeted interception powers of the IPA (Home Office, 2015, s. 1). This entails that targeted interception could have been used instead of bulk interception, however, the collection of metadata in bulk is the primary function of the Norwegian system and therefore bulk interception is a more accurate term.

6.2 In favor

The positive texts make several arguments in favor of bulk interception. By examining the different arguments there are four key themes that emerge. These area *Norway as an outsider*, the *threat environment*, *democratic process and control*, and *mass storage*. These themes are connected by an overarching theme of *national security*. In the following, these themes will be examined further, together with their supporting arguments.

6.2.1 Norway as an outsider

By pointing to the fact that other states, both allies and others, already have a system for bulk interception of cross-border data, is framing Norway as an outsider. Following this statement, is the argument that NIS is dependent on receiving information gathered by bulk interception systems from allies to provide the adequate intelligence (Bakke-Jensen, 2020). This "dependency" is framed as problematic for the intelligence service. It requires NIS to justify the reason for the request for information, and lack of domestic control, exemplified as the other agency will keep a copy of the information (Johnsen, 2017). Although it is not stated specifically, it is possible to interpret that requests can be denied, which will negatively affect the service's ability to provide information to decision-makers. In addition, foreign agencies might collect more data than requested, which undermine Norwegian control and privacy. None of the texts argue that this situation undermines Norwegian sovereignty, however it is certainly implied by the use of different terms such as "independent intelligence production" (Lysne, Grytting, Jarbekk, Lunde, & Reusch, 2016) or "national ability" (Skogen, 2021). Framing Norway as an outsider invokes negative feelings in the reader, and a desire to

become part of the in-group. The underlying conclusion is that bulk interception will "restore" Norwegian independence and sovereignty.

Another supporting argument is the negative impact omitting bulk interception will have on Norway's status among allies and ability to comply with international commitments. NUPI argue in their hearing response that omitting bulk interception will send a signal to allies that Norway takes cybersecurity lightly, and it will make cooperation difficult (Norsk utenrikspolitisk institutt, 2019). This implies that Norway will be a weak spot in NATO, which is a position Norway should not occupy as NATO is essential to Norway's security. Another text claim that Norway is mentioned in ISIS propaganda as a good transit country due to lack of control (NTB, 2019). Associating Norway with ISIS in this way, frames Norway as an enabler of terror by omission and not intentionally. These arguments exacerbate the image of Norway as an outsider.

To further support the value bulk interception will bring towards securing Norway, one opinion piece provides statistics from the UK as a parallel to the benefits it will bring with it (Omand, 2020). Providing statistics on terrorism prevention makes the value quantifiable and more objective, which thereby makes it easier to convey. Compared to qualitative value descriptions, numbers appear less subjective and more believable. However, this line of argumentation quickly runs into problems as full statistical insight is for reasons of secrecy difficult, and it weakens the statistics' positive impact.

On the other hand, NUPI's hearing response downplays the "problematic" nature of data collection by framing data as a "international commodity" and that Norwegian's data is already collected to such a large extent and that this debate is not about data being collected, but rather if NIS will be allowed to participate (Norsk utenrikspolitisk institutt, 2019). There is a high level of probability that much, if not all, of Norwegian's data is already collected, especially by commercial private companies. This is an interesting argument as it brings forward the fact that Norwegian citizens to a large extent accept data collection for economic interests, but when it comes to Norway's national security it is met with significantly more scrutiny and reluctance.

6.2.2 Threat environment

The threat environment is a theme that is brought forward directly or indirectly in almost all texts. In some texts it is only mentioned as a reason for supporting bulk interception. Others give some examples to what the threat environment consists of.

Cyberattacks, terrorism, and hybrid threats are frequently mentioned components of the threat environment. The central concern is that NIS does not have the tools necessary to discover and counteract these threats and characterize Norway as being vulnerable (Johnsen, 2017). Bulk interception is presented as the missing piece that will ensure Norway's security. This is a tall order to set in terms of the effectiveness of the method. The expectations readers could be left with, might be greater than what can be delivered and may create issues of trust in the intelligence and security services long-term. Anecdotal evidence, such as claiming that there will be celebrations in Russian and Chinese spy agencies if Norway does not implement bulk interception (NTB, 2019), is meant to support the theme.

Another text argues that since we do not live in an ideal world, we must adapt to changes in our environment without falling into "ideological trenches" to protect different rights and freedoms without debate (Seglsten, 2022). In addition, other invasive tools might have to be implemented in the future, due to negative changes in our environment. This line of argument is rooted in the "realism-idealism" dichotomy. By using the term "ideological trenches", the message is that the opposition must be more flexible in their stance and allow for a more "realistic" perspective. It is meant to "ridicule" or "belittle" the critics "idealistic" opinions, and frame it as incompatible with the "real-world".

Bulk interception is also presented as a way to protect the values and rights Norway population currently enjoys. However, there is a logical mismatch in the argumentation. To protect rights and values, it must at times be broken. One text goes further by suggesting that to secure the collective, it is necessary to sacrifice individuals' privacy (Førsund & Utne, 2019). However, although there is a logical mismatch in this line of argument, it is widely understood that the rights that all ordinary "well-intended" individuals enjoy, unfortunately provide "cover" for those with malicious intent. This is directly followed by the third supporting theme, which is that of democratic process and control.

6.2.3 Democratic process and control

To counter the issue of protecting rights and freedoms, they at times must be broken, most of the texts highlights how there has been a democratic process and there will be several control mechanisms which will ensure that there is a fair balance. Some texts only mention that there has been a lengthy democratic process to improve and adjust the law in general, and bulk interception in particular. This argument is certainly valid. The report that this thesis treats as the "starting point" of the discourse, the Lysne-committee report, was published in

2016. Other texts are more direct in their commentary of the process. One text state that there should be an appreciation for such an open process as many states implement this tool without informing the public (NTB, 2019). It is an attempt to put a positive stamp on the openness and the virtues of the intelligence service and Norwegian democracy. However, any citizen of a democratic state, should take it for granted that such a significant change in the intelligence services power would be publicly debated, especially if it greatly impacts their privacy. In this context, the statement could be interpreted as the intelligence service is doing the citizens a favor by having a public debate. This is certainly an unfortunate attitude to convey.

Another text focus on the core objective of a democracy, which is providing security to its citizens (Omand, 2020). It argues that secret intelligence is fundamental to this task, and the issue of breaking rights to protect rights, can be regulated through law. This argument is a nod to Hobbes and the social contract. It also brings forward the benefits of democracy when this kind of tool becomes necessary. A democracy has certainly as one of its prime objectives to provide security for its citizens. However, it is also tasked with securing multiple rights and freedoms. The key is to ensure that the democratic control mechanisms manage to balance these objectives properly. Most texts, both positive and negative, acknowledge this. Oslo District Court will control the access and the EOS-committee will oversee that the collection is according to the court's directive (Bakke-Jensen, 2020). This seems like proper democratic control by having a system of checks and balances in which a judiciary and legislative agency oversee an executive agency's power execution.

The question of sharing surplus data is also found within this theme. Other agencies are interested in surplus data that could prevent other serious crimes or that could be relevant to their area of operations (Nasjonal sikkerhetsmyndighet, 2019). To prevent NIS from sharing information that could prevent serious crimes seems counterproductive, and it is therefore exceptions for emergencies. The issue is if the definition of emergencies widens, which will be a form of "formålsutglidning". However, prevention of serious crimes is a valid reason to share information with the appropriate agencies. One text is very confrontational with regards to this issue by accusing Datatilsynet of sowing doubt and crying "wolf-wolf" over the EOS-committee and the courts ability to perform their role (Lunde, 2019). The purpose of these accusations is both to discredit the concerns and show support to the control mechanisms. However, the confrontational tone is dismissive, rather than reassuring, to counter legitimate concerns. This gives the impression that there is no willingness to accommodate nor negotiate. Another unfortunate attitude to convey.

The last argument within democratic control is foreign intelligence as legitimate. Although the positive texts acknowledge that bulk interception is a violation of some human rights, especially the right to privacy, they consider the violation legitimate (Lunde, 2019). The legitimacy is built on intelligence vital role in ensuring national security, and within the boundaries set by Norway's international commitments to human rights. Intelligence's role in national security is difficult to argue against, and most negative texts also acknowledge this. Whether the bulk interception system is within the boundaries set by human rights is the area of contention. In the aftermath of two European Court of Human Rights (ECHR) court rulings, the Norwegian government performed a judicial analysis on the potential impact Norway's system for bulk interception. It found that the Norwegian system complies with the requirements set by the ECHR (Forsvarsdepartementet, 2022). Furthermore, it found that although Norway is bound by the Data Privacy Directive, it is currently under review, and it is expected to take years to conclude. Furthermore, the transfer of data from Communication Service Providers to security services for national security reasons is recommended by multiple states to not be part of the new directive. In addition, it found that the ECHR acknowledge that states may find that a system for bulk interception is necessary for national security reasons. The conclusions lend judicial support to the claim that the Norwegian system is within reasonable human rights boundaries. However, as the assessment has been conducted by the government, it is open for discussion whether an independent analysis would arrive at a different conclusion.

6.2.4 Mass storage

The last supporting argument is that the system is one of "mass storage", and not "mass surveillance" (Gram, 2022). Texts negative towards the bulk interception system have framed the system as "mass surveillance". The use of the term "mass storage" in exchange for "mass surveillance" is primarily to present the system as less invasive and remove the negative connotations that accompany surveillance. "Mass storage" may be perceived as significantly less troublesome than "mass surveillance". In addition, it is an attempt to reclaim ownership of the terminology. The reason being that the one that is able to dictate the "frames" of the discourse, such as the terminology, will gain a significant advantage.

It is also a skewing of the focus on one specific part of the system, the collection and storage, rather than encompassing the entire system, which includes what the data will be used for. It is also a direct engagement with those who claim the system is "mass

surveillance". Presenting the systema as "mass storage" is reactive, rather than proactive. By changing the term, the aim is to gain acceptance for it. The introduction of the term "mass storage" opens up a debate over what we consider surveillance to consist of. The most common description may be of Orwellian nature. However, it is certainly a spectrum, and it is this spectrum this argument is attempting to exploit, and to distance the system as far as possible from the Orwellian representation.

6.3 Critical

As with the positive texts, the negative texts also have an overarching theme with several supporting arguments. Overall, the negative texts have *privacy* as their overarching theme. In addition, there is four key themes: *violation of human rights*, *mass surveillance*, *limited value*, and *the public's trust and control mechanisms*. In the following, each theme will be examined with their supporting arguments.

6.3.1 Violation of human rights

The first supporting theme is found in multiple texts. It is both a direct challenge to the overarching theme of national security and an attempt to reframe the debate as one of human rights. Although the texts point to the fact that the bulk interception system will impact multiple rights, such as freedom of expression and freedom of communication, the issue is mostly the negative impact it will have on the right to privacy. This is due to the nature of modern communication. Most of Norwegians communication will cross the border, despite both sender and receiver being in Norway. The bulk interception system will therefore naturally collect Norwegian's ordinary communication. The government acknowledge this issue but attempts to assure critics that this communication will be filtered out (Gram, 2022). The counter argument is that it is not technically possible to filter out all information and it raises privacy concerns (Datatilsynet, 2019, s. 10). Bringing up the technical limitations of the filtration, is an effort to move the discussion from general and down to the details to sow doubt. It is a clear tactic in accordance with to the well-known saying "the devil is in the details".

Furthermore, some negative texts claim that the system does not comply with human rights requirements for surveillance systems. The argumentation points mainly to requirements that the European Court of Human Rights have used in previous and, at the time, ongoing cases. One text points to the issue of who is storing the data as a vital

difference (Juliussen, 2021). If the CSP are storing the data instead of the intelligence and security service, then the system will to some extent be within the requirements. Again, a focus on the specifics. By involving a supranational institution, the critics are attempting to improve their standing vis-à-vis the state. It shifts the debate from "bilateral" to "multilateral" by involving a third party and it aids in evening out the power disparity between the opposing sides.

Lastly, the issue of protecting rights by breaking rights is also addressed by some negative texts. The argument is that bulk interception is an anti-democratic tool, and therefore it has no place in protecting a democratic society (Juliussen, 2021). It clearly states the logical mismatch of the issue and is meant to use the influence of logic to persuade the audience that the system should not be implemented. Between the lines it is possible to interpret that it is an accusation of hypocrisy, as Norway criticize other states for violating human rights by means of surveillance, and now the government wants to implement mass surveillance themselves.

6.3.2 Mass surveillance

Closely connected to the issue of protecting rights by breaking rights, is that of mass surveillance. The labeling of the system as "mass surveillance" is to invoke feelings of an Orwellian nature in the audience. With regards to the timeline, critics were using the mass surveillance label early in the debate, which afforded them power of definition. This is a powerful tool and put the supporters in a defensive position. The supporters had to attempt to explain why that is an incorrect label, and eventually the term "mass storage" was presented to compete with the other. How successful each label was is difficult to estimate, however, "mass surveillance" is a term with a wide understanding and needs no further explanation. With the term "mass storage" the specifics of the system must be brought forward, which weakens its usage and persuasive power.

However, labeling the system to support the critics view is not the only reason to use the term "mass surveillance". The system will collect metadata in bulk. Several texts point out that despite metadata giving the impression of being less "harmful", it can reveal more information than perceived. By combining the different datapoints that metadata consists of, it is possible to make very accurate assumptions about an individual, otherwise known as profiling, and thereby reveal a significant amount of information (Haugsbø & Harkestad, 2022). The "mass surveillance" label offers the critics definition power, and it rests on a technically solid foundation.

6.3.3 Limited value

The third supporting theme is the issue of the benefits of bulk interception. Some texts point to the fact that the benefits that are presented by the government are without substantial public evidence (Simen, 2020). The value of the system is therefore difficult to determine. This difficulty is due to the secrecy that is a fundamental part of the security and intelligence services. The proponent's claims may be true, but without any way to support the claims with verifiable and empirical documentation, it becomes an issue of trust. This is one of the core weaknesses of the positive argumentations which critics exploits. Making grand claims quickly becomes hollow when evidence cannot be presented. On the other hand, as one text points out, the negative effects of state surveillance are well documented (Simen, 2020).

Another text argues that the amount of data will be so large that it cannot be beneficial (Andersen, 2019). Someone that is potentially a threat will be like looking for a needle in a haystack and the system will fail to live up to its promises. This is another well-known challenge for intelligence and security services, as well as companies and individuals. By pointing out that NIS may experience the same issue as companies and individuals face, the critics are able to familiarize their argument with the public and win support for their views. In dealing with the public, the intelligence services need for secrecy becomes a problem which undermines their argumentation from the beginning.

There is one text that offer a counterargument to the claim that there is no alternative solution to bulk interception (Jørgenrud, 2017). The warning-system for digital infrastructure (in Norwegian: varslingssystem for digital infrastruktur (VDI)) is a system of "penetration detection sensors" placed in important public and private institutions and companies to discover if there is a breach or attempt of breach of their systems (Nasjonal sikkerhetsmyndighet, 2022). This suggestion is directly addressing one of the tasks of the bulk interception system, which if that of protecting digital infrastructure. This argument carries some weight as it plays a part in digital infrastructure protection; however, bulk interception is primarily intended to collect foreign intelligence, which in turn will aid in the protection of Norway. This may be the reason why there are few texts that bring forward the role of VDI, and rather focus on the limitations or abolishment of the bulk interception system.

6.3.4 The public's trust and control mechanisms

The last key supporting theme of the negative side is that of the public's trust and control mechanisms. As have been presented already, this theme is connected with the secrecy that is intrinsic to the intelligence world. These services are dependent on the public's trust, and by suggesting control mechanisms, there is an attempt to compromise and tackle this issue directly. However, critics have several concerns regarding the control mechanisms that in sum may impact the public's trust.

The most prominent concern is that the control mechanisms lack the necessary competence to be effective (Norges institusjon for menneskerettigheter, 2019). One text fear that court approval may turn into a formality (Coll & Nielsen, 2022). This concern is rooted in the technical aspects of the system. It requires significant technical expertise for the mechanisms to be fulfilling their tasks. The concern is further connected to fear of abuse, a cooling effect, and multiplying the systems purpose ("formålsutglidning"). By bringing forward the lack of competence and the connected fears, the negative texts are able to sow doubt about the court and the EOS-committee's ability to perform their role. Thereby they gain support for their view that the impression of proper democratic control is false. It is a counterargument to how well democracies can regulate these ethical risks through law. Clearly, law is not enough, and once again the importance of the details become confirmed.

Furthermore, several texts worry that the law in general is too vague, and it will allow for a grey zone that can be exploited to expand the purpose of the system (Aftenposten, 2016). This issue is connected to the limited value theme, in that the negative effects of state surveillance is well documented. The underlying argument is that the shift of power from the people to the government is too extensive and carries too much risk to be allowed.

Lastly, there is the issue of Norwegian's data being collected. Norwegian's data is regarded as irrelevant for the intelligence service. Both the positive and negative texts have acknowledged this. The majority of the positive texts attempt to downplay the issue by assuring that most of the data will be deleted immediately and whatever is left is deleted after 18 months (Lunde, 2019). The critics partly base their mass surveillance claim on the length of storage. It can be understood that having access to this information for 18 months will be too tempting to be left alone and therefore it carries a large potential for abuse. Combining all of these issues the concern is that the system and faulty control mechanisms will gradually erode the public's trust in the government and democratic institutions. Therefore, many texts advocate for a significant strengthening of these mechanisms to counter these issues, despite a

general view that the system should not be implemented, due to the forementioned faults and limitations.

7 Discussion and Conclusion

In the following section, the findings will be critically discussed. It will begin with a brief summary of the findings and then it will place the findings into a broader context. Next, our attention will turn towards discussing the results from a theoretical perspective and provide an answer to the research questions. Lastly, the limitations and possible implications of this thesis will be discussed.

7.1 Summary of study results

The purpose of this study was to gain a better understanding of the potential impact bulk interception will have on both Norwegian national security and privacy. The results have provided some interesting insights. The findings strongly imply that there is potential for significant impact on both ends, and it can be summarized into three main categories. First, there is the issue of the value of bulk interception in terms of increased security. Proponents claim that bulk interception will remove some of Norway's "problematic" dependency on other states and may bring Norway a higher status among allies. In addition, the intelligence service will gain a robust ability to counteract terrorism, cyberattacks, and unwanted intelligence efforts, among others. On the other hand, critics argue that these claims lack substantial supporting evidence, and that the consequences on privacy are significantly better documented.

Second, the consequences it will have on individual's privacy. The opposite sides contest the extent of the intrusion on privacy. The supporters of the system argue that it is "mass storage" rather than "mass surveillance", and its purpose is legitimate foreign intelligence. Furthermore, the system is in accordance with the European Court of Human Rights' requirements for bulk interception. Critics present a different interpretation of the ECHR's requirements and find the system not to be in accordance with them. In addition, bulk interception of all cross-board data is regarded as a violation of privacy rights from the offset, and correctly termed "mass surveillance". They also highlight the potential for abuse, a cooling effect on the public, and that the purpose of the collection will multiply

(formålsutglidning"). Taken together, these concerns support the omission of bulk interception, or at least the substantial strengthening of the control mechanisms.

Third, the design and ability of the control mechanisms. The proponents of bulk interception argue that by involving both a judiciary and legislative control mechanisms, represented by Oslo District Court and the EOS-committee respectively, there is proper democratic control of this system. The critics agree that both of these institutions must be involved for proper control. However, their concern is connected to their technical competence of the system. For effective control, both must be strengthened, and there is doubt that the resources dedicated are not adequate.

7.2 The Norwegian case in a broader context

The Norwegian case finds itself as one of the latest additions to a growing field. The pattern of results is consistent with previous literature in that privacy has established itself as the main right to be impacted by developments in the security field – privacy can increasingly be considered a "currency" to "purchase" security (Dragu, 2011, s. 66). This "new" trade-off can be attributed to the growth of technological surveillance capabilities, such as digital communication, found by Jawaid (2020, ss. 5-6), and consistent with this study. The exposure of secret surveillance programs highlighted in Watt's study (2017, s. 773) is certainly also relevant to the development of the security-privacy trade-off, despite not being a significant part of this thesis. In addition, the findings of this study in regards of the importance of the control mechanisms are consistent with Jawaid's highlighting of proper oversight and the development of laws to regulate surveillance (2020, ss. 5-6).

Past researchers have found that threats towards privacy from intelligence activities rises with an increase in threats towards citizen's security (Pulver & Medina, 2018, ss. 251-252). The present study supports this view as the *threat environment* is a central theme and serves as justification for the implementation of a bulk interception system in Norway.

The contestation of whether these kind of surveillance systems are within the limits of human rights found in this study is certainly in line with previous research. Cooper (2018, s. 119) found that in the New Zealand case, the legislature was framed as ensuring security and respecting human rights. Upon evaluating the laws according to international human rights principles, Cooper's conclusion was that it was not within the requirements. However, these studies differ in that this thesis did not evaluate the system by human rights principles.

Whereas Asaf Lubin (2018, ss. 505-506) found that surveillance directed abroad is met with support and if it is directed domestically, then it is met with opposition, the present study has shown that in the Norwegian context, this is generally not true. Critics argue that despite the system's purpose being foreign surveillance, it represents a substantial threat to Norwegian's privacy. The reason for this inconsistency may be due to the nature of the system and that Norwegians communications will also be collected. However, the negative response by individuals found in the results are consistent with Rønn and Søe's finds that people are generally against information about them being collected (2019, ss. 362-363).

7.3 Findings and the security-privacy trade-off

In Hobbes' Leviathan, free men form a sovereign by giving up their rights and in return the sovereign will provide security. Hobbes' trade-off makes clear that security holds the highest value as it is worth to trade it for all of man's rights. Although the trade-off remains ever relevant, this absolutist trade, is incompatible with a liberal democracy. Liberal values are entrenched in this form of government, and rival security in terms of value. The objective of liberal democracies is to provide both security and liberty. Today, this trade-off takes form in more nuanced ways, by focusing on the trading of specific liberal rights. As shown in chapter three, privacy is a liberal right, that can be considered a "currency" which can be used to "purchase" more security. The Norwegian debate over bulk interception is an example of this. The supporters of bulk interception make clear, security-oriented arguments in favor of the system. Both the *outsider* and *threat environment* themes are clear security arguments. They form the reason for why a bulk interception system is necessary – to secure Norway. In addition, there is an admission from the proponents that the system involves an intrusion of privacy due to the nature of such a system. On the other side, the critics make clear privacy-oriented arguments. The *human rights* and *mass surveillance* themes are certainly privacy focused. Therefore, the findings can be said to be in accordance with the theoretical framework.

Within this overarching security-privacy trade-off, there are three underlying and intertwined contestations. First, the discussion over the value of bulk interception, e.g., whether it actually increases security to such an extent that the loss of privacy is worth it. Second, is the extent of the intrusion, in other words, the mass surveillance – mass storage sub debate. Third, the effectiveness of the control mechanisms. For Hobbes, these contestations might not have needed taken place as the citizens originally formed the state to provide

security, and therefore the state can be considered to have obtained a form of security "carte blanche" from its people. In practice, it is not that simple. The Norwegian case is further complicated, by being about the trading of some, not all of, privacy for increased security, as the government is not proposing to eradicate privacy.

The issue with the lack of a value metric within the theory becomes apparent when comparing a security measure and the privacy "cost". The critics' "limited value" theme contests the proponents claim that bulk interception will drastically increase security. Therefore, the findings do not provide a definitive answer. From an objective perspective it is difficult to determine whether the "price" is "fair". This is where the extent of the intrusion becomes relevant in determining the "fairness". The security perspective focuses on the fact that the purpose of the system is foreign intelligence and not surveillance of Norwegian citizens. On the other hand, the privacy perspective argues that by having Norwegian citizens' data stored and available, it can already be considered mass surveillance. The availability is where the third contestation becomes apparent. The purpose of the democratic control mechanisms is to ensure that the availability of the data does not turn into mass surveillance or other forms of abuse. As long as the control mechanisms are able to prevent the development of any abuse, and that the system is only used for its intended purpose, in addition to providing the promised increase in security, then the "payment" can be considered "fair". Therefore, the extent of bulk interceptions positive impact on Norway's national security is potentially high, however, it is not possible to properly determine the full extent as it requires access to data currently not available. The degree of the effect on Norwegian's privacy is also potentially high, but difficult to determine for those same reasons. Lastly, the possible long-term implications on the dynamics of Norwegian society are both small and large. However, bulk interception may be only the first of several new intelligence capabilities Norwegian society must learn how to manage. It is safe to assume that the balancing act will remain relevant and a continuous challenge for Norwegian democracy.

7.4 Limitations, implications, and directions for future research

There are some potential limitations concerning the results of this study. A first limitation concerns the access to data. All data have been collected from publicly available sources. Due to the nature of this topic, there are limits on the kind of information which has been made available to the public. This means that data which could be useful in answering the research questions are not included. Examples of this kind of information could be

statistics on the number of request the intelligence service has made to foreign services, how often it is granted, and what is required in return. Another example could be statistics on attempted, prevented, and successful terrorist attacks and cyber operations. Both of these statistics would aid in providing an impression of the scope of the issue and gauging how bulk interception is projected to reduce or improve these numbers.

A second potential limitation is that this thesis is a limited analysis of the discourse surrounding bulk interception. The data that has only been collected from written sources and excludes relevant information that could be obtained from interviews or other quantitative methods. However, the available data has been very large and despite attempts to include as much as possible, some data has not been included in the results. This is due to both time-constraints and the researcher's capacity and could have led to some relevant information to go without consideration.

A third potential limitation is the potential for bias. The author has been following and discussing this subject for several years and has formed opinions which could leak into the thesis despite the best efforts taken to achieve an objective presentation. It is important that the reader keeps this in mind.

A fourth potential limitation is that the theoretical approach is of a more "simplistic" nature in that it takes the trade-off as granted and does not consider the possible complex dynamics of security, privacy, and liberty. A more complex theoretical approach could arrive at different findings which could lead to drawing different conclusions.

Despite these limitations, these findings suggest several theoretical and practical implications. The findings support the continued prominence for the existence of a trade-off between security and liberty. Furthermore, it implies that security can be regarded as tradeable to specific rights and freedoms, and not necessarily all liberties at once, which contrasts and nuances Hobbes' absolutist presentation. In addition, it supports the view that privacy is the right that is most impacted by developments of new security capabilities due to technological developments, and it implies that this development will only continue to grow. It is highly likely that this theoretical lens will continue to shape how future discussions on these kinds of topics are conducted.

For the practical implications, the findings suggest that the key to a satisfactory balancing act is effective control mechanisms. Highly effective control mechanisms will mitigate the potential negative consequences on Norwegian democracy and wider society. This entails an increase in both their capacity and expertise, as it will allow them to perform independent control without support from the intelligence service or other executive agencies

who could influence their decisions in their favored directions. In addition, it will support the continued high level of trust between the government and the public. Furthermore, the findings suggest that having a publicly debate for a longer time-period allows for broad collection of perspectives which ultimately leads to an improvement of laws and democratic institutions. This is one of the strengths of democracy, and the intelligence and security service should aim to be as open as possible, and not interpret the process as negative despite opposition.

Lastly, this thesis serves as a first step in the evaluation of the bulk interception system. Future research might aim to provide a more definitive answer to the questions presented in this study as more in-depth data becomes more available. In addition, data should be collected and analyzed to determine potential societal consequences at different intervals to determine if people's habits online have changed due to bulk interception. Furthermore, research of this topic could take the form of a quantitative study, which will provide generalized results. A later study may also apply a theoretical framework which accounts for a more complex relationship between security, liberty, and privacy, which could shed light on possible adjustments to the bulk interception framework. Ultimately, it is important to continue to conduct research into the expansion of intelligence and security capabilities for enhanced national security, both now and in the future.

Works cited

Aftenposten. (2016, Juli 27). *Aftenposten mener: E-tjenesten i juridisk gråsone*. Retrieved March 1, 2023, from Aftenposten: https://www.aftenposten.no/meninger/leder/i/9qGWM/aftenposten-mener-e-tjeneste-i-juridisk-graasone

Amnesty International. (2019, February 12). *Høringssvar fra Amnesty International*. Retrieved March 24, 2023, from Regjeringen.no: https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=80ab5e7a-f6a0-456b-a925-fb28eec589c4

Andersen, E. (2019, April 23). *Etterretning, etterrettelighet og moderne lovgiving*. Retrieved March 1, 2023, from Digi.no: https://www.digi.no/artikler/kommentar-etterretning-etterrettelighet-og-moderne-lovgiving/463427

Arvesen, E., Bakke, S., Brodwall, J., & Lysaa, B. (2020, June 10). *Opprop mot Tilrettelagt Innhenting*. Retrieved March 1, 2023, from Medium: https://medium.com/@ti_opprop/opprop-mot-tilrettelagt-innhenting-507fdc0fb47f

Bakke-Jensen, F. (2020, April 22). *Forsvarsministerens innlegg ved presentasjonen av forslag til ny etterretningstjenestelov*. Retrieved February 26, 2023, from Regjeringen.no: https://www.regjeringen.no/no/dokumentarkiv/regjeringen-solberg/aktuelt-regjeringen-solberg/fd/taler-og-innlegg/ministeren/taler-og-innlegg-av-forsvarsminister-frank-bakke-jensen/2020/forsvarsministerens-innlegg-ved-presentasjonen-av-forslag-til-ny-etterr

Bakke-Jensen, F. (2020, September 14). *Ny e-lov gir bedre beskyttelse mot digitale angrep*. Retrieved March 1, 2023, from Regjeringen.no: https://www.regjeringen.no/no/dokumentarkiv/regjeringen-solberg/aktuelt-regjeringen-solberg/fd/taler-og-innlegg/ministeren/taler-og-innlegg-av-forsvarsminister-frank-bakke-jensen/2020/elovenbeskytter/id2741266/

Bryman, A. (2012). Chapter 22: Language in qualitative research. In A. Bryman, *Social Research Methods Fourth edition* (pp. 521-541). New York: Oxford University Press.

Bryman, A. (2012). Ethics and politics in social research. In A. Bryman, *Social Research Methods 4th Edition* (pp. 129-155). New York: Oxford University Press.

Bryman, A. (2012). Getting started: reviewing the literature. In A. Bryman, *Social Research Methods 4th Edition* (pp. 97-128). New York: Oxford University Press.

Bryman, A. (2012). Sampling. In A. Bryman, *Social Research Methods 4th Edition* (pp. 184-207). New York: Oxford University Press.

Bryman, A. (2012). The nature of qualitative research. In A. Bryman, *Social Research Methods 4th Edition* (pp. 379-414). New York: Oxford University Press.

Coll, L., & Nielsen, J. M. (2022, October 25). *Digital masseovervåking*. Retrieved March 1, 2023, from NRK: https://www.nrk.no/ytring/digital-masseovervaking-1.16151494

Cooper, S. (2018). An Analysis of New Zealand Intelligence and Security Agency. *Auckland University Law Review, 24*, pp. 92-120. Retrieved October 24, 2022, from https://heinonline-org.mime.uit.no/HOL/Page?lname=&public=false&collection=journals&handle=hein.journals/auck24&men_hide=false&men_tab=toc&kind=&page=92

Datatilsynet. (2019, February 6). *Høringssvar fra Datatilsynet*. Retrieved March 24, 2023, from Regjeringen.no: https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=e0b87829-2c74-4f2c-8066-c75801bcd0d5

Dragu, T. (2011, February). Is There a Trade-off between Security and Liberty? Executive Bias, Privacy Protections, and Terrorism Prevention. *The American Political Science Review, 105*(1), pp. 64-78. Retrieved January 23, 2023

Døvik, O. (2020, October 26). *Ny lov for e-tjenesten blir vedtatt*. Retrieved May 6, 2023, from NRK: https://www.nrk.no/norge/flertall-pa-stortinget-for-ny-etterretningstjenestelov-1.15045224

Eoyang, M. (2017). Beyond Privacy and Security: The Role of the Telecommunications Industry in Electronic Surveillance. *Journal of National Security Law and Policy*, pp. 259-282. Retrieved October 24, 2022, from https://heinonline.org/HOL/P?h=hein.journals/jnatselp9&i=269

Etterretningstjenesteloven. (2021). Lov om Etterretningstjenesten (LOV-2020-06-19-77). Lovdata. Retrieved October 12, 2022, from https://lovdata.no/dokument/NL/lov/2020-06-19-77

Etterretningstjenesten. (2022). *Focus 2022.* Oslo: Etterretningstjenesten. Retrieved October 12, 2022, from https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus/rapporter/Focus%202022%20%20-%20english.pdf/_/attachment/inline/2bec2656-0ca8-4556-8878-c3fe2ee3a11e:161a477e1ab332bdf02ed556e6c963251537bf22/Focus%202022%20%20-%20english.pdf

Forsvarsdepartementet. (2022, June 27). *Forslag til endringer i etterretningstjenesteloven på høring.* Retrieved April 5, 2023, from Regjeringen.no: https://www.regjeringen.no/contentassets/054e4ac7519e42c79de8a01229a3c4b4/2021-08-24-helhetlig-rettslig-analyse-ti.pdf

Førsund, B., & Utne, R. (2019, March 22). *Digitalt grenseforsvar – samfunnets behov for sikkerhet bør ikke vike for personvernet*. Retrieved February 26, 2023, from Computerworld: https://www.cw.no/debatt-digitalt-grenseforsvar-sikkerhet/digitalt-grenseforsvar-samfunnets-behov-for-sikkerhet-bor-ikke-vike-for-personvernet/778420

Galtung, J. (1969). Violence, Peace, and Peace Research. *Jorunal of Peace Research*, pp. 167-191.

Gram, B. A. (2022, October 21). *Nei, det blir ikke masseovervåking av norske borgere*. Retrieved March 1, 2023, from NRK: https://www.nrk.no/ytring/nei_-det-blir-ikke-masseovervaking-av-norske-borgere-1.16147557

Gram, B. A. (2022, October 31). *Vi kan ikke ha et analogt forsvar i en digital verden*. Retrieved February 26, 2023, from NRK: https://www.nrk.no/ytring/vi-kan-ikke-ha-et-analogt-forsvar-i-en-digital-verden-1.16159366

Haugsbø, E., & Harkestad, I. (2022, October 18). *Masseovervåkning uten sidestykke*. Retrieved March 5, 2023, from NRK: https://www.nrk.no/ytring/masseovervakning-uten-sidestykke-1.16133987

Haugsvær, S. (2020, April 22). *Etterretningslov: Støtter forslaget. Tar dissens om omfattende overvåking*. Retrieved March 4, 2023, from Venstre: https://www.venstre.no/artikkel/2020/04/22/etterretningslov-stotter-forslaget-tar-dissens-om-omfattende-overvaking/

Hoff, F. R. (2020, September 17). *Et oppgjør med den nye E-tjenesteloven*. Retrieved March 4, 2023, from Stratagem: https://www.stratagem.no/et-oppgjor-med-den-nye-e-tjenesteloven/

Home Office. (2015, October 30). *Investigatory Powers Bill: Factsheet - Bulk Interception.* Retrieved January 23, 2023, from Investigatory Powers Bill: fact sheets: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473751/Factsheet-Bulk_Interception.pdf

Home Office. (2015, October 30). *Investigatory Powers Bill: Factsheet – Targeted Interception.* Retrieved January 23, 2023, from Investigatory Powers Bill: fact sheets: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473739/Factsheet-Targeted_Interception.pdf

Innst. 357 L (2019–2020). (2020). *Innstilling fra utenriks- og forsvarskomiteen om Lov om Etterretningstjenesten (etterretningstjenesteloven)*. Retrieved October 12, 2022, from https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Innstillinger/Stortinget/2019-2020/inns-201920-357l/

Jawaid, T. (2020, July). Privacy vs National Security. *International Journal of Computer Trends and Technology*, pp. 1-7. Retrieved October 26, 2022, from https://arxiv.org/ftp/arxiv/papers/2007/2007.12633.pdf

Johnsen, A. B. (2017, January 21). *E-sjefen: Frykter dataangrep mot stortingsvalget*. Retrieved March 1, 2023, from VG: https://www.vg.no/nyheter/innenriks/i/82WgG/e-sjefen-frykter-dataangrep-mot-stortingsvalget

Juliussen, B. A. (2021, August 31). *Tilrettelagt innhenting og etterlevelse av EØS-rettslige forpliktelser*. Retrieved April 15, 2023, from Rett24: https://rett24.no/articles/tilrettelagt-innhenting-og-etterlevelse-av-eos-rettslige-forpliktelser

Justis- og beredskapsdepartement. (2019, March 5). *Høringssvar fra Justis- og beredskapsdepartementet.* Retrieved March 25, 2023, from Regjeringen.no: https://www.regjeringen.no/contentassets/287d2d52ddb847849cddb49796456129/horingssvar-med-merknader---jd.pdf?uid=Justis-_og_beredskapsdepartementet

Jørgenrud, M. B. (2017, February 3). *Lysne-utvalget har feilet i oppgaven sin – det finnes allerede et digitalt grenseforsvar i Norge*. Retrieved March 1, 2023, from Digi.no: https://www.digi.no/artikler/kommentar-lysne-utvalget-har-feilet-i-oppgaven-sin-det-finnes-allerede-et-digitalt-grenseforsvar-i-norge/376074

Lubin, A. (2018, January 1). "We Only Spy on Foreigners": The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance. *Chicago Journal of International Law*, pp. 502-552. Retrieved March 5, 2022, from https://www.proquest.com/docview/2012378804?parentSessionId=3UTur7CGESUcJwhHe8EgCTZEyTZM4N8hZkQl0t5KcMI%3D&pq-origsite=primo&accountid=17260

Lunde, M. H. (2019, February 14). *Å rope «ulv-ulv»*. Retrieved March 1, 2023, from NRK: https://www.nrk.no/ytring/datatilsynet-bommer-1.14429046

Lysne, O., Grytting, T., Jarbekk, E., Lunde, E., & Reusch, C. (2016). *Digitalt Grenseforsvar.* Oslo: Forsvarsdepartamentet. Retrieved October 12, 2022, from https://www.regjeringen.no/globalassets/departementene/fd/dokumenter/lysne-ii-utvalgets-rapport-2016.pdf

Nasjonal kommunikasjonsmyndighet. (2019, February 12). *Høringssvar fra Nasjonal kommunikasjonsmyndighet (Nkom).* Retrieved April 7, 2023, from Regjeringen.no: https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=db44a957-54a6-47c4-9afc-d53f684826cd

Nasjonal sikkerhetsmyndighet. (2019, February 12). *Høringssvar fra Nasjonal sikkerhetsmyndighet.* Retrieved March 26, 2023, from Regjeringen.no: https://www.regjeringen.no/contentassets/287d2d52ddb847849cddb49796456129/horingssvar-med-merknader---nsm.pdf?uid=Nasjonal_sikkerhetsmyndighet_(NSM)

Nasjonal sikkerhetsmyndighet. (2022). *Risiko 2022.* Oslo: Nasjonal sikkerhetsmyndighet. Retrieved October 12, 2022, from https://nsm.no/getfile.php/137798-1644424185/NSM/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekeltsider.pdf

Nasjonal sikkerhetsmyndighet. (2022, June 28). *Varslingssystem for digital infrastruktur (VDI)*. Retrieved April 15, 2023, from NSM: https://nsm.no/tjenester/varslingssystem-vdi/

Norges institusjon for menneskerettigheter. (2019, February 12). *Høringsuttalelse om forslag til ny lov om Etterretningstjenesten*. Retrieved March 24, 2023, from Regjeringen.no: https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=1b03fe18-1d1e-4be5-a7ce-5f1dc785695a

Norsk utenrikspolitisk institutt. (2019, January 30). *Høringssvar fra NUPI - Norsk utenrikspolitisk institutt*. Retrieved March 24, 2023, from Regjeringen.no: https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=d4630119-b015-4ef7-8110-60be2a90c0be

NTB. (2019, February 12). *E-sjefen: – Det blir fest i Russland og Kina hvis Norge dropper datalagring*. Retrieved February 26, 2023, from Digi.no: https://www.digi.no/artikler/e-sjefen-det-blir-fest-i-russland-og-kina-hvis-norge-dropper-datalagring/457799

Omand, D. (2020, April 30). *Uten sikkerhet er ikke friheten og rettssikkerheten fullstendig*. Retrieved February 26, 2023, from DN: https://www.dn.no/innlegg/etterretningstjenesten/digitalt-grenseforsvar-dgf/personvern/innlegg-uten-sikkerhet-er-ikke-friheten-og-rettssikkerheten-fullstendig/2-1-798509

Politiets sikkerhetstjeneste. (2019, February 12). *Høringssvar fra PST - Forslag til ny lov om Etterretningstjenesten.* Retrieved March 24, 2023, from Regjeringen.no: https://www.regjeringen.no/contentassets/287d2d52ddb847849cddb49796456129/horingssvar-med-merknader---pst.pdf?uid=PST

Politiets sikkerhetstjeneste. (2022). *National Threat Assessment for 2022.* Oslo: Politiets sikkerhetstjeneste. Retrieved October 12, 2022, from https://pst.no/globalassets/ntv/2022/nasjonal-trusselvurdering-2022-pa-engelsk.pdf

Posner, E. A., & Vermeule, A. (2007). Chapter One: Emergencies, Tradeoffs, and Deference. In E. A. Posner, & A. Vermeule, *Terror in the Balance: Security, Liberty, and the Courts* (pp. 27-95). New York: Oxford University Press. Retrieved from https://ebookcentral-proquest-com.mime.uit.no/lib/tromsoub-ebooks/reader.action?docID=415817&ppg=4

Pulver, A., & Medina, R. M. (2018, June 22). A review of security and privacy concerns in digital intelligence. *Intelligence and National Security*, pp. 241-256. Retrieved October 24, 2022, from https://www-tandfonline-com.mime.uit.no/doi/pdf/10.1080/02684527.2017.1342929?needAccess=true

Rønn, K. V., & Søe, S. O. (2019, February 12). Is social media intelligence private? Privacy in public and the nature of social media intelligence. *Intelligence and National Security*, pp. 362–378. Retrieved March 05, 2022, from https://www-tandfonline-com.mime.uit.no/doi/full/10.1080/02684527.2019.1553701

Seglsten, P. H. (2022, August 16). *IKT-Norge og E-tjenesten: Cybertruslene gjør at vi må tenke nytt om personvern*. Retrieved February 26, 2023, from Digi.no: https://www.digi.no/artikler/ikt-norge-og-e-tjenesten-cybertruslene-gjor-at-vi-ma-tenke-nytt-om-personvern/521444

Sikkerhetsloven. (2019, January 1). Lov om nasjonal sikkerhet (LOV-2018-06-01-24). Lovdata. Retrieved October 12, 2022, from https://lovdata.no/dokument/NLE/lov/2018-06-01-24

Simen, B. (2020, May 10). *Nytten av masseovervåkning er ikke godt nok dokumentert*. Retrieved March 4, 2023, from DN: https://www.dn.no/innlegg/etterretningstjenesten/digitalt-

grenseforsvar-dgf/terror/innlegg-nytten-av-masseovervakning-er-ikke-godt-nok-dokumentert/2-1-805033

Skaug, H. S. (2022, January 4). *Elsevier.* Retrieved January 5, 2022, from The ethics of trading privacy for security: The multifaceted effects of privacy on liberty and security: https://www.sciencedirect.com/science/article/pii/S0160791X21003298

Skogen, T. (2020, May 13). *Ja, vi har nytte av å lagre metadata*. Retrieved March 1, 2023, from DN: https://www.dn.no/innlegg/innlegg-ja-vi-har-nytte-av-a-lagre-metadata/2-1-807749

Skogen, T. (2021, September 2). *Tilrettelagt innhenting styrker vår sikkerhet*. Retrieved February 26, 2023, from Rett24: https://rett24.no/articles/tilrettelagt-innhenting-styrker-var-sikkerhet

Tekna - Teknisk-naturvitenskapelig forening. (2019, February 12). *Høringssvar fra Tekna - Teknisk-naturvitenskapelig forening*. Retrieved March 24, 2023, from Regjeringen.no: https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=c576f91f-c92d-4001-bc64-4c164fcd0717

Teknologirådet. (2007, June 18). *Slik blir du overvåket*. Retrieved May 10, 2023, from Teknologirådet: https://teknologiradet.no/slik-blir-du-overvaket/

Thon, B. E. (2019, February 16). *Etterretningssjef med utestemme*. Retrieved March 4, 2023, from NRK: https://www.nrk.no/ytring/etterretningssjef-med-utestemme-1.14433046

Tonkiss, F. (2017). Discourse Analysis. In C. Seale, *Researching Society and Culture* (pp. 477-492). N/A: SAGE Publications.

Veen, J., & Boeke, S. (2020, January 1). Which is more important: online privacy or national security?: The Dutch position in the ongoing encryption debate. *Atlantisch Perspectief*, pp. 36-40. Retrieved March 7, 2022, from https://www-jstor-org.mime.uit.no/stable/48600570?pq-origsite=summon&seq=1#metadata_info_tab_contents

Watt, E. (2017, May 23). The right to privacy and the future of mass surveillance. *The International Journal of Human Rights*, pp. 773-799. Retrieved March 04, 2022, from https://www-tandfonline-com.mime.uit.no/doi/pdf/10.1080/13642987.2017.1298091?needAccess=true