EOS COMMITTEE

NORWEGIAN PARLIAMENTARY OVERSIGHT COMMITTEE ON INTELLIGENCE AND SECURITY SERVICES

Special Report to the Storting concerning the legal basis for the Norwegian Intelligence Service's surveillance activities

Photo: Lars Aamodt / NTB Scanpix

To the Storting

In accordance with Act No 7 of 3 February 1995 relating to the Oversight of Intelligence, Surveillance and Security Services (the Oversight Act) Section 8 subsection 2 second sentence, the Committee hereby submits a special report to the Storting concerning the legal basis for surveillance activities carried out by the Norwegian Intelligence Service.

The report is unclassified, cf. the Oversight Act Section 8 subsection 2 third sentence. Pursuant to the Act relating to Protective Security Service (the Security Act), the issuer decides whether or not information is classified. Before the report is submitted to the Storting, the Committee sends the final draft to the relevant service to clarify whether the report complies with this requirement. The service has also been given the opportunity to check that there are no factual errors or misunderstandings.

Oslo, 17 June 2016

Eldbjørg Løwer

Svein Grønnern | Trygve Harvold | Theo Koritzinsky

Øyvind Vaksdal | Håkon Haugli | Inger Marie Sunde

Henrik Magnusson

The Norwegian Parliamentary Oversight Committee on Intelligence and Security Services. Left to right: Håkon Haugli, Eldbjørg Løwer (chair), Theo Koritzinsky, Svein Grønnern (deputy chair), Trygve Harvold, Inger Marie Sunde and Øyvind Vaksdal.

Contents

Preface

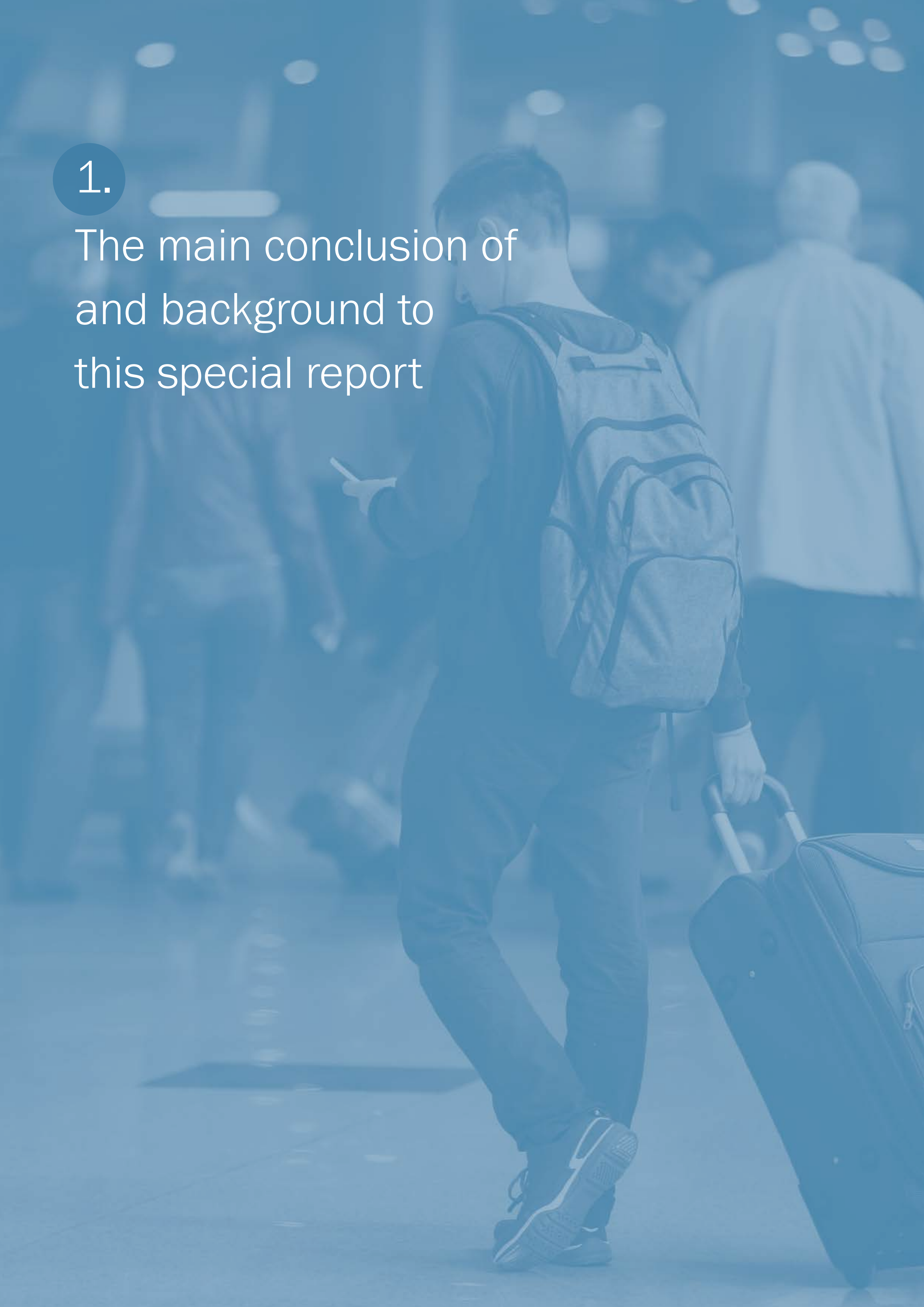
The primary purpose of the EOS Committee's oversight is to ensure that the intelligence, surveillance and security services (the EOS services) do not subject individuals to unjust treatment. In its work on this special report to the Storting, the Committee has taken this purpose as its point of departure, but has also taken into consideration the importance of the duties the Norwegian Intelligence Service is tasked with performing in order to protect national security and independence and the security of the inhabitants of Norway.

Several dilemmas arise where these interests intersect. It is a challenge for a state based on the rule of law to balance individuals' right to privacy against the need to protect society and individuals against different forms of attack.

It is one of the Committee's duties to bring to the attention of the Storting any potential need for legislative amendment. The Committee is of the opinion that actual, technological and legal developments indicate that the time has come to notify the Storting of a potential need to amend the Norwegian Intelligence Service's regulatory framework.

The purpose of this special report to the Storting is to safeguard fundamental democratic considerations in a field where citizens' trust in the authorities is of crucial importance. The Committee would like to make clear that it has not found reason to criticise the service.

1. The main conclusion of and background to this special report



1.1 The EOS Committee's main conclusion

The EOS Committee has for a long time had internal discussions about the significance of actual, technological and legal developments for the adequacy of Act No 11 of 20 March 1998 relating to the Norwegian Intelligence Service (the Intelligence Service Act) as a legal basis for the service's surveillance activities.

The most important reason for reviewing the legal basis is that Norwegian legal persons are increasingly being targeted by the intelligence service as a result of participation in international terrorism. The Committee will use as a basis the Norwegian Intelligence Service's (NIS) expert assessments of the necessity of technical information collection.

After considering general questions relating to legal authority and carrying out concrete assessments of specific methods, the Committee has arrived at the following main conclusion:

> **The Committee hereby notifies the Storting of a potential need to change the regulatory framework relating to NIS, cf. Directive No 4295 of 30 May 1995 relating to the Oversight of Intelligence, Surveillance and Security Services Section 13 subsection 3 letter h.**

The Committee would like to make clear that it has not found reason to criticise the service. The purpose of this report is to notify the Storting of a potential need for legislative amendment. The Committee is concerned that the legal provisions authorising interventions by the EOS services must be sufficiently clear for it to be possible to determine whether or not the services conduct their activities in accordance with the intentions of the legislators.

The Committee shares NIS's view that the regulatory framework governing the service's activities must facilitate the service's ability to efficiently perform its tasks and to address security considerations. In the Committee's opinion, the democratic considerations pointed out in this report nevertheless indicate the need for the Storting to consider again how the different considerations can best be balanced in the Intelligence Service Act.

1.2 The significance of actual, technological and legal developments

One of the Committee's most important tasks is to oversee compliance with the prohibition in Section 4 first paragraph of the Intelligence Service Act. This provision states that NIS shall not on Norwegian territory 'monitor or in any other covert manner collect information concerning Norwegian physical or legal persons'. The grounds given for the prohibition in the preparatory works to the Intelligence Service Act Section 4 can serve as an illustration of what developments have taken place.

The prohibition was partly based on legal uncertainty regarding the scope of the principle of legal authority in relation to 'simple collection of information'.[1] The right to respect for private and family life pursuant to the European Convention on Human Rights (ECHR) Article 8 and the fact that the right to privacy[2] was enshrined in law in the Constitution in 2014 indicate that an intelligence service's collection of information about individuals is covered by the principle of legal authority, meaning that interference with this right must be warranted by law.[3]

The prohibition was also included to 'focus on the fact that the Intelligence Service's activities address circumstances outside Norwegian territory'.[4] A clear distinction between matters of relevance to foreign and domestic intelligence is also assumed in the preparatory works to Act No 7 of 3 February 1995 relating to the Oversight of Intelligence, Surveillance and Security Services (the Oversight Act), which states the following about the Committee's oversight of NIS:

> *'As regards the Intelligence Service, the Commission finds that, seen in isolation, there is no need for oversight based on the considerations by which the Storting was motivated,* assuming that the activities are kept within their stipulated framework. Moreover, complaints against the service are so rare that they do not warrant the establishment of a permanent oversight arrangement. Formal oversight, which must also be able to cover the communication of information to foreign parties and national collaboration, will therefore suffice.'[5]

Since the Intelligence Service Act and the Oversight Act were adopted, both the threat situation and communication technology have undergone significant development. Individuals and organisations not associated with any state

1 Proposition No 50 to the Odelsting (1996–1997) chapter 9 *Særlig om forholdet til norske borgere* ('About Norwegian citizens in particular' – in Norwegian only).

2 The Norwegian Constitution Article 102.

3 It can be mentioned here that the view of what is protected under Article 8 of the ECHR has developed. The following is an extract from an article entitled *Grunnlovsfesting av retten til privatliv?* ('Enshrining the right to privacy in law in the Constitution?') by Alf Petter Høgberg and Njål Høstmælingen, published in the Norwegian journal for law students, *Jussens Venner,* 2010 pages 98–146: 'Police registers containing neutral information (such as names, addresses, phone numbers etc.) were not originally deemed to constitute interference in the sense of Article 8 (1). Attitudes have changed as a result of, among other things, the growing tendency in society towards keeping more registers and devising ways of coordinating information.'

4 Proposition No 50 to the Odelsting (1996–1997) chapter 9 *Særlig om forholdet til norske borgere* ('About Norwegian citizens in particular' – in Norwegian only).

5 Official Norwegian Report NOU 1994:4 *Kontrollen med "de hemmelige tjenestene"* ('Oversight of the 'secret services' – in Norwegian only), chapter 1.5 *Kontrollbegrepet og kontrollbehovet* ('The concept of and need for oversight').

can represent a threat. Threat actors change their location and have connections in multiple countries, and technological development has made it possible to carry out preparations for terrorist acts across national borders. Norwegian legal persons have become increasingly relevant to Norway's intelligence operations abroad as a result of participation in international terrorism.

The fact that NIS and the Norwegian Police Security Service (PST) increasingly cross paths has become apparent in different ways, for example through the requirement for them to collaborate introduced in Instructions No 1151 of 13 October 2006 for the Collaboration between the National Intelligence Service and the Norwegian Police Security Service, and through the establishment of the Joint Counter Terrorism Centre (FKTS) in 2014. In its recommendation to the EOS Committee's annual report for 2012, the Standing Committee on Scrutiny and Constitutional Affairs emphasised the importance of close collaboration between PST and NIS, but also pointed out that 'increased interaction and collaboration will also present new oversight challenges that must be tackled as the collaborative relationships develop'.[6]

Professor of Law Erling Johannes Husabø has concluded that it is 'doubtful whether the Intelligence Service's present legal basis meets the requirements that currently apply under the ECHR'.[7] He points to several of the circumstances that the Committee has described above as the basis for his conclusion:

> 'Overall, NIS's surveillance of foreign and (abroad) Norwegian citizens clearly has a weaker legal basis than that applicable to PST. The facts that NIS has in recent years shifted its attention towards groups and individuals as a result of the terrorist threat at home and abroad and that the service cooperates closely with PST in such cases makes matters more problematic than before. The same is true of the rapid technological developments that continually provide new possibilities for cross-border surveillance. Generally speaking, the ECHR is becoming increasingly sceptical of the states' arguments that considerations of national security require rules in this area to be more vaguely worded. Incorporating some of the rules currently found in the Instructions and the supplementary provisions into the Act itself would make them more accessible and improve their democratic legitimacy. In addition, a somewhat more detailed description of which methods the service is permitted to use ought to be provided, particularly to what extent the service may use methods that resemble or exceed those available to PST. The fact that some other European countries do this in corresponding regulations indicates that this can be done without undermining the considerations that the service is meant to safeguard.'

The Committee has noted that several reports and other work of importance to the intelligence, surveillance and security field are currently under way.[8]

In addition to the developments pointed out, two concrete matters were particularly important in triggering the work that led to the submission of this special report. These will be reviewed in sections 1.3 and 1.4.

1.3 Proposal for and consideration of statutory regulation of digital border control

NIS does not currently have access to electronic communication transmitted via communication networks/cables under Norwegian jurisdiction. The report *Unified effort* presented by the *Expert Commission on Norwegian Security and Defence Policy* stated that accessing information from cable traffic 'will not be principally different from other forms of foreign intelligence, but it will be a question of large amounts of data'.[9]

The Committee of Digital Vulnerabilities in Society stated in Official Norwegian Report NOU 2015:13 *Digital sårbarhet – sikkert samfunn ('Digital vulnerability – secure society' – in Norwegian only)*:

> 'The committee notes the information provided that some countries with which we like to compare ourselves have digital border surveillance in place, and understands the need from an intelligence perspective to consider introducing it in Norway as well. However, the committee is of the opinion that digital border surveillance should not be introduced without prior public debate. This debate should be prepared through an Official Norwegian Report (NOU) or equivalent document. This will ensure that the measure will be subject to a broader debate than the committee has been able to subject it to.'[10]

On 24 February 2016 the Ministry of Defence appointed a committee tasked with looking into issues relating to the right to obtain information from telecommunications and data traffic into and out of Norway. The ministry-appointed committee is scheduled to submit its report by the end of June 2016.

According to the ECHR, interference with the right to privacy must be proportional – and in the EOS Committee's opinion, this can best be ensured by having all available methods considered by the legislators simultaneously. This will ensure that any conditions stipulated by the Storting to safeguard individuals' due process protection and protection of privacy will be generally applicable to all the service's information collection methods that involve intervention in relation to individuals, and not just to one specific method.[11] This view is supported by the fact that the choice of method should not be decisive to the due process protection of individuals.

1.4 Searches conducted by NIS in stored metadata relating to Norwegian legal persons in Norway to find selectors for purposes relevant to foreign intelligence

In 2014, the Committee was made aware that NIS carries out searches in stored metadata[12] relating to Norwegian legal persons in Norway to find selectors[13] relevant to the performance of the service's tasks. This means searches for communication between, for example, Norwegian phone numbers in Norway and unknown phone numbers abroad of intelligence targets. These searches are considered more closely in chapter 5 below. This issue lies at the point of intersection between considerations of personal data protection on the one hand and of national security and the security of the inhabitants of Norway on the other. In the Committee's opinion, this is such an important matter of principle that it must be submitted to the Storting.

1.5 NIS's overriding considerations

NIS has stated to the EOS Committee that there are 'shortcomings in the argument' on which the Committee's assessments and Professor Husabø's conclusion[14] are based. NIS writes that it 'emphasises legal predictability for all parts of its activities and agrees with the EOS Committee's statement that the collection of information about individuals falls under the scope of the principle of legal authority'. NIS states that 'human rights govern all our activities abroad'.

NIS has also stated that it 'is self-evident that police methods used by a domestic security service are regulated to a considerably greater extent that the methods used by a foreign intelligence service'. NIS also writes that 'comparing strategic foreign intelligence activities with domestic police activities for the purpose of preventing and fighting crime demonstrates a lack of knowledge of the fundamental differences between the two'. The foreign intelligence service is tasked with 'casting a wide net (target searches) to find information needed by superior authorities'. NIS writes that its 'focus is on information, not individuals, and there is in principle no stigma attached to being of interest to NIS'.

With particular reference to 'public allegations of inadequate legal basis in itself representing a challenge', NIS nevertheless takes a positive view of a review of its legal basis. NIS also notes that 'the Lysne II Committee can hardly consider granting the service new access if the framework conditions for the service are otherwise perceived to conflict with the applicable human rights requirements'.

Finally, the service writes that 'another argument for revising the law is that actual, technological and legal developments require continuous assessment of NIS's legal basis'.

NIS's statement is included in full as Appendix 1 to this report.

1.6 The EOS Committee's work on questions relating to the legal basis for NIS's surveillance activities

The Committee has received verbal briefings from NIS during its inspections of the service, conducted its own searches in NIS's systems and reviewed documents. On this basis, the Committee prepared a classified report that has been sent to NIS for review and comments in two rounds. The Committee felt that in this matter there were particularly strong grounds for giving NIS the opportunity to respond to both the Committee's understanding and its arguments in order to elucidate the case as well as possible. This special report is based on the above-mentioned report and NIS's written feedback following review of the report. During the Committee's inspection of NIS in March 2016, a meeting was held between the Committee and the service to clarify procedural questions relating to this special report.

---

6 Recommendation No 376 to the Storting (2012–2013), chapter 7.2.

7 Professor Erling Johannes Husabø, *Hvilke krav stiller Grunnloven og EMK til etterfølgende kontroll av sikkerhets- og etterretningstjenestenes inngrep i menneskerettigheter?* ('What requirements do the Constitution and the ECHR stipulate for subsequent oversight of the security and intelligence services' interference with on human rights?'), prepared on assignment from the Evaluation Committee for the EOS Committee and included as Appendix 4 in the Report to the Storting from the Evaluation Committee for the Norwegian Parliamentary Intelligence Oversight Committee, Document 16 (2015–2016).

8 Consultation document of 27 April 2016 from the Ministry of Justice and Public Security on amendment of the Criminal Procedure Act and the Police Act – disclosure of information obtained by means of covert coercive measures from PST to the Intelligence Service; On 24 February 2016 the Ministry of Defence appointed a committee tasked with looking into issues relating to the right to obtain information from telecommunications and data traffic into and out of Norway; Private Member's Motion No 94 (2015–2016) from Members of the Storting Trine Skei Grande and Iselin Nybø to establish a privacy protection committee for the justice sector and the Evaluation Committee for the EOS Committee; Report to the Storting from the Evaluation Committee for the Norwegian Parliamentary Intelligence Oversight Committee, Document 16 (2016).

9 The Expert Commission on Norwegian Security and Defence Policy, United Effort, page 78.

10 Official Norwegian Report NOU 2015:13 *Digital sårbarhet – sikkert samfunn* ('Digital vulnerability – secure society' – in Norwegian only), section 21.11.8.

11 NIS has informed the EOS Committee that the service 'disagrees with the presentation of access to information transmitted via fibre optic cable as a new method', cf. letter to the EOS Committee of 4 May 2016.

12 By metadata is meant information about data, such as times, duration, to/from indicators, type of traffic and other parameters that describe a technical event that has taken place in a communication network.

13 A selector can be a phone number, an email address, a Facebook username etc.

14 Professor Husabø is quoted in section 1.2 of this report.

2.

A review of the Norwegian Intelligence Service's legal basis

2.1 Introduction

The present regulation of NIS is characterised by several distinct features that are rooted in history, constitutional law and international law. Below is an account of the legal basis of NIS provided in order to shed light on key premises for the Committee's special report.

2.2 The functions of NIS and the EOS Committee's oversight

The EOS Committee continuously oversees NIS, which is Norway's civilian and military foreign intelligence service. NIS's activities are regulated by the Intelligence Service Act[15] and the Intelligence Service Instructions[16]. Pursuant to the Intelligence Service Instructions Section 17, unclassified supplementary provisions were adopted concerning NIS's collection of information concerning Norwegian persons abroad and the disclosure of personal data to cooperating foreign services.[17]

The Intelligence Service Act regulates the overriding principles for the activities of NIS, including the service's organisation and tasks, and its relations with Norwegian persons. The purpose of the Act is to establish conditions so that the Norwegian Intelligence Service can contribute effectively to monitoring and counteracting external threats to the independence and security of the realm and other important national interests, and to safeguard confidence in and secure the basis for oversight of the activities of the Intelligence Service.[18]

Section 3 of the Intelligence Service Act sets out NIS's tasks. This provision states that the service shall 'collect, process and analyse information regarding Norwegian interests viewed in relation to foreign states, organisations or private individuals, and in this context prepare threat analyses and intelligence assessments to the extent that this may help to safeguard important national interests'. The provision lists important examples of such interests, but the list is not exhaustive.[19] Among other things, the service is to contribute to the design of Norwegian foreign, defence and security policy, obtain information concerning international terrorism, and obtain information concerning proliferation of weapons of mass destruction etc.[20]

A key limitation on the service's activities is set out in the Intelligence Service Act Section 4 and in the Intelligence Service Instructions Section 5, which prohibit it from monitoring or in any other covert manner collect information concerning Norwegian physical or legal persons on Norwegian territory. In its oversight of NIS, the Committee is particularly concerned with ensuring that this statutory prohibition is complied with.

The Committee shall regularly oversee the practice of intelligence, surveillance and security services in civilian and military administration, cf. the Oversight Act Section 3 first paragraph. According to the Oversight Act Section 2 first paragraph, the purpose of the oversight is:

> '1. to ascertain and prevent any exercise of injustice against any person, and to ensure that the means of intervention employed do not exceed those required under the circumstances, and that the services respect human rights,
> 2. to ensure that the activities do not involve undue damage to civic life,
> 3. to ensure that the activities are kept within the framework of statute law, administrative or military directives and non-statutory law.'

The Committee's oversight tasks in relation to NIS are specified in the Directive relating to Oversight of the Intelligence, Surveillance and Security Services Section 11 (1) letters a) and e), where it is stated that the Committee shall 'ensure that activities are carried out within the framework of the service's established responsibilities, and that no injustice is done to any person' and 'ensure that the cooperation and exchange of information between the services is kept within the framework of service needs and applicable regulations'.[21] Pursuant to the Oversight Act Section 2 second paragraph, the Committee shall 'show consideration for national security and relations with foreign powers'.

2.3 The legal basis for NIS's surveillance activities

The Intelligence Service Act does not contain any provisions that specifically authorise NIS's use of methods, but Section 3 of the Act describes the service's tasks. It states that the service 'shall collect, process and analyse information regarding Norwegian interests viewed in relation to foreign states, organisations or private individuals' to the extent that this may 'help to safeguard important national interests', cf. the Intelligence

15 Act No 11 of 20 March 1998 relating to the Norwegian Intelligence Service. The preparatory works to the Intelligence Service Act are Proposition No 50 to the Odelsting (1996–1997) and Recommendation No 19 to the Odelsting (1997–1998).

16 Royal Decree No 1012 of 31 August 2001 relating to Instructions for the Norwegian Intelligence Service.

17 Supplementary provisions concerning the Norwegian Intelligence Service's collection of information concerning Norwegian persons abroad and the disclosure of personal data to cooperating foreign services, adopted by the Ministry of Defence on 24 June 2013 pursuant to the Intelligence Service Instructions Section 13.

18 See Proposition No 11 to the Odelsting (1997–1998), page 1. The purpose and scope of the Intelligence Service Instructions are identical to those of the Intelligence Service Act, cf. the Intelligence Service Instructions Section 1. The Instructions supplement the provisions of the Act and set out more detailed rules regarding the service's organisation, tasks and activities.

19 See also the Intelligence Service Instructions Section 7 second paragraph first sentence: 'The tasking in the Act's Section 3 is not exhaustive.'

20 It is specified in Section 8 of the Intelligence Service Instructions that the main task of NIS is 'to collect, assess and analyse information on foreign countries' political and social development, intentions and military forces, which may constitute a real or potential risk'.

21 As a rule, the oversight activities do not include activities which concern persons or organisations not domiciled in Norway, or foreigners whose stay in Norway is in the service of a foreign state, cf. the Directive relating to Oversight of the Intelligence, Surveillance and Security services Section 4 first paragraph.

Service Act Section 3. The implementation of intelligence operations, including their use of methods, must fall within the service's defined tasks under Section 3.[22]

The Act and the Instructions do not specify which intrusive methods may be used, nor do they limit which medium (radio, satellite, cable etc.) may be used to transmit information obtained by the service.

> It is stated on page 8 of Proposition No 50 to the Odelsting (1996–1997) that the two main methods that the service uses to collect information are (i) technical information collection from radio, radar and acoustic sources, and (ii) human intelligence collection. It is also stated that information collection takes place through cooperation and exchange of information with the intelligence services of other countries, cf. pages 9 and 15. The preparatory works make no further comment on the service's information collection capacity other than to say that it must have the 'necessary collection capacity to cover prioritised needs'.[23]

As regards the Intelligence Service Act as a legal basis for the service's activities, the Ministry of Defence has previously expressed the following opinion to the Committee:[24]

> 'The service's activities are aimed at activities abroad and governed by Norway's security policy interests. Based on the service's history and legal basis, as well as consistent and long-standing state practice, it must be assumed that the Storting intended the Act, whose preparatory works refer to special information collection methods, to authorise covert and intrusive information collection methods despite the fact that the actual wording of the Act does not specify methods and does not list all the different ways of collecting information.'

However, this does not mean that the service is free to use any technology and methods. It follows from the Intelligence Service Act Section 6 second paragraph that NIS's activities should be kept within the framework of current legislation, administrative or military directives and non-statutory law. Two fundamental limitations can be said to apply to the service's information collection activities. Firstly, the service shall not 'on Norwegian territory monitor or in any other covert manner collect information concerning Norwegian physical or legal persons', cf. the Intelligence Service Act Section 4 first paragraph. Secondly, all intelligence activities shall take place within the framework of Norway's commitments under international law, including the ECHR.

2.4 The importance of 'political approval' of the lawfulness of methods

The Intelligence Service Instructions Section 13 letter d) requires 'matters of particular importance, or that raise questions of principle' to be submitted to the Ministry of Defence for consideration. This provision means that new methods etc. are subject to what is known as political approval. This is not dealt with in Proposition No 50 to the Odelsting (1996–1997), but political control over the service is described in chapter 11:

> 'The Minister of Defence, on behalf of the Government, has constitutional and parliamentary responsibility for the Norwegian Intelligence Service's activities, as for the Armed Forces in general. The political control is exercised through the Chief of Defence, who is the head of the intelligence service's immediate superior. The Chief of Defence, subordinate to the Minister of Defence, is responsible for the intelligence service. Therefore, the Chief of Defence is obliged, under the instructions for the Chief of Defence, to provide, via the Minister of Defence, the Government with such information as is of importance to its work.'

In 2004, the Committee raised questions regarding the legal basis in an area of NIS's technical information collection activities.[25] The matter was first raised with NIS and subsequently, in a more general form, with the Ministry of Defence. The question discussed with the Ministry concerned the scope of the Intelligence Service Act as an independent legal basis for the use of intrusive methods and the bearing it has on a method's lawfulness that it has been considered and approved by the responsible political authorities. The Committee's assessments particularly targeted technical information collection methods and the relationship between the Intelligence Service Act and the General Civil Penal Code, as the description of offences in some provisions of the General Civil Penal Code could overlap with certain technical information collection methods.

Initially, the Ministry of Defence expressed the opinion that the Act, seen in conjunction with its preparatory works, the history of the service and long-standing state practice, must be deemed to constitute a general legal basis for using intrusive methods as long as their use lies within the scope of the purpose of the Act. The Committee, on the other hand, was of the opinion that the political process of approval should be given greater weight in the assessment of the legal situation. After further consideration, including meetings with the Ministry, the Ministry specified its view in a letter to the Committee to the effect that an overall assessment of the lawfulness of specific applications of a method must place considerable emphasis on whether the method has undergone political approval. The Ministry also wrote that new information collection methods will in any case always be considered matters of particular importance that should be submitted to the Ministry of Defence for consideration pursuant to the Intelligence Service Instructions Section 13. The Ministry's view means that political approval is required for new methods, and that failure to obtain such approval can, depending on the circumstances, have a bearing on the question of whether use of the method can be considered lawful. The Committee saw no reason to pursue the legal questions any further. Matters that have been submitted to the Ministry pursuant to Section 13 of the Intelligence Service Instructions are routinely presented to the Committee during its inspections of NIS. The Committee is also given access to the Ministry's written feedback to the service, but not to the Ministry's internal documents concerning the approval.[26]

2.5 Relations with Norwegian physical and legal persons

Relations with Norwegian physical and legal persons is regulated by Section 4 of the Intelligence Service Act:

> 'The Norwegian Intelligence Service shall not on Norwegian territory monitor or in any other covert manner collect information concerning Norwegian physical or legal persons.
>
> The Norwegian Intelligence Service may only hold information concerning Norwegian physical or legal persons when such information is directly associated with the duties of the Norwegian Intelligence Service pursuant to section 3 or is directly associated with such persons' work or assignments for the Norwegian Intelligence Service.'

This provision is supplemented by Section 5 of the Intelligence Service Instructions:

> Should the Intelligence Service, while carrying out its tasks, receive surplus information which is relevant in a surveillance or other context, and which the Service cannot retain (cf. Section 4, second paragraph of the Act), such information may be transmitted to the appropriate Norwegian public authorities in accordance with the rules on reporting in Chapter 4 of these Instructions.
>
> The Intelligence Service may carry out measures to verify the credibility of its sources.
>
> Section 4 of the Act does not preclude the Intelligence Service from gathering information on foreign intelligence activities in Norway, including Norwegian individuals and organisations which conduct such activities, to the extent that the Intelligence Service has a need for such information. This information collection shall occur through, or with the approval of, the Police Security Service.
>
> The cooperation with the Police Security Service is regulated in a separate instruction, adopted by the King in Council.'

The Ministry specifies on page 10 of Proposition No 50 to the Odelsting (1996–1997) that the Intelligence Service Act Section 4 should not be interpreted conversely. This means that the service's right to collect information about Norwegian citizens abroad or foreign citizens in Norway is not without limitations. It also states that:

> 'To the extent that it is necessary for the service in order to fulfil the purpose of the Act and perform the tasks it is charged with in this context, however, it is necessary to limit the statutory prohibition in relation to foreign citizens' activities in Norway and Norwegian citizens' activities abroad. NIS should of course not be prohibited from, for example, receiving information about foreign intelligence activities in Norway from persons who contact the service on their own initiative, and forwarding such information to the surveillance service. In this context, the expression foreign intelligence activities is of course also understood to include activities carried out by Norwegian physical or legal persons on Norwegian or foreign territory on assignment from or for the benefit of foreign states, organisations or individuals.'

In other words, there is an absolute prohibition against monitoring or in any other covert manner collecting information concerning Norwegian physical or legal persons, except for Norwegian persons engaged in foreign intelligence activities in Norway. The legal position of Norwegian physical and legal person *outside Norwegian territory* is not regulated by the Intelligence Service Act. According to the preparatory works to the Act, information can be collected in such cases 'to the extent that it is necessary for the service in order to fulfil the purpose of the Act and perform the tasks it is charged with in this context'. However, the service is obliged to respect human rights, including ECHR Article 8 concerning the right to private and family life, also outside Norway.

Pursuant to the Intelligence Service Instructions Section 17, the Ministry of Defence on 24 June 2013 adopted supplementary provisions concerning NIS's collection of information concerning Norwegian persons abroad and the disclosure of personal data to cooperating foreign services. Three conditions must be met in order for NIS to be allowed to monitor or in any other covert manner collect information concerning Norwegian persons abroad. Firstly, the collection of information must take place as part of NIS's performance of its statutory duties. Secondly, the information concerned must be information which NIS can lawfully hold pursuant to the Intelligence Service Act Section 4 second paragraph. Finally, the collection must be deemed necessary following a proportionality assessment where account is taken of the need to safeguard important national interests and the consequences for the person about whom information is collected.

---

22 NIS expressed in its letter to the Committee dated 6 September 2007 (case 20070003) that intelligence operations of any kind can also be initiated on the basis of a concrete emergency situation (defence of self and others or principle of necessity) under the Act relating to Special Measures in Time of War, Threat of War and Similar Circumstances and military command authority during armed conflict.

23 See Proposition No 50 to the Odelsting (1996–1997), section 8.

24 See letter with the Committee's reference number 2004-0050HHH and the Ministry of Defence's reference number 2002/00105-2VFDII5/JEH/352.

25 The matter is discussed in the EOS Committee's annual report for 2005 Document No 20 (2005–2006), chapter 4 under the heading *Rettslige aspekter ved Etterretningstjenestens virksomhet* ('Legal aspects of the activities of the Norwegian Intelligence Service').

26 The EOS Committee does not have right of inspection in relation to the Ministries, cf. the Oversight Act Section 6.

3.

NIS's legal basis in light of the ECHR

Pursuant to the Norwegian Constitution Section 92, the authorities of the State shall respect and ensure human rights. Act No 30 of 21 May 1999 relating to the Strengthening of the Status of Human Rights in Norwegian Law (The Human Rights Act) incorporated the ECHR into Norwegian law with precedence over other legislation, cf. Section 3. The Oversight Act instructs the EOS Committee to 'ensure that the services respect human rights'. This wording was added with effect from 1 June 2009, at the Committee's proposal. One of the Committee's reasons for the addition was that Norway's commitment to respect human rights 'can be at least as important in the Committee's oversight area as in other areas of public administration' and that it would 'send an important signal both to the services and to the general public'.[27]

In connection with the new provision on the right to privacy in Section 120 or the Constitution, the Storting's Standing Committee on Scrutiny and Constitutional Affairs stated that technological development is a good thing, but demands more of us when it comes to safeguarding privacy.[28] The *Storting's Human Rights Commission* stated the following in its report on human rights in the Constitution:

> 'Enshrining protection of privacy and personal data in law in the Constitution can also prove to be an important legal tool when faced with future technological developments, precisely because it can be difficult to predict which concrete problems will arise in future. This gives rise to the need for general and overriding protection, where the principle of protection of privacy and personal data are enshrined in the supreme source of law. It cannot be ruled out that technological developments will make such a constitutional provision important in the coming decades.'[29]

Article 8 of the ECHR states that everyone has the right to respect for his private and family life, his home and his correspondence. No public authorities may interfere with this right, except when such interference is in accordance with the law and is necessary in a democratic society in the interests of e.g. national security. An intelligence service's surveillance and registration of people will constitute an interference with the right to respect for private and family life under Article 8. However, the ECHR does not prevent states from having what is known as secret services, as concluded in the case Klass versus Germany[30]. Such services must exercise their authority within the limits defined by the Convention. Interference with interests protected under the ECHR Section 8 can be justified if three main conditions are met: the interference must be in accordance with the law, it must be in pursuit of a legitimate objective, and it must be necessary in a democratic society.

The rule-of-law requirement means that the rule must be accessible and foreseeable, but it also refers to the quality of law, as it must comply with fundamental principles of rule of law. *The latter aspect is crucial to the Committee, since the Committee's oversight is dependent on the legal basis being of such a quality that actual oversight is possible.*

From an oversight perspective, it can be questioned whether the methods used by NIS that represent interference with the rights of individuals should be enshrined in law, cf. the rule-of-law requirement that the ECHR cites for interference with rights under Article 8. The Evaluation Committee for the EOS Committee wrote the following in its report to the Storting:

> 'In the Evaluation Committee's opinion, a clear and up-to-date legal framework is one of several elements in the overall oversight system that apply to the services' activities, and a clear regulatory framework improves the basis for oversight by the EOS Committee and others. Considerations for the EOS Committee's ability to exercise oversight therefore indicate that the activities of the Intelligence Service should be regulated through more specific and publicly accessible regulations.'[31]

There may be grounds for examining whether a law that does not regulate methods for obtaining information about individuals meets the rule-of-law requirement enshrined in the ECHR.[32]

In a statement to the Committee, NIS has assumed that all the service's information collection meets important human rights requirements, including the conditions for justification of interference pursuant to the ECHT Article 8. NIS also pointed out a need to look into 'the extraterritorial application of human rights in relation to information collection methods that do not involve the service having territorial control or actual and effective control over a person'.[33]

The Committee agrees with NIS that there is a need to examine the relationship with human rights more closely. In the Committee's opinion, this should be done as part of a legislative review process.

Other than the above, the Committee has not considered or reached concrete conclusions about the Intelligence Service Act's relationship with the ECHR and Article 102 of the Constitution, but the questions raised by the Committee form one of the premises for the main conclusion that the legal basis for NIS's surveillance should again be subjected to consideration by the Storting.

27 Letter of 17 April 2009 from the EOS Committee to the Storting.

28 Recommendation No 186 to the Storting (2013-2014), chapter 2.1.9.

29 Doc. No 16 (2011–2012) chapter 30.6.5.

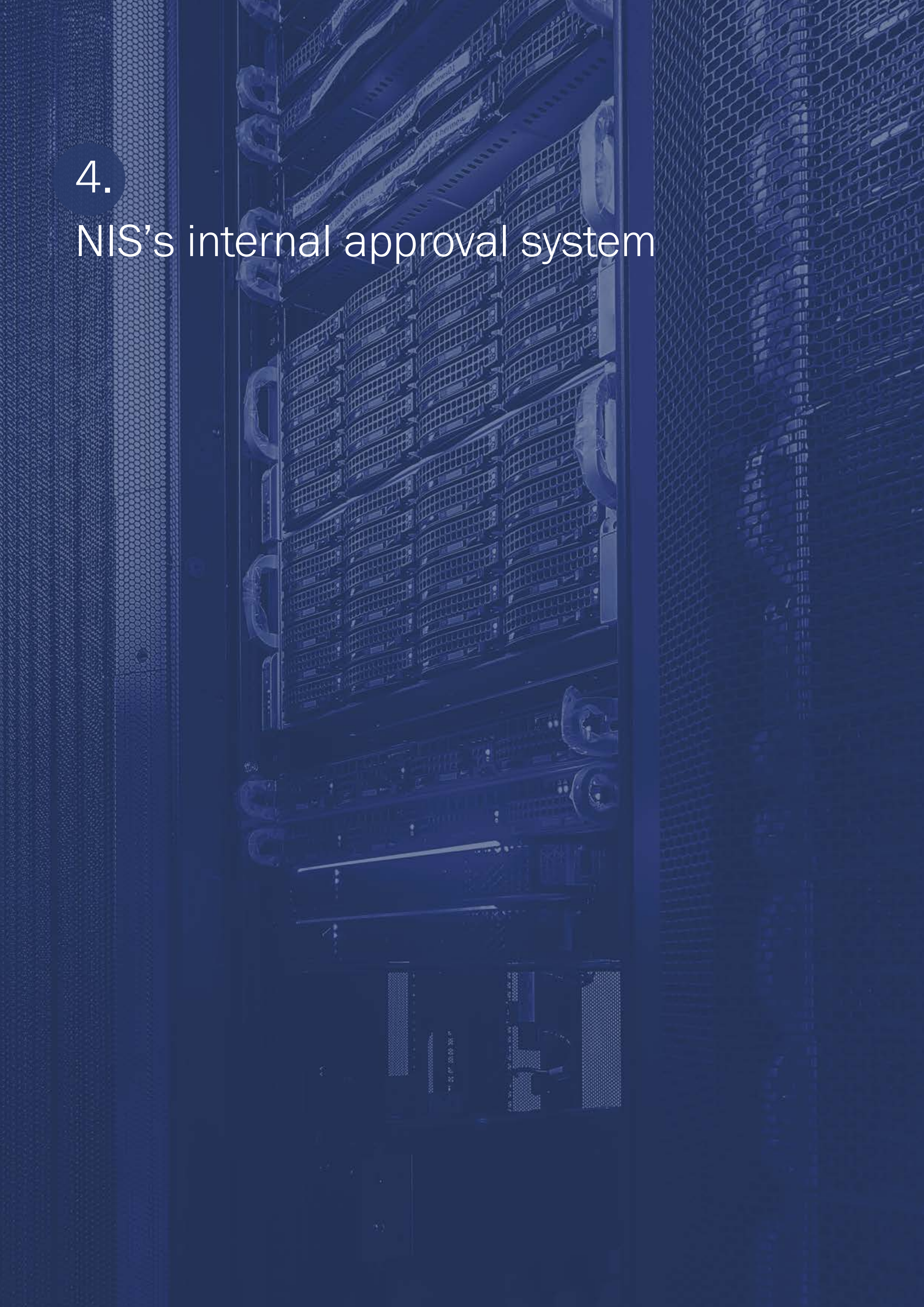
30 Klass and others v. Germany, 6 September 1978, Published in Series A 28 (1979).

31 *Report to the Storting from the Evaluation Committee for the Norwegian Parliamentary Intelligence Oversight Committee*, Document 16 (2015–2016), section 27.2.3.

32 In his report prepared for the Evaluation Committee entitled *Hvilke krav stiller Grunnloven og EMK til etterfølgende kontroll av sikkerhets- og etterretningstjenestenes inngrep i menneskerettigheter?* ('What requirements do the Constitution and the ECHR stipulate for subsequent oversight of the security and intelligence services' interference with on human rights?'), Professor Erling Johannes Husabø concludes as follows in section 3.2.2: 'It is therefore doubtful whether the Intelligence Service's present legal basis meets the requirements that currently apply under the ECHR.'

33 Letter of 28 January 2016 from NIS to the EOS Committee.

4. NIS's internal approval system



The general requirements set out in Act No 31 of 14 April 2000 relating to the Processing of Personal Data (the Personal Data Act) concerning specification of purpose, necessity and relevance apply to all processing of personal data by NIS.[34] NIS has developed an internal approval system for certain categories of processing, sharing and collection of information.

First of all, NIS has a general procedure in place for approving the processing of information about persons with connections to Norway in accordance with the Intelligence Service Act Section 4 second paragraph, cf. Section 3. The second internal approval procedure is based on the supplementary provisions concerning the Norwegian Intelligence Service's collection of information concerning Norwegian persons abroad and the disclosure of personal data to cooperating foreign services, adopted by the Ministry of Defence on 24 June 2013 pursuant to the Intelligence Service Instructions Section 17. NIS carries out technical surveillance of certain Norwegian persons abroad in accordance with the guidelines provided in the above-mentioned provisions. The third and final approval procedure relates to the service's searches in stored metadata to find communication between selectors linked to Norwegian legal persons in Norway and intelligence targets abroad for purposes relevant to foreign intelligence. As mentioned above, these searches raise particular questions that will be discussed in greater detail in chapter 5.

All internal approvals are routinely submitted to the Committee. The regime developed by NIS shows that the service is concerned with the due process protection of individuals in that the basis for processing, sharing and collecting information is assessed and documented. This documentation also allows the Committee to perform its oversight tasks. The assessment criteria correspond to the ordinary principles for the processing of personal data, cf. the above reference to the Personal Data Act.

It can be argued that there are special considerations relating to the activities of NIS that indicate that the conditions for collecting and processing personal data should be more closely regulated by law. In the Committee's opinion, more detailed regulation in law would strengthen due process protection in an area where individuals have no right to access information stored about them and cannot even get an answer about whether or not NIS is processing information about them. Not even when the Committee criticises NIS's processing of information about a person who has filed a complaint with the Committee will the person in question be informed about which personal data the service is processing or what the basis for the criticism was.[35]

In the same way as the use of covert coercive measures by the police and PST is authorised by the courts in advance, external prior approval of use of intrusive methods by NIS is also conceivable. This is particularly relevant when surveillance targets Norwegian citizens abroad, which is currently happening in practice in counterterrorism work. In the current situation, the authority to make decisions regarding surveillance activities targeting a Norwegian citizen abroad lies with NIS itself, while PST must obtain prior court approval to use coercive measures when the person in question is in Norway. PST is also subject to a requirement for renewed court approval at certain intervals when using coercive measures.

NIS's internal approval system confirms that the service is highly aware of the challenges its activities involves in relation to the protection of privacy and the fact that surveillance activity is subject to internal regulation. The Committee has not found that the service initiates surveillance outside the scope of its oversight regime.

> **The Committee is of the opinion that it is necessary for the legislators to consider whether NIS's processing of personal data in the performance of its tasks should be regulated further in law, and whether the use of intrusive methods should be subject to court approval or similar in addition to the EOS Committee's subsequent external oversight.**

34 The Personal Data Act Sections 31 (Obligation to give notification), 33 (Obligation to obtain a licence) and Section 44 first to third paragraphs (Access of the supervisory authorities to data) do not apply to '[p]ersonal data processing that is necessary in the interests of national security or the security of allies, the relationship to foreign powers and other vital national security interests', cf. the Personal Data Regulations Section 1-2.

35 See Document 7:1 (2014-2015) The EOS Committee's annual report to the Storting for 2014, section 6.7.

5.

About particular issues relating to collection of and searches in metadata

5.1 Background

In its annual report for 2014, the Committee stated that it was working on issues relating to the legal basis in the Intelligence Service Act for NIS's use of methods.[36] NIS conducts searches in stored metadata based on selectors relating to Norwegian legal persons in Norway. The purpose of these searches is to identify selectors for purposes relevant to foreign intelligence, typically selectors belonging to Norwegian counterterrorism targets abroad. By metadata is meant information about data, such as times, duration, to/from indicators, type of traffic and other parameters that describe a technical event that has taken place in a communication network. A selector can be a phone number, an email address, a Facebook username etc.

The head of NIS adopted *Provisions for metadata searches that could concern Norwegian legal persons* on 13 August 2014. These provisions show that the overriding objective of metadata searches is either to attempt to uncover information about foreign targets not previously known to the service, or to collect further information about known foreign targets.

The actual collection of metadata that may include metadata about communication to and from Norwegian legal persons in Norway is assessed in section 5.2, while the service's searches in metadata for purposes relevant to foreign intelligence will be assessed in section 5.3.

5.2 Collection of metadata that may include metadata about communication to and from Norwegian legal persons in Norway

5.2.1 Introduction

The background to this issue is NIS's technical collection of metadata following technical analysis. All the metadata are stored without any information being filtered out. The metadata collected may include communication to and from Norwegian legal persons in Norway if they communicate with persons in geographical areas targeted by NIS's technical collection capacity. For technical reasons, it will *never* be the case that both parties to the communication are located in Norway. NIS has informed the Committee that metadata are only deleted after being stored for several years, and that the storage period is based on intelligence grounds.

The collection of metadata targets the thematic areas about which the service is tasked with obtaining information pursuant to the Intelligence Service Act and the Ministry of Defence's priorities, cf. the Intelligence Service Act Section 3. The collection of metadata entails 'processing' of 'personal data', as the information in question that is used by NIS is 'information (...) that may be linked to a natural person'.[37, 38]

5.2.2 NIS's assessment

NIS's regulatory framework is technology-neutral, and the methods to be used are not specified, but the methods must be used to carry out the tasks defined in Section 3 of the Intelligence Service Act. Section 4 of the Intelligence Service Act limits the service's remit by prohibiting covert collection of information about Norwegian legal persons on Norwegian territory. The service obtains large quantities of metadata based on what is assumed to yield as much information as possible relevant to foreign intelligence.

NIS distinguishes between what is known as target identification and covert collection. Target identification is the work carried out to find and collate information to allow a legal or physical person to be identified. It is only once technical data collection is initiated on the basis of an identified person's selectors that the processing of information is defined by the service as covert collection and must not fall under the prohibition on monitoring of Norwegian citizens in Norway set out in Section 4 of the Intelligence Service Act. NIS is of the opinion that the wording of the prohibition against covert collecting of information 'concerning' Norwegian persons must be understood to mean 'targeted'. This must be interpreted to mean that an intention to monitor must be involved. The collection of metadata that may include communication to and from Norwegian legal persons falls under the service's tasks as defined in the Intelligence Service Act Section 3. Such collection involves no intention to monitor, and does not, therefore, constitute a violation of the Intelligence Service Act Section 4.

NIS points out that a different interpretation would have dramatic consequences for the service's ability to perform its statutory duties.

NIS's statement is included in full as Appendix 2 to this report.

5.2.3 The EOS Committee's assessment

Section 3 of the Intelligence Service Act instructs NIS to 'collect, process and analyse information' for certain purposes. The prohibition in Section 4 of the Act concerns monitoring or in any other covert manner collecting information. When these two provisions are viewed together, that raises the question of whether 'collect' in Section 3 means the same as 'monitor or in any other covert manner collect' in Section 4. If these terms are to be understood to mean the same, it will mean that the prohibition will apply to all information actively

36 See Document 7:1 (2014-2015) The EOS Committee's annual report to the Storting for 2014, section 1.4.3.

37 Cf. Act No 31 of 14 April 2000 relating to the Processing of Personal Data (the Personal Data Act) Section 2 first paragraph (1).

38 Cf. the Personal Data Act Section 2 first paragraph (3).

collected by NIS if the information includes data concerning Norwegian legal persons on Norwegian territory. If the term as used in Section 4 of the Intelligence Service Act is to be interpreted more narrowly than the term 'collect' used in Section 3, the question becomes by which criteria a specific information collection method must be deemed to constitute monitoring in the sense of the prohibition.

The Committee has concluded that there are two possible interpretations regarding the lawfulness of NIS's collection of metadata that may include communication to and from Norwegian legal persons in Norway:

5.2.3.1 Interpretation 1

The wording 'monitor or in any other covert manner collect information' in the Intelligence Service Act Section 4 could be interpreted as referring to the use of covert methods to obtain information that is not publicly accessible. Under this interpretation, the collection of metadata as described above would violate the prohibition in Section 4 of the Intelligence Service Act simply because it includes metadata concerning Norwegian legal persons in Norway.

The challenge of such an interpretation is that it does not take into consideration the purpose of the Intelligence Service Act and NIS's ability to perform its tasks in an effective manner, cf. the Intelligence Service Act Sections 1 and 3, and this is an argument in favour of a narrow interpretation of the concept of collection in the prohibition.

5.2.3.2 Interpretation 2

NIS collect metadata in order to obtain 'targeted, timely and relevant information about foreign circumstances that correspond to the national authorities' defined intelligence needs' and is of the opinion that it is 'necessary to analyse and process huge amounts of information to which the service has access'.[39] The Committee bases its work on NIS's statement regarding effectiveness and the intelligence need to collect metadata. NIS is of the opinion that the prohibition in the Intelligence Service Act Section 4 must be understood to apply to covert collection *targeting* Norwegian persons, and that, consequently, it must be interpreted to mean that an intention to monitor must be involved.

Based on the above, it can be argued that the statement regarding a qualified form of surveillance in the preparatory works indicate that the wording 'monitor or in any other covert manner collect information' must be understood more narrowly in order to ensure that NIS can perform its tasks effectively, cf. the Intelligence Service Act Sections 1 and 3.

The challenge associated with such an interpretation is that the legislation provides no directions about where the line must nevertheless be drawn. This raises the question of when an intention to monitor exists and to what extent the measure interferes with protection of privacy.

5.2.3.3 The EOS Committee's conclusion

The Committee is of the opinion that this issue arises as a result of developments in the threat situation and technology, and it raises the question of where the point of intersection between personal data protection and consideration for national security and inhabitants' security should be. In the Committee's view, some uncertainty is attached to the legality of collection of metadata that may contain information about Norwegian citizens in Norway. This indicates that the issue should be submitted to the Storting.

> **The EOS Committee is of the opinion that NIS's practice for collecting metadata that may include selectors belonging to Norwegian legal persons in Norway should be submitted to the Storting for consideration of whether it is necessary to amend the Intelligence Service's regulatory framework.**

5.3 Searches conducted by NIS in stored metadata relating to Norwegian legal persons in Norway to find selectors for purposes relevant to foreign intelligence

5.3.1 Introduction

It came to the Committee's attention in 2014 that the service conducts searches in stored metadata relating to Norwegian legal persons in Norway in order to obtain information relevant to foreign intelligence. One side of the communication will originate with a selector used abroad, while the other side could originate with a Norwegian legal person in Norway.

NIS has the capacity to conduct advanced searches in and complex analyses of large amounts of data. These searches and analyses can be of different types and take place in different ways.

5.3.2 NIS's assessment

NIS refers to the fact that its target identification work is carried out by searching large amounts of source data legally collected by the service by means of their technical capacities, cf. section 5.2.2 above. The searches are conducted with a view to identifying information about legal intelligence targets. Such searches yield, either directly or following analysis, information about targets of intelligence interest that covert information collection measures can then be initiated in relation to.

NIS emphasises 'both that the searches do not target the Norwegian person, but are based solely on the person in question's selector, and that the searches are not carried out with the intention of monitoring the person in question'.[40] In the NIS's opinion, the metadata searches are thus not considered collection under the Intelligence Service Act Section 4. NIS also points out that 'the term covert relates to the collection method and focus of the collection activity, not to the subsequent analysis and collation of information that has already been collected'.[41]

NIS also refers to the fact that the foreign intelligence purpose means that it is not one of PST's tasks to collect the relevant data.

NIS emphasises that discontinuing this method would have serious consequences for the service's ability to perform its statutory tasks in some areas.

NIS's statement is included in full as Appendix 2 to this report.

5.3.3 The EOS Committee's assessment

The Committee has seen examples of searches conducted by NIS in stored metadata that originated with different categories of persons. The internal approvals[42] emphasise whether there are weighty operational reasons for conducting such searches, assessments of threat potential in relation to Norway, and concrete grounds for necessity, including the expected outcome of the searches.

NIS has specified that the searches are not designed or conducted to obtain information about the Norwegian legal person. However, the issue that the Committee problematises is that selectors belonging to Norwegian legal persons in Norway are used as a means to achieving what is, pursuant to Section 3 of the Intelligence Service Act, a legitimate goal. In the Committee's opinion, it is difficult to find support for such a method in the present regulatory framework.

NIS points out that the term 'covert' in the prohibition refers to the actual collection of information, not subsequent searches and collation. The Committee does not agree with this interpretation. Active searches in and collation of information from selectors belonging to identified Norwegian legal persons obtained using covert collection capacities cannot be deemed to be anything other than targeted information collection targeting these persons, even if it is not done for the purpose of collecting information about the Norwegian legal persons in question. New information is always processed in connection with searches and analyses. This will apply regardless of NIS's expert assessment of relevance considered in isolation. The prohibition in the Intelligence Service Act Section 4 limits the service's possibility to obtain information relevant to foreign intelligence. In the Committee's opinion, it is for the legislators to decide whether such restrictions *should* or *should not* be imposed on NIS.

Pursuant to the Oversight Act Section 2 second paragraph, the Committee shall 'show consideration for national security and relations with foreign powers' in its oversight activities. It is stated in the preparatory works to the Oversight Act that the Committee's duty to balance oversight considerations against national security considerations means 'that the Committee's opinions shall be arrived at following an assessment which takes account of the considerations that the intelligence, surveillance and security services are charged with safeguarding'.[43] These instructions are intended to 'prevent a one-sided emphasis on the oversight purposes while exercising oversight'.[44]

In light of NIS's legal assessment and account of the intelligence need to conduct searches in order to be able to effectively perform its statutory tasks and the Committee's duty to take account of national security considerations, the Committee has not found grounds for criticising the service or requesting that use of the methods be suspended. The purpose of this report is to notify the Storting of a potential need for legislative amendment.

> **In the Committee's opinion, the legal position of NIS's searches in metadata for selectors belonging to Norwegian legal persons for foreign intelligence purposes is so unclear that the Storting is hereby informed.**

> **The Committee considers it a task for the legislators to decide whether NIS should be permitted to collect information relevant to foreign intelligence via selectors relating to Norwegian legal persons in Norway and, if so, what conditions and oversight mechanisms should apply.**

---

39 NIS's memo of 21 July 2014.

40 Letter of 28 January 2016 from NIS to the EOS Committee.

41 Letter of 28 January 2016 from NIS to the EOS Committee.

42 See chapter 4 of this special report.

43 Official Norwegian Report NOU 1994:4 *Kontrollen med "de hemmelige tjenestene"* ('Oversight of the 'secret services' – in Norwegian only), section 7.2.2 *Om kontrollen* ('About the oversight').

44 See Proposition No 83 to the Odelsting (1993-1994), chapter VI.

6.
Summary

The Committee is of the opinion that the actual, technological and legal developments that have taken place since the Intelligence Service Act was adopted give reason to notify the Storting of a potential need to examine whether NIS should be given a clearer legal basis for all the methods it uses that interfere with the rights of individuals, with pertaining due process protection. The fact that Norwegian legal persons increasingly become foreign intelligence targets as a result of participation in international terrorism indicates that the legal challenges that this gives rise to should be considered by the Storting.

NIS has kept the Committee informed about developments in the service's use of methods. The service has prepared internal procedures to ensure that surveillance takes place in compliance with the legal basis for the service, including the framework stipulated by the head of NIS on the basis of political approval of its methods. NIS has also facilitated the Committee's oversight of all surveillance conducted under this regime. The Committee finds that NIS has demonstrated understanding of the Committee's oversight requirements.

The Committee is of the opinion that NIS's collection of metadata that may include selectors belonging to Norwegian legal persons in Norway should be submitted to the Storting for consideration of whether it has sufficient legal basis.

In the Committee's opinion, NIS's searches in stored metadata based on selectors relating to Norwegian legal persons in Norway for purposes of foreign intelligence are problematic in relation to Section 4 of the Intelligence Service Act. NIS has a different view of the legal status of these searches than the Committee. NIS has also explained its assessment of the necessity of these searches in order to perform the service's tasks, and the Committee has taken note of this account. Considering the legal ambiguity and the expert assessment of the need for these searches, the Committee has neither found reason to criticise the service nor requested it to suspend some information collection methods pending possible consideration by the Storting of the issues raised by the Committee.

The Committee shares NIS's view that the regulatory framework for the service's activities must both facilitate its ability to perform its tasks effectively and address security considerations, but is of the opinion that the democratic considerations pointed out by the Committee indicate that the Storting should, following a report, consider how the different considerations can best be balanced against each other.

7. Appendices

7.1 Appendix 1 – NIS's general statement

The following statement was made by NIS in a letter to the EOS Committee dated 4 May 2016.

'NIS is of the opinion that there are shortcomings in the argument that forms the basis for concluding [*The EOS Committee's comment: NIS's summary of Professor Husabø's conclusion*] that the legal basis is vague and questionable from a human rights perspective. NIS emphasises legal predictability for all parts of its activities and agrees with the EOS Committee's statement that the collection of information about individuals falls under the scope of the principle of legal authority. We are also of the opinion that human rights govern all our activities abroad. Our activities are regulated by the Human Rights Act, the Personal Data Act and the Intelligence Service Act, and these laws must be seen in conjunction with each other. The legislation of most other countries is no more specific or detailed when it comes to the use of methods and the processing of personal data. Our tasks are regulated by law in as much detail as for PST, and the processing of personal data is in principle as clearly regulated in the Personal Data Act for NIS as it is in the Police Register Act for PST. The oversight provisions are no more limited than they are for PST. NIS has requested from the EOS Committee an account of what, if any, specific shortcomings the Committee finds in the present legal basis, but has received no reply.

The PST's use of methods is likewise not fully regulated in law. Furthermore, it is self-evident that police methods used by a domestic security service are regulated to a considerably greater extent that the methods used by a foreign intelligence service. The methods cannot be described in detail in publicly accessible regulations. When the Intelligence Service Act was adopted, it was a well-considered decision to make the legal basis for collecting method- and technology-neutral, and this is also the norm for corresponding legislation in comparable states. Comparing strategic foreign intelligence activities with domestic police activities for the purpose of preventing and fighting crime demonstrates a lack of knowledge of the fundamental differences between the two. While police agencies focus on building a legal case relating to a criminal offence that has been committed or is being planned (historical perspective with strong focus on the chain of evidence), intelligence services focus on reducing uncertainty for important decision-makers, with a particular focus on predicting the future – assessing unknown trends and actions carried out by states, organisations and individuals without considering whether they have committed criminal offences or will commit a crime, and without consideration for preserving the integrity of information in such a way that it can be used in court proceedings. A foreign intelligence service must necessarily cast a wide net (target searches) to find information needed by superior authorities. Intelligence is, by its nature, about collecting and analysing large amounts of information. The focus is on information, not individuals, and there is in principle no stigma attached to of interest to NIS.

If the Intelligence Service Act does not comply with human rights, then the same applies to the vast majority of European states. When NIS nevertheless takes a positive view of our legal basis being reviewed with a view to updating and modernising it, it is partly because public allegations of the inadequacy of our legal basis represent a challenge in themselves. It is also problematic that such allegations are made while matters of principle relating to digital border control are under consideration, because the Lysne II Committee can hardly consider granting the service new access if the framework conditions for the service are otherwise perceived to conflict with the applicable human rights requirements. NIS therefore takes a positive view of its legal basis being reviewed with a view to making any necessary adjustments in order to prevent similar allegations in future. Another argument for revising the law is that actual, technological and legal developments require continuous assessment of NIS's legal basis.'

7.2 Appendix 2 – NIS's statement Collecting of and searches in metadata

The following statement was made by NIS in a letter to the EOS Committee dated 4 May 2016.

'There is no getting away from the fact that information collection targeting legal foreign targets will make it necessary for the service to be able to also legally process information about Norwegian persons. This is assumed in Section 4 second paragraph of the Intelligence Service Act. What is prohibited is to engage in active and covert collection targeting Norwegian persons in Norway. In order for collection to be prohibited, the service must know or deem it highly likely that the collection targets such a person. In the opposite case, all (surplus) information about Norwegian persons which the service receives as part of its collection targeting non-Norwegian persons will constitute a violation of the Intelligence Act Section 4 first paragraph. Such an interpretation will also mean that storing metadata (which may also relate to Norwegian persons) in itself constitutes a violation of the Intelligence Act Section 4 first paragraph. This is an understanding of the law that has never before been advocated, and one that would have dramatic consequences for the service's existing activities. ***Among other things, it would mean that all target search activities and***

all storage of metadata would have to cease. In practice, this would make it impossible to carry out foreign intelligence services in Norway, because all intelligence work is based on the principle that it is legitimate and necessary to have access to large amounts of data in order to be able to identify unknown threats and relevant information, and that it is legitimate and necessary to store selected data in order to allow for retrospective analyses. In other words: You will never find the needle in the haystack unless you have access to relevant parts of the haystack, and intelligence work can never be based solely on information available at a specific moment. NIS must also store information over time so that it can gain a clearer picture of the normal situation and be able to see when something deviates from the norm. This part of the intelligence process, which starts with target searches, is fundamentally different from, and can in no way be compared with, the police's criminal intelligence work, which requires a direct and contextual link to specific (potential) criminal offences before storage of personal data is permitted.

This understanding of the law also contrasts with statements previously made by the EOS Committee, including the Committee's concluding letter to the service in connection with what was known as the sources archive case, in which it was emphasised that the registration of source information about Norwegian third parties was not based on an intention to monitor them.

Target identification is one of NIS's most important activities. Metadata searches for target identification purposes give NIS a unique opportunity to identify new threat actors abroad that communicate with Norwegian persons so that NIS can obtain information critical to protecting Norway and Norwegian interests against external threats. In line with the service's statutory tasks, communication data is collected and stored by the service on a daily basis. Collection is targeted and based on criteria used to select information that is relevant from a foreign intelligence perspective. Metadata storage is both a relevant and a necessary part of intelligence work. The types of communication data stored and how they are selected cannot be described in more detail in a public presentation.

To begin with, NIS would like to note that we see arguments in favour of metadata storage and searches being mentioned in publicly accessible regulations. The service's internal legal assessment of 21 July 2014 concluded that it '[should] be considered whether elements can be publicly communicated or included in unclassified regulations'. At the same time, however, we consider it unlikely and inexpedient for the Storting to enshrine in law details relating to the service's different log searches in different types of data stored by the service. This would make the regulation of the service's information management far more detailed than that which applies to PST or other Norwegian public authorities. We therefore believe that it would be more expedient for it to be regulated in underlying regulations, which could very well be publicly accessible. We see no reason to deviate from the customary principles concerning what traditionally belongs in formal laws and what belongs in regulations or similar.

NIS emphasises that log searches do not result in covert collection of more information than the service already possesses; such searches only select relevant metadata from a large amount of communication data already stored by the service. The crux of the matter is which search methods the service should use when searching for information relevant to foreign intelligence in different types of source data already legally held by the service. The goal of the search, what the service is searching *for*, is always within the scope of the tasks defined in Section 3 of the Intelligence Service Act. If the opposite were the case – if the search was aimed at obtaining information about Norwegian persons in Norway – that would be a clear violation of the Intelligence Service Act Section 4 first paragraph.

The following example can serve to illustrate the search method:

The information need that NIS works to meet is *'Obtain unknown selectors (phone number, email address or similar) belonging to a known terrorist in conflict area X.'* NIS has received indications from other sources that the terrorist is communicating with acquaintances in Oslo, and the service has received information from PST or other authorities about the identity of the acquaintances in question and the selectors they use. In such a case, collection is not initiated for any selectors. However, the answer to the information need may already exist in traffic data previously stored by NIS for foreign intelligence purposes. Searches in such data can either be based on foreign selectors, with countless queries of the type 'Has selector A in conflict area X been in contact with a selector in Oslo?' or 'Has selector B in conflict area X been in contact with a selector in Oslo?', etc. When the search returns a hit for a selector in Oslo, the next query will be: 'Is the selector in Oslo identical to the selector belonging to the terrorist's acquaintance?' This search method uses the foreign terrorist as its point of departure. The more time-efficient alternative search method is to use the Norwegian selector as the point of departure and ask: 'Has the selector belonging to the terrorist's acquaintance communicated with selectors in conflict area X?' In this case, the Norwegian selector is the point of departure, and the method arrives at the same answer faster compared with using the foreign selector as the point of departure. In both cases, NIS has no interest in the Norwegian acquaintance.

The country that is most important to the Norwegian foreign intelligence service is Norway, both generally and from a threat perspective. In order for NIS to be able to warn of external threats to Norway, foreign threat actors' activities in and related to Norway are obviously matters of foreign intelligence interest. This includes communication between foreign parties of interest and Norwegian persons.

The legislators predicted as early as in 1998 that NIS would have to process information about Norwegian citizens in order to perform its statutory tasks. Section 4 of the Intelligence Service Act is based on this assumption. Moreover, Section 3 of the Intelligence Service Act states that the service is to collect information 'regarding Norwegian interests' viewed in relation to foreign states, organisations or private individuals. The link between Norwegian interests and the foreign intelligence target will therefore be of interest to a foreign intelligence service. In its searches for information about a foreign intelligence target, NIS will sometimes need to be able to use information that it already possesses about Norwegian persons as a starting point for searches, for example mapping foreign connections of intelligence interest who communicate with Norwegian persons. Only the foreign connections have further intelligence value, and any covert information collection measures initiated will only target them. As mentioned above, there is no question of collecting new information about the Norwegian person using covert methods or of collecting or processing information with a view to mapping domestic circumstances or circumstances relating to the Norwegian person. NIS is therefore of the opinion that such searches do not fall under the prohibition in the Intelligence Service Act Section 4. In its legal assessment of 21 July 2014, the service concluded that the method is not in violation of the regulatory framework that applies to the service's activities, and that metadata searches based on a Norwegian person's selector are not generally considered covert collection in violation of the Intelligence Service Act Section 4 first paragraph. However, we pointed out that there are some elements of legal uncertainly associated with such searches, particularly if the purpose of the search is unclear. In order to remedy this situation, the service, on 13 August 2014, put in place internal regulations *(Bestemmelser for metadatasøk som kan berøre norske rettssubjekter)* that stipulate clear criteria for when the method can be used and how it should be overseen by the EOS Committee. Target identification using metadata searches based on a selector belonging to an identified Norwegian person is only conducted with the approval of the head of NIS, and only when warranted by weighty operational reasons.

Target identification based on a Norwegian selector is a highly valuable tool in several areas, including in counterterrorism. One example is that the service can use a Norwegian IP address which it knows has experienced a serious cyber incident as a starting point for its endeavours to find communication to and from the address that could identify espionage by a foreign state and that party's modus operandi.

One might wonder why corresponding data cannot be collected by PST under its legal basis. The answer to this question is simple: PST is not a foreign intelligence service. It is not PST's job to obtain metadata that is assumed to result in information relevant to foreign intelligence, nor does it have the legal right to do so. Thus, target identification on the part of NIS as described above does not involve circumvention, since PST neither can nor should provide answers to such information needs. This tasks lies exclusively with NIS. ***The loss of this opportunity would have serious consequences for the service's ability to carry out its statutory tasks, particularly in the areas of counterterrorism, counterproliferation and SIGINT support for the Norwegian Cyber Defence***. The decisive argument for retaining the method is not the operational need, however, but the fact that the method involves no intention to monitor Norwegian persons in Norway, and therefore does not constitute covert collection of information concerning Norwegian persons on Norwegian territory. The term covert relates to the collection method and focus of the collection activity, not to the subsequent analysis and collation of information that has already been collected. The actual collection of data has sufficient legal basis in the Intelligence Service Act Section 3. The service emphasises both that the searches do not target the Norwegian person, but are based solely on the person's selector, and that the searches are not carried out with the intention of monitoring that person. The type of information collection concerned, the way in which metadata searches are conducted, the number of searches conducted, and the fact that searches and information needs and thus the subsequent analysis and reporting exclusively target legitimate foreign intelligence targets are all factors that indicate that interpretation 2 is a correct and satisfactory interpretation of the Intelligence Service Act and that the service's practice as regards metadata searches is both legitimate and necessary.'

Photo: Forsvaret/Kjosvold

EOS COMMITTEE

NORWEGIAN PARLIAMENTARY OVERSIGHT COMMITTEE
ON INTELLIGENCE AND SECURITY SERVICES

fdesign.no

Contact information

Telephone: +47 23 31 09 30
Email: post@eos-utvalget.no
Postal address: PO box 84 Sentrum, N-0101 Oslo, Norway
Office address: Akersgata 8, Oslo

www.eos-utvalget.no