



**NORWEGIAN PARLIAMENTARY  
OVERSIGHT COMMITTEE**  
ON INTELLIGENCE AND SECURITY SERVICES



# ANNUAL REPORT 2018

**DOCUMENT 7:1 (2018–2019)**




## 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 17 third paragraph, the Committee hereby submits its report about its activities in 2018 to the Storting.

The annual report is unclassified, cf. the Oversight Act Section 17 third paragraph. Pursuant to the Act relating to Protective Security Services (the Security Act), the issuer decides whether or not information is classified. Before the report is submitted to the Storting, we send the relevant sections of the report text to each of the respective services for them to clarify whether the report complies with this requirement. The services have also been given the opportunity to check that there are no errors or misunderstandings in the text.

Oslo, 27 March 2019

  
Eldbjørg Løwer

  
Svein Grønnern

  
Theo Koritzinsky

  
Øyvind Vaksdal

  
Håkon Haugli

  
Inger Marie Sunde

  
Eldfrid Øfsti Øvstedal

  
Henrik Magnusson



Photo: Ingar Sørensen

The Norwegian Parliamentary Intelligence Oversight Committee in 2018. From left: Inger Marie Sunde, Håkon Haugli, Eldfrid Øfsti Øvstedal, Theo Koritzinsky, Eldbjørg Løwer (Committee Chair), Svein Grønnern (Deputy Chair) and Øyvind Vaksdal.

# Contents

<b>1.</b>	<b>The Committee's remit and composition</b>	<b>6</b>
<b>2.</b>	<b>Overview of the Committee's activities</b>	<b>9</b>
2.1	Summary – main issues in the oversight of the services	10
2.2	Oversight activities carried out	10
<b>3.</b>	<b>Developments and international oversight cooperation</b>	<b>12</b>
3.1	The Secretariat's technology unit has been strengthened, but needs more resources	13
3.2	International oversight cooperation	13
3.3	Anonymity for whistle-blowers	14
<b>4.</b>	<b>The Committee's consultation submissions</b>	<b>15</b>
4.1	Consultation concerning a draft bill for a new Intelligence Service Act	16
4.2	Consultation concerning draft regulations to the Security Act	16
4.3	Consultation concerning the application of the Security Act for the Storting's external bodies	16
<b>5.</b>	<b>The Norwegian Police Security Service (PST)</b>	<b>17</b>
5.1	General information about the oversight	18
5.2	PST's disclosure of information in security clearance cases	18
5.2.1	Introduction	18
5.2.2	How PST discloses information – use of meetings and inadequate documentation	18
5.2.3	Can PST withhold relevant information?	19
5.2.4	Disclosure of unconfirmed information	20
5.2.5	Conclusions and follow-up	21
5.3	PST's disclosure of information to the security clearance authorities in three cases	21
5.3.1	Background	21
5.3.2	Case 1 – Inadequate documentation of information disclosed	21
5.3.3	Case 2 – Unlawful disclosure of information about political involvement	21
5.3.4	Case 3 – Disclosure of incorrect information	21
5.4	For how long can PST store information before an assessment of necessity must be carried out?	22
5.5	PST's collection of chat logs	22
5.6	Non-conformity reports – PST's use of coercive measures	24
5.7	Complaint cases considered by the Committee	24
<b>6.</b>	<b>The National Security Authority (NSM)</b>	<b>25</b>
6.1	General information about the oversight	26
6.2	Special report to the Storting on differing practices in the security clearance of persons with connections to other states	26
6.3	Complaint cases considered by the Committee	27
6.3.1	Introduction	27
6.3.2	Complaint case 1 – Person with no need for security clearance	27

6.3.3	Complaint case 2 – Inadequate access to information in a case where the Committee disagrees with the grounds given by NSM	28
6.3.4	Complaint case 3 – Inadequate grounds and information to the complainant and inadequate documentation	28
6.3.5	Complaint case 4 – Long case processing time	29
6.4	Case processing times in security clearance cases	29
<b>7.</b>	<b>The Norwegian Defence Security Department (FSA)</b>	<b>30</b>
7.1	General information about the oversight	31
7.2	Use of vetting information for purposes other than security clearance assessments	31
7.3	Case processing times in security clearance cases	31
<b>8.</b>	<b>The Norwegian Intelligence Service (NIS)</b>	<b>32</b>
8.1	General information about the oversight	33
8.2	NIS's collection of information from open sources about persons in Norway	33
8.3	NIS's collection of content data about a Norwegian citizen	34
8.4	NIS is not permitted to go through content data collected in breach of the law	35
8.5	Collection of communication when one party is in Norway	36
<b>9.</b>	<b>Oversight of other EOS services</b>	<b>37</b>
9.1	General information about the oversight	38
9.2	The Joint Cyber Coordination Centre (FCKS)	38
9.3	Inspection of the Army Intelligence Battalion	38
9.4	Inspection of the Norwegian Special Forces Command	39
9.5	Inspection of the Norwegian Communications Authority (Nkom)	39
9.6	Inspection of Telia Norge AS	39
9.7	The personnel security service of the Office of the Auditor General	39
9.8	Security interviews project	40
9.9	Complaints against security clearance decisions made by the Ministry of Defence	40
<b>10.</b>	<b>Communication, external relations and the media in 2018</b>	<b>41</b>
10.1	Publication of Committee statements via channels other than the annual report	42
10.2	External relations, annual conference and study trip to the USA	42
10.3	The EOS Committee in the media in 2018	43
10.4	Administrative matters	43
<b>11.</b>	<b>Appendices</b>	<b>44</b>
	Appendix 1 – Meetings, visits, lectures and participation in conferences etc.	45
	Appendix 2 – News from foreign oversight bodies	47
	Appendix 3 – Consultation concerning a draft bill for a new Intelligence Service Act	48
	Appendix 4 – Joint statement with four other oversight bodies: Strengthening oversight of international data exchange between intelligence and security services	67
	Appendix 5 – Act relating to oversight of intelligence, surveillance and security services (The Oversight Act)	78



**1.**

## The Committee's remit and composition

The EOS Committee is a permanent, Storting-appointed oversight body whose task it is to oversee all Norwegian entities that engage in intelligence, surveillance and security activities (EOS services). Only EOS services carried out by, under the control of or initiated by the public administration are subject to oversight by the EOS Committee.<sup>1</sup>

Pursuant to the Oversight Act<sup>2</sup> Section 2 first paragraph, the purpose of the oversight is:

1. to ascertain whether the rights of any person are violated and to prevent such violations, 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 unduly harm the interests of society, and
3. to ensure that the activities are kept within the framework of statute law, administrative or military directives and non-statutory law.

The Committee shall show consideration for national security and relations with foreign powers in its oversight activities.<sup>3</sup> We shall not seek more extensive access to classified information than warranted by the oversight purposes<sup>4</sup>, and shall insofar as possible show consideration for protection of sources and the safeguarding of information received

from abroad. Subsequent oversight is practised in relation to individual cases and operations, but we are entitled to be informed about the services' current activities. The Committee may not instruct the EOS services it oversees or be used by them for consultations. The oversight shall cause as little inconvenience as possible to the services' operational activities.<sup>5</sup>

The Committee has seven members. They are elected by the Storting in plenary session on the recommendation of the Storting's Presidium for terms of up to five years.<sup>6</sup> No deputy members are appointed. Following a statutory amendment in 2017, the members may be re-appointed once and hold office for a maximum of ten years.

The Committee is independent of both the Storting and the Government.<sup>7</sup> This means that the Government cannot issue instructions to the Committee, and members of the Storting cannot also be members of the Committee. The Committee has a broad composition so that both different political backgrounds and experience from other areas of society are represented. The committee members and secretariat employees must have top-level security clearance and authorisation, both nationally and pursuant to treaties to which Norway is a signatory.<sup>8</sup> This means security clearance and authorisation for TOP SECRET and COSMIC TOP SECRET, respectively.

1 References to the Oversight Act are found in Act No 10 of 20 March 1998 relating to Protective Security Services (the Security Act) Section 30, Act No 11 of 20 March 1998 relating to the Norwegian Intelligence Service (the Intelligence Service Act) Section 6, Instructions No 695 of 29 April 2010 for Defence Security Service Section 14, and Act No 16 of 28 May 2010 regarding Processing of Information by the Police and Prosecuting Authority (the Police Register Act) Section 68.

2 Act No 7 of 3 February 1995 relating to the Oversight of Intelligence, Surveillance and Security Services (the Oversight Act). The Act was most recently amended in June 2017.

3 Cf. the Oversight Act Section 2 second paragraph.

4 Cf. the Oversight Act Section 8 third paragraph. It is stated in the Oversight Act Section 8 fourth paragraph that the Committee can make binding decisions regarding right of access and the scope and extent of oversight. Any objections shall be included in the annual report, and it will be up to the Storting to express an opinion about the dispute, after the requested access has been granted (no suspensive effect). In 1999, the Storting adopted a plenary decision for a special procedure to apply for disputes about access to National Intelligence Service documents. The decision did not lead to any amendments being made to the Act or Directive governing the Committee's oversight activities, see Document No 16 (1998–1999), Recommendation No 232 to the Storting (1998–1999) and minutes and decisions by the Storting from 15 June 1999. The Storting's 1999 decision was based on the particular sensitivity associated with some of the Norwegian Intelligence Service's sources, the identity of persons with roles in occupation preparedness and particularly sensitive information received from cooperating foreign services. In 2013, the EOS Committee asked the Storting to clarify whether the Committee's right of inspection as enshrined in the Act and Directive shall apply in full also in relation to the Norwegian Intelligence Service, or if the Storting's decision from 1999 shall be upheld. At the request of the Storting, this matter was considered in the report of the Evaluation Committee for the EOS Committee, submitted to the Storting on 29 February 2016, see Document 16 (2015–2016). When the Evaluation Committee's report was considered in 2017, the limitation on access to 'particularly sensitive information' was upheld, but without the wording of the Act being amended.

5 Cf. the Oversight Act Section 2.

6 Cf. the Oversight Act Section 3.

7 'The Storting in plenary session may, however, order the Committee to undertake specified investigations within the oversight mandate of the Committee,' cf. the Oversight Act Section 1 final paragraph second sentence.

8 Cf. the Oversight Act Section 11 second paragraph.

#### Non-statutory law

Non-statutory law is prevailing law that is not enshrined in statute law. It is created through precedent, partially through case law, but also through customary law.

#### Classified information

Information that shall be protected for security reasons pursuant to the provisions of the Security Act. This information shall be marked with a security classification, for example CONFIDENTIAL.

#### Security clearance

Decision by a security clearance authority regarding a person's presumed suitability for a specified security classification.

#### Authorisation

Decision about whether to grant a person with security clearance access to information with a specified security classification.

Below is a list of the committee members and their respective terms of office:

**Eldbjørg Løwer**, Kongsberg, chair  
1 July 2011 – 30 June 2019

**Svein Grønnern**, Oslo, deputy chair  
13 June 1996 – 30 June 2021

**Theo Koritzinsky**, Oslo  
24 May 2007 – 30 June 2019

**Håkon Haugli**, Oslo  
1 January 2014 – 30 June 2021

**Øyvind Vaksdal**, Karmøy  
1 January 2014 – 30 June 2021

**Inger Marie Sunde**, Bærum  
1 July 2014 – 30 June 2019

**Eldfrid Øfsti Øvstedal**, Trondheim  
1 July 2016 – 30 June 2021

Of the seven committee members, five have political backgrounds from different parties. The other two have professional backgrounds from the fields of law and technology. The broad composition helps to strengthen the Committee's expertise and legitimacy.

We are supported by a secretariat. At the end of 2018, the Committee Secretariat consisted of fourteen full-time employees – the head of the secretariat (who has a law degree), six legal advisers, three technological advisers, one head of security, one communications adviser and two administrative advisers.



## Overview of the Committee's activities



## 2.1 Summary – main issues in the oversight of the services

The EOS Committee's most important task is 'to ascertain whether the rights of any person are violated and to prevent such violations'. The Committee performs this task by checking whether PST's registration of persons is in accordance with the law, ensuring that the Intelligence Service does not violate the prohibition against surveillance Norwegians in Norway, and checking whether security clearance cases have been processed in a fair manner.

### The Norwegian Police Security Service (PST):

- In a high proportion of cases, PST has communicated information to the security clearance authorities verbally without documenting this in writing. This is in violation of the law.
- In one case, PST has registered information about a person's political involvement and disclosed it to a security clearance authority. This is prohibited, and the Committee criticised the service.
- PST disclosed information to a security clearance authority that a person, for whom security clearance was applied for, belonged to what PST calls an 'extreme group with a potential for violence'. However, the person did not belong to the group in question.
- The Committee criticised PST for collecting a chat log on unlawful grounds.
- PST reported two non-conformities to the Committee. One of them concerned covert video surveillance where a camera was turned off nine days after the court's permission had expired.

### The National Security Authority (NSM):

- In one complaint, NSM has not complied with the Committee's recommendation to grant the complainant access to correspondence between NSM and the Committee. The Committee finds this regrettable.
- NSM has violated a complainant's rights by putting the person through a security clearance process without justification. The initial decision was 'NO CLEARANCE', which had negative consequences for the complainant.
- The Committee has finished the project about security clearance of persons with connection to other states. The project has resulted in a Special Report to the Storting.

### The National Intelligence Service (NIS):

- The NIS was of the opinion that the service had the right to go through information originating from communication between persons in Norway, even if the information had

been unlawfully collected. The EOS Committee concluded as a matter of principle that the NIS is not permitted to go through such information. The Committee did not find that the NIS has actually done so.

- There is reason to doubt whether the service's collection of information from open sources about Norwegian persons in Norway is lawful.
- The Committee has spent a lot of time working on the consultation submission to the Ministry of Defence's proposal on the new Intelligence Service Act. The submission is enclosed as appendix 3.

### Other intelligence, surveillance or security services:

- The Committee has criticised the Office of the Auditor General of Norway for not giving people who are denied security clearance grounds for the decision.

## 2.2 Oversight activities carried out

The Committee's oversight activities can be divided into three broad categories. Firstly, we carry out local inspections of the EOS services. Secondly, we investigate and issue statements on individual cases. Such cases are often a result of issues uncovered during our inspections. Thirdly, we consider complaints from individuals.

After the amendment of the Oversight Act in 2017, the Committee is required to carry out at least 13 inspections per year.

In 2018, the Committee conducted 20 inspections and visited all entities demanded by the Oversight Act. The Police Security Service (PST) was inspected seven times, the National Intelligence Service (NIS) four times, the National Security Authority (NSM) twice and the Norwegian Defence Security Department (FSA) twice. The Army Intelligence Battalion, the Norwegian Communications Authority, the Norwegian Army Special Forces Command, Telia Norge AS and the Joint Cyber Coordination Centre were all inspected once.

The Committee can carry out most of its inspections directly in the services' electronic systems. This means that the inspections contain considerable unannounced elements. The services do not know which searches we perform in their systems until we ask questions, either verbally during an inspection or in writing afterwards. One inspection on short notice was conducted in 2018, of the PST office at Oslo Airport Gardermoen.

#### Security clearance authority

Public body authorised to decide whether or not people should be granted security clearance.

In order to ensure that the Committee's oversight is targeted and effective, the Secretariat makes thorough preparations at the services' premises. Preparation for inspections is a resource-intensive activity, and the preparations have been continuously strengthened over the past ten years. A new milestone was reached in 2018 when the Committee Secretariat's technology unit was established. See section 3.1 for more details.

The Committee raised 22 cases on its own initiative in 2018, compared with 31 in 2017. The cases raised by the Committee on its own initiative are mostly follow-up of findings made during inspections. The Committee concluded 22 cases raised on its own initiative in 2018, compared with 30 cases in 2017. The cases that were investigated in 2018 have generally been more demanding than the cases in 2017.

The Committee investigates complaints from individuals and organisations. In 2018, the Committee received 19 complaints against the EOS services, compared with 26 complaints in 2017.<sup>9</sup> Complaints that fall within the Committee's

oversight area are investigated in the service or services that the complaint concerns. The Committee has a low threshold for considering complaints.

The committee members meet for several days every month, except in July. The workload of the chair of the committee corresponds to nearly 30% of a full-time position, while the office of committee member is equivalent to nearly 20% of a full-time position. In 2018, we had 12 internal working meetings at the Committee's office, in addition to internal working meetings on site in connection with inspections. At these meetings, we discuss planned and completed inspections. The Committee also considers complaints and cases raised on the Committee's own initiative, reports to the Storting and administrative matters.

The EOS services have generally demonstrated a good understanding of our oversight. Experience shows that the oversight helps to safeguard individuals' due process protection and to create public confidence that the services operate within their statutory framework.



Eldbjørg Løwer, the chair of the EOS Committee, delivered on 10 April the annual report for 2017 to the President of the Storting, Tone Wilhelmsen Trøen.

Photo: Stortinget

<sup>9</sup> Some complaints concern more than one of the services.

A stylized world map composed of a grid of small dots, overlaid with several thin, curved white lines that suggest global connectivity or data flow. The map is rendered in a light gray tone against a darker gray background.

**3.**

## Developments and international oversight cooperation

### 3.1 The Secretariat's technology unit has been strengthened, but needs more resources

In its annual report for 2017, the Committee mentioned its plans to establish a technology unit with at least five employees. This is the size we believe the unit should be, given the current oversight requirements. In its consideration of the annual report for 2017, the Storting also emphasised how important it is for the Committee to add to its technological expertise. The allocation from the Storting for 2018 allowed us to start this work, and we have appointed the first two technological advisers to the new unit. However, this was not followed up in the Storting's budget for 2019, and it is not possible at present to augment the technology unit towards the goal of five staff.

In autumn 2018, a technical director and a senior engineer were appointed to the technology unit. Together with 0,5 full-time equivalent that was already in place, the unit now has 2.5 full-time equivalents. This is sufficient to start to provide better technical support both to the Committee and to the rest of the Secretariat. It is important that the technology unit has the necessary overview of and insight into the systems, so that the technological advisers can support the Committee before and during its inspection and help to follow up issues identified in connection with the inspections.

It will be important in the time ahead to look into how oversight can be rationalised by means of automation and other modern tools. This rationalised control will require knowledge about the services' systems as well as knowledge of good tools.

The technology unit has started a project of overall mapping and documentation of the systems used by the different services.

The technological advisers have also started networking with existing IT communities in Norway, particularly in the field of security. The technology unit gains useful knowledge through seminars and other meetings, and by talking to experts. Another goal is to make the EOS Committee better known in the expert community, so that we will attract many good applicants for future positions.

The consultation round on the new Intelligence Service Act has taken up a lot of time in late 2018. The proposal for facilitated bulk collection (digital border defence) introduces the concept of 'enhanced oversight' and points to the EOS Committee both for the near real-time oversight, which is a brand new role, and subsequent oversight, which represents a broadening of the Committee's current role.

If a comprehensive new Intelligence Service Act that includes facilitated bulk collection is introduced, the technology unit will need to be expanded to employ more than the five staff members needed at present.

The Committee's needs in connection with facilitated bulk collection and a new Intelligence Service Act are described in more detail in the Committee's consultation statement to the draft bill, see section 4.1 and appendix 3.

### 3.2 International oversight cooperation

The EOS services are increasingly engaging in international cooperation, and they are also sharing more and more data across national borders – and a lot of these data are sensitive personal data. This development brings new challenges for the oversight bodies as well. Therefore we need contact with foreign oversight colleagues in order to share experience and receive input that could help us to improve our oversight.

Since 2015, the EOS Committee has taken part in a cooperation project together with the oversight bodies of Denmark, Switzerland, Belgium and the Netherlands. In this project, the oversight bodies investigated their national services' international exchange of personal data about foreign terrorist fighters. The EOS Committee has not uncovered matters that warrant criticism of the Norwegian services, but has noted that the structure of the services' systems has made it difficult to find a full overview in one place of what information has been shared about an individual.

All meetings with foreign oversight bodies took place at an unclassified level, and the meetings were mentioned in the annual reports for the years 2015–2017.

#### Facilitated bulk collection (Digital border defence)

The gist of the proposal to introduce facilitated bulk collection is to allow the Intelligence Service to collect transboundary electronic communication between Norway and other countries. The proposal is part of the draft bill for a new Intelligence Service Act distributed for consultation in 2018.

#### Sensitive personal data

The Personal Data Act, which is based on the EU General Data Protection Regulation (GDPR), defines certain information (referred to as 'special categories' in the Act) as sensitive. This applies to information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of identifying a person, health data, information about a person's sexual orientation or sex life, and personal data relating to criminal convictions and offences.

We intend to continue to cooperate with the four oversight bodies, and hopefully others will join us in the years ahead.

On 14 November 2018, the group published a joint statement about the experience gained from the project. The statement and a press release about the statement are included as appendix 4 to this annual report. In the statement, we point out the risk that an oversight gap could occur when sharing of personal data between services is international, while oversight is limited to the national level. When a Norwegian service shares information with a partner abroad, we can see everything that happens at the Norwegian service, but our oversight stops once the information is sent out of the country.

We advocate a strengthened cooperation between oversight bodies. It would be a valuable step towards closer cooperation to minimise secrecy between oversight bodies and allow some sharing of information. Once data have been exchanged between the services, the oversight bodies could also share the same data for oversight purposes. This could reduce the risk of an oversight gap developing.

In our statement, we also point to the importance of developing new oversight methods, both legal and technological ones, to help to improve and rationalise oversight of international exchange of data.

The British oversight body IPCO has subsequently issued a public declaration in support of our joint statement.

*There are currently several initiatives under way to increase cooperation on oversight of international cooperation between services. The EOS Committee is following these initiatives.*

### 3.3 Anonymity for whistle-blowers

An article published by the online newspaper aldrimer.no on 5 March 2018 criticised the Committee on the grounds that ‘apparently there is still no framework established that makes it possible for the committee to offer source confidentiality to employees of the secret services who want to report matters that warrant criticism’. The chair of the Committee wrote in a response published on aldrimer.no on 18 April that the Committee has a duty to ensure that the identity of persons who have provided information to the EOS Committee in confidence is protected and not exposed when we examine matters in the services that may warrant criticism:

‘If a matter is reported to us, we have to assess whether and how the committee can use information from the whistle-blower without disclosing his or her identity. The committee can raise cases on its own initiative without having to give the services grounds for its investigations.’

The Committee has nevertheless had to provide information about the risk that a whistle-blower could be identified as the source of the information if the Committee initiated an investigation.

However, we will not use information from whistle-blowers who wish to remain anonymous without their consent. Neither do we reveal the identity of whistle-blowers or complainants to the Storting either.

We are also of the opinion that people who are employed by enterprises that fall within the scope of the Committee’s oversight area should be free to notify us of internal matters that might warrant criticism notwithstanding their duty of secrecy.

*The Committee is of the opinion that regulating protection of whistle-blowers in the Oversight Act and possibly also in the legal framework for the respective EOS services should be considered.*



4.

## The Committee's consultation submissions

#### 4.1 Consultation on a draft bill for a new the Intelligence Service Act

On 12 November 2018, we received the Ministry of Defence's consultation paper on the draft bill for a new the Intelligence Service Act.

It has been the EOS Committee's practice to have a high threshold for submitting consultation statements. It does not fall within the Committee's remit to take a stance on which surveillance methods (such as facilitated bulk collection) the Storting as the legislative body should permit the Intelligence Service to use. However, this draft bill directly affects the EOS Committee's oversight. Moreover, we see that this draft bill would have consequences that the Storting should be aware of before considering it.

The Committee has noted that the consultation paper consistently refers to the EOS Committee as a safeguard. It is important to underline that the EOS Committee is no guarantee that errors cannot be made in the EOS services. Our oversight is based on spot checks and is not intended as a complete review of all surveillance activities carried out by the EOS services. Nonetheless, our wide-ranging right of access probably has a strong disciplinary and thus also preventive effect.

On a general level, we would like to point out that the draft bill does not resolve important ambiguities relating to the Intelligence Service's surveillance of persons in Norway. Moreover, several of the Committee's critical remarks have been incorporated in the draft bill as exceptions from the prohibition against surveillance of persons in Norway. The consequence will be that the Intelligence Service will be granted extended powers in Norway.

We would also like to draw attention to the proposal that the NIS's intention should be the factor determining the service's possibility to collect information about persons in Norway. Firstly, this criterion is unsuitable for oversight. Secondly, the criterion seems to obscure the fact that the Intelligence Service can use methods against person in Norway – as long as the 'intention' is to target persons or circumstances outside Norway.

The consultation paper proposes two amendments to the Oversight Act. In our opinion, the proposed amendments create a need to clarify their consequences for the

Committee's activities.

The Committee is also of the opinion that if facilitated bulk collection is introduced, the Secretariat should be strengthened by more than the four positions proposed by the Ministry of Defence.

The consultation submission is enclosed as appendix 3 to this report.

#### 4.2 Consultation on draft regulations to the Security Act

On 2 July 2018, we received the Ministry of Defence's consultation paper on the draft regulations to a new Security Act. The Ministry proposes new regulations on the roles and responsibilities of the authorities in the field of national security, on the protective security work of enterprises, and on security clearance of suppliers and personnel.

The Committee submitted its consultation statement on 6 September 2018. The Committee requested the Ministry to consider whether the due process guarantees that apply in security clearance cases should also apply to decisions to grant authorisation for RESTRICTED. We referred to the fact that negative decisions regarding security clearance and authorisation can affect a person's career. The Committee has raised this issue before.<sup>10</sup>

#### 4.3 Consultation on the application of the Security Act for the Storting's external bodies

The Storting will consider how the new Act relating to National Security is to be applied to the Storting's external bodies and requested feedback from the EOS Committee, among others.

The Committee submitted its consultation statement on 31 January 2019. The Committee took a positive view of the Security Act being made applicable to our activities. We stated that constitutional considerations give grounds for exempting us from certain provisions of the Security Act, and proposed a regulation corresponding to the provisions set out for the application of the Security Act in relation to the Storting's administration. The Committee also has views on which security clearance authority should handle the security clearance cases of committee members and secretariat employees.

<sup>10</sup> The issue was first mentioned in the Committee's annual report for 2005, Document no 20 (2005–2006), page 13. The follow-up of this was described in the annual reports for 2011 and 2012 (Document 7:1 (2011–2012) chapter V section 3 and Document 7:1 (2012–2013) chapter V section 3, respectively).

#### RESTRICTED

A business, organization or a government body must classify and label information it produces if it can damage national security interests if unauthorized persons get access to it. RESTRICTED is the lowest level, and one needs authorization to get access to RESTRICTED information. To access information that is classified CONFIDENTIAL, SECRET or TOP SECRET one requires security clearance.



5.

## The Norwegian Police Security Service (PST)

## 5.1 General information about the oversight

In 2018, the Committee conducted four inspections of the PST Headquarters (DSE). The Committee also inspected the PST entities in Agder and Innlandet police districts and the PST office at Oslo Airport Gardermoen. We have followed up the inspection of the PST office at Oslo Airport Gardermoen, but the case was not concluded in 2018.

The Committee has also inspected PST in its role as a party to the Joint Cyber Coordination Centre (FCKS).

In our inspections of the service, we focus on the following:

- The service's collection and processing of personal data.
- The service's new and concluded [prevention cases](#) and [investigation cases](#).
- The service's use of covert coercive measures (for example telephone and audio surveillance, [equipment interference](#) and secret searches).
- The service's exchange of information with foreign and domestic partners.

The Committee's inspections consist of a briefing part and an inspection part. PST's briefings are useful in giving us insight into the service's view on its responsibilities, assessments and challenges. The Committee mostly selects the topics of the briefings, but the service is also asked to brief us on any other matters it deems relevant to the Committee's oversight. Broad insight into the service's activities enables us to conduct more focused inspections. During the inspections, we are briefed about PST's ongoing activities, the service's national and international cooperation and cases that have triggered public debate, among other things. The Committee asks verbal questions during the briefings and sends written questions, if any, afterwards.

During the inspection part, we conduct searches directly in the service's electronic systems. PST is not informed about what we search for. This means that the inspections contain considerable unannounced elements. The Secretariat makes thorough preparations for our inspections which enable us to conduct more targeted inspections.

## 5.2 PST's disclosure of information in security clearance cases

### 5.2.1 Introduction

The purpose of security clearance is to assess whether persons are fit to process classified information. When a person is considered for security clearance, the security clearance authority can obtain information about the person in question from many public registers to use in its assessment of his or her suitability for security clearance. This is called vetting. PST is one of the sources from which information is obtained.

The Committee regularly checks what information PST is disclosing to security clearance authorities in security clearance cases.<sup>11</sup> Findings made during inspections of PST, NSM and the FSA in 2017 and 2018 gave grounds for a more thorough investigation of what information PST is communicating to the security clearance authority. We have also investigated in which form information is disclosed and whether it is sufficiently well documented what information has been disclosed.

We have reviewed the information disclosed by PST about just under 20 persons from 2015 to 2017.<sup>12</sup> We have also investigated what information PST has registered about these persons in the service's systems and registers, and how the security clearance authorities have processed the information in the security clearance case.

### 5.2.2 How PST discloses information – use of meetings and inadequate documentation

The Security Act 1998<sup>13</sup> states that PST is obliged to disclose registered information to the security clearance authority, notwithstanding their duty of secrecy. The information must be communicated in writing.<sup>14</sup>

The Committee asked PST several questions about disclosure in writing, the use of meetings and documentation of what was disclosed. PST stated in its reply that the service '... as a rule [discloses] information in writing, and in some cases, further information has been provided in a meeting with the security clearance authority'.

In the Committee's opinion, the service has established a practice whereby meetings are held with the security clearance authority as a matter of routine if the service has 'more details than it has included in the letter or the specialist section wishes to clarify the information disclosed'.<sup>15</sup> The

#### Prevention case

Case opened for the purpose of investigating whether someone is preparing to commit a criminal offence that PST is tasked with preventing.

#### Investigation case

Case opened for the purpose of investigating whether a criminal offence that falls within PST's area of responsibility has taken place.

#### Equipment interference

A method that involves taking control over a mobile phone/computer through a cyberattack. The method, which entails monitoring all activity on the device in question, can be used by PST subject to court approval.

Committee referred to the fact that several of the written disclosures from PST to the security clearance authority concludes with 'for further information, please contact PST'.

PST met with the security clearance authority in about half of the cases that the Committee looked at. This probably means that disclosure of information at meetings is far more common than described by the service in its reply to us.

We are of the opinion that there are good reasons why vetting information should be disclosed in writing.

Firstly, considerations for the correct and complete communication of vetting information is an argument for disclosing it in writing. Information received from PST will normally be particularly relevant and carry great weight in a security clearance case. The party disclosing the information is best placed to record it correctly.<sup>16</sup>

Secondly, information should be disclosed in writing out of consideration for verifiability. Failure to provide information disclosed by PST in writing makes it difficult for the appellate body, for any special advocates<sup>17</sup> and for the EOS Committee to check what information the security clearance authority has had access to and based its decision on. In some cases, the person for whom security clearance has been applied for is not entitled to be given grounds for the decision.<sup>18</sup> This applies, for example, to information from PST. It is particularly important that it is possible to review all aspects of the case because the person in question will not be informed that the denial is fully or partly based on information received from PST.

PST has stated that it would have been an advantage if the service gave more information to the security clearance authority in writing in individual cases. PST also stated that documentation of what vetting information was disclosed at meetings has not been satisfactory. The service has tightened up its practice.

We share the service's view and expect PST to mainly

disclose information to security clearance authorities in writing from now on. Written disclosure of information will reduce the need for meetings between PST and the security clearance authorities. The Committee expects PST to ensure satisfactory documentation of information disclosed in any cases where meetings are required.<sup>19</sup>

*The Committee criticised PST on the grounds that the service's practice for the disclosure of vetting information did not comply with the statutory requirement for information to be communicated in writing.*

### **5.2.3 Can PST withhold relevant information?**

PST did not answer the Committee's question about whether the service has legal authority for withholding information of relevance in a security clearance case from the security clearance authority.

On a general basis, the service nevertheless expressed the view that it must assess on a case-to-case basis what information can be disclosed. PST stated that considerations for the service's activities, operational considerations, considerations for ongoing investigations and protection of sources and third-party information must be taken into account, while the security clearance authority must receive adequate information.

We expressed our understanding of such considerations. However, the Committee remarked that we find it difficult to see how the Security Act's provisions on vetting allows PST to carry out its own assessment of whether to disclose information as long as it is relevant for vetting purposes. The Committee stated that it should be clearly regulated how considerations for PST's performance of its duties can be weighed against disclosure of negative information about persons for whom security clearance is applied for.

*The Committee stated that exemptions from the duty to disclose information should be regulated in the Security Act or Regulations to the Security Act.*

11 The Committee commented on PST's disclosure of information to security clearance authorities in its reports to the Storting for 1998, p. 11, and 2001 p. 7.  
 12 The selection criteria included whether a final decision had been made in the security clearance case and whether the documents in the case were available in the case processing system for security clearance cases (Mimir).  
 13 Act No 10 of 20 March 1998 relating to Protective Security Services (the Security Act 1998) Section 20 fourth paragraph. The Security Act 1998 was repealed with effect from 1 January 2019 – the day on which the Act of 1 June 2018 relating to National Security (the Security Act) came into force.  
 14 The requirement for information to be disclosed in writing follows from the Security Act 1998 Section 20 fourth paragraph and the Police Register Regulations Section 11-3 first paragraph, cf. the Police Register Act Section 30 and the Police Register Regulations Section 9-6 first paragraph (11).  
 15 This is stated in PST's memo presented to the Committee during the inspection of the PST Headquarters in December 2017.  
 16 This is also expressed in NSM's guidelines, which advise that if information received verbally is to be used in the processing of security clearance cases, 'the security clearance authority must request (...) written confirmation', cf. NSM's guide to the Security Act 1998 Chapter 6 and the Regulations concerning Personnel Security, from the guidelines on Section 20.  
 17 It follows from the Security Act 1998 Section 25b second paragraph that security clearance cases where no grounds are given can, subject to certain conditions, be forwarded to a lawyer appointed as a special advocate for advice on whether the person should appeal the decision. The lawyer will be given access to the facts of the case and the grounds that are unknown to the person assessed for security clearance. The lawyer cannot represent the person in an appeal case.  
 18 Cf. the Security Act 1998 Section 25 third paragraph.  
 19 Cf. the Police Register Regulations Section 11-4 second paragraph.

The Committee notes that it has been included in Section 12 of the Clearance Regulations,<sup>20</sup> which came into force on 1 January 2019, that the police and PST shall enter into an agreement with NSM concerning disclosure by the police and PST of information obtained from intelligence registers for use in security clearance cases. This provision is intended to take into account considerations for the operational and preventive needs of the police and PST on the one hand and of NSM and the security clearance authorities on the other. Disagreement concerning the use and disclosure of information shall be decided by the Ministry of Justice and Public Security.

The Committee in any case expects PST to inform the clearance authority that PST *has* information of relevance to a security clearance case that the service will not disclose. If not, no disagreement regarding whether information *shall* be disclosed, can surface.

#### 5.2.4 Disclosure of unconfirmed information

Before PST discloses information in connection with vetting, the service must check the quality of the information and describe any uncertainty as to its accuracy.<sup>21</sup>

PST informed the Committee that the service's concerns regarding a person will often be based on unconfirmed information. The service's registers are not registers of facts in the same way as the registers of criminal cases or the National Registry.

The Committee stated that PST has in some cases not been clear enough about uncertain information. Information provided to the security clearance authority can appear to be first-hand information from PST ('PST is aware of...'), while PST has in reality received the information from a contact or source, and the service has no way of confirming the information.

The security clearance authorities shall seek to ensure that security clearance cases are as well-informed as possible. Information from PST will usually be a weighty argument in a security clearance case, while the security clearance authorities themselves are rarely in a position to verify or disprove the information. For example, the security clearance authority cannot necessarily confront the person in question with information received from PST in a security interview.

*The Committee stated that it is particularly important that PST makes clear any uncertainty associated with the information.*



#### Security interview

Interview conducted by the security clearance authority in order to assess a person's suitability in a security clearance case.

### 5.2.5 Conclusions and follow-up

The responsibilities of the Committee include to ascertain whether the rights of any person are violated and to prevent such violations and to ensure that the services act in accordance with statutory and regulatory requirements.<sup>22</sup> Our investigation showed that PST's practice for disclosure of information to security clearance authorities does not comply with the applicable requirements. The service's practice also entails a risk of violation of the rights of persons for whom security clearance is applied for. A negative security clearance decision can have a significant impact on a person's career.

*This case has illustrated the value of the Norwegian system of having one committee to oversee all the services, which allows the Committee to consider both the division of work and the sharing of information between services.*

We have noted that PST has changed its practice and revised the procedure for disclosing information to the security clearance authorities, and that PST and NSM will draw up a new cooperation agreement.

*The Committee will keep informed about the measures the service implements to follow up this matter and continue its oversight of PST's disclosure of information to the security clearance authorities.*

## 5.3 PST's disclosure of information to the security clearance authorities in three cases

### 5.3.1 Background

As explained in section 5.2, the Committee has looked into PST's disclosure of information to security clearance authorities and commented on three specific cases following its investigation. In one of these cases, the outcome was that security clearance was denied. The Committee has no reason to believe that shortcomings in PST's disclosure has had a bearing on the outcomes of these cases.

### 5.3.2 Case 1 – Inadequate documentation of information disclosed

In one case, PST's notes to a meeting with the security clearance authority stated that a briefing about intelligence by a foreign state would be given. That PST was concerned that the person in question might have links to foreign intelligence did not emerge, neither from the written disclosure

before the meeting nor from the minutes of the meeting.

When asked by the Committee what information was shared at the meeting, PST responded that the service was concerned that the person for whom security clearance was applied for might be an intelligence officer or otherwise cooperated with the authorities of a specific state.

*The Committee stated that the disclosure in this case illustrates the problematic aspects of PST's practice as discussed in section 5.2 above. It was not documented what information had been disclosed. We were also of the opinion that PST's disclosure could give the impression that the service vouched for the truth of the information in the letter, even though PST had not confirmed the information.*

### 5.3.3 Case 2 – Unlawful disclosure of information about political involvement

Political involvement, including membership of, sympathy with or active support of lawful political parties or organisations or other lawful social involvement, shall not be of significance for the assessment of a person's suitability with respect to security, cf. the Security Act Section 21 second paragraph.

In one case, PST had registered information about a person's political involvement and shared this information with the security clearance authority. In connection with follow-up, PST stated that the statement falls within the scope of freedom of expression. PST informed the Committee that there was no basis for processing the information about the person and that the registered information was therefore deleted.

We agreed with PST's assessment of the registration, and added that the statement does not exceed the limits of lawful political activity or other lawful social involvement.

*The Committee criticised PST for having disclosed information about political involvement to the security clearance authority in breach of the prohibition set out in the Security Act Section 20 fifth paragraph.<sup>23</sup>*

### 5.3.4 Case 3 – Disclosure of incorrect information

PST disclosed information to a security clearance authority that the person for whom security clearance was applied for was a member of an organisation that PST described as an extreme group with a potential for violence. Our investigation of the registration of this person in PST's register *Smart*

20 Regulations No 2054 of 20 December 2018 regarding security clearance and other clearances (the Clearance Regulations).

21 Cf. the Regulations concerning Personnel Security Section 3-4 fourth paragraph. This is also regulated in the Police Register Act, where Section 67 third paragraph refers to Section 20, which contains special provisions and the requirement for information to be communicated in writing for disclosure of non-verified information.

22 Cf. the Oversight Act Section 2 first paragraph.

23 Cf. the Security Act 1998 Section 21 second paragraph.

showed that the working hypothesis was not supported by information.

PST stated that they had initially received information indicating that the person was a member of the organisation, but that more recent information had shown this to be incorrect. By mistake, the working hypothesis of membership was not deleted, and the incorrect information was subsequently disclosed to the security clearance authority.

Because of the Committee's questions, PST has deleted the working hypothesis and notified the security clearance authority that incorrect information was disclosed about the person in question. In order to prevent similar occurrences in future, the department in PST that discloses vetting information will be notified when it is discovered that incorrect information is registered about a person the service has disclosed information about.

*The Committee emphasised how important it is for PST to check that information is correct before disclosing it to the security clearance authority.<sup>24</sup> The Committee takes note of the measures that PST has implemented.*

#### 5.4 For how long can PST store information before an assessment of necessity must be carried out?

Information processed by the police and PST shall not be stored for longer than 'necessary for the purpose of the processing'.<sup>25</sup>

In the annual report for 2017,<sup>26</sup> the Committee wrote that we have questioned in several cases whether it is necessary to continue to store information about persons in the intelligence register Smart. PST has argued on a general basis that information registered in the intelligence register can be stored for five years before PST has to assess whether the intelligence registrations are still relevant and necessary to the service. The service has referred to what is known as the five-year rule in the Police Register Regulations Section 22-3 third paragraph. At the same time, PST has pointed out that the necessity and relevance of an intelligence registration is to be reassessed when new information about a registered person is entered in the intelligence register Smart.

The Committee stated in 2017 that intelligence registrations should be reviewed regularly by the person responsible for

having registered the information. The purpose of this is to ensure that the intelligence register contains up-to-date, correct, necessary and relevant information.

PST disagrees with the Committee that intelligence registrations must be reviewed more often than every five years. We therefore raised the matter with the Ministry of Justice and Public Security.

In a letter to the Committee in 2018, the Ministry referred to the different time intervals stipulated in the Police Register Regulations for reviewing information in different registers. These provisions were set because it is not considered possible to carry out continuous assessments of whether the necessity requirement is met. The length of the intervals is based on a concrete assessment of how long it is deemed justifiable to process information for without making a new concrete assessment of its necessity. The Ministry had no objections to PST's outlined practice.

*The Committee will base its future oversight work on the Ministry's understanding.*

#### 5.5 PST's collection of chat logs

The Committee considered a case in 2018 that illustrates how new ways of communicating challenge the traditional distinction between verbal and written communication. Pursuant to the Criminal Procedure Act Section 216 I, PST can, subject to certain conditions, 'use technological devices to listen in to or make recordings of telephone conversations or other conversations with the suspected person if the police either take part in the conversation themselves or have received the consent of one of the parties to the conversation'.

PST carried out an assessment and concluded that the Criminal Procedure Act Section 216 I provided legal authority for collecting a chat log.

An online chat is similar to a conversation in form, but takes place in writing. The Committee therefore asked PST whether a chat can be considered a 'conversation' in the sense of the Criminal Procedure Act Section 216 I.

PST answered that the natural understanding of the wording of the provision indicated that written conversations via the internet and telephone apps such as Snapchat, Instagram and Messenger are covered by the term 'conversation' in the

##### The five-year rule

The requirement for PST's intelligence registrations to be re-evaluated if no new information has been added during the past five years.

##### Intelligence registration

Processing of information that is deemed necessary and relevant for PST in the performance of its duties, and that does not warrant opening of or processing in a prevention case.

Criminal Procedure Act Section 216 I. The service referred to the fact that the word 'chat' is used to describe a form of communication between verbal and written communication, and that the Norwegian dictionary *Bokmålsordboken* defines it as talking online, from the English word chat meaning 'talk, converse'; a conversation taking place via the internet using a computer keyboard. PST was of the opinion that this supported the understanding that conversations are not exclusively verbal, but that written communication via the internet contains a strong verbal element. PST also referred to the preparatory works to the Act:

'The conversations listened in to or recorded can be telephone conversations or other conversations. (...) A broad interpretation of "conversation" shall apply. The crucial thing is whether the parties are communicating verbally. If one party does most of or all of the talking, that does not alter the situation'.<sup>27</sup>

PST referred to the fact that this was written about 20 years ago, when the communication platforms we have today did not exist. PST summarised its interpretation of the provision as follows:

'It is therefore PST's opinion, with reference to ordinary source of law principles, that considerable importance should be attached to society's natural understanding

of the wording. PST therefore believes that the Criminal Procedure Act Section 216 I should be applicable to conversations in the form of online conversations/chats when the other conditions stipulated in the provision are met.'

The service otherwise referred to the fact that the method represented a modest interference in relation to the person concerned, who was already subject to other surveillance approved by the district court.

In its concluding statement to PST, the Committee expressed a view on the scope of Section 216 I of the Criminal Procedure Act that differs from PST's view. PST is right that in everyday language, 'conversation' is also used about online 'chatting', so that the once clear distinction between the verbal and the written has become blurred.

Being able to communicate with others in confidence is such a valuable right that it is protected both in the Norwegian Constitution and in the European Convention on Human Rights (ECHR). The Norwegian Constitution Article 102 states that everyone is entitled to respect for their communication, while ECHR Article 8 gives everyone the right to respect for their correspondence. In principle, the authorities can only depart from this if they have a basis in law.

Despite the fact that a broad interpretation of the word



24 This is required by the Regulations concerning Personnel Security Section 3-4 fourth paragraph.

25 Cf. Regulations No 1097 of 20 September 2013 regarding Processing of Information by the Police and Prosecuting Authority (the Police Register Regulations) Section 22-3 first paragraph first sentence, cf. the Police Register Act Section 6 first paragraph (3).

26 Cf. Document 7:1 (2017–2018) *The EOS Committee's annual report for 2017*, section 5.4.

27 See Proposition No 64 to the Odelsting (1998–99), page 163.

‘conversation’ in the Criminal Procedure Act Section 216 I should apply, the preparatory works to the act establish that the crucial thing is whether the parties communicate ‘verbally’. In the Committee’s opinion, the provision cannot be interpreted in a wider sense with reference to society’s understanding of the word ‘conversation’.

The fact that PST cannot, in our opinion, use the Criminal Procedure Act Section 216 I as a basis for accessing a chat log does not mean that PST is prevented from collecting chat logs. Subject to certain conditions, the service is permitted to use ‘audio surveillance of conversations or other communications conducted to or from specific telephones, computers or other apparatus (...)’ pursuant to the Criminal Procedure Act Section 216 a. Surveillance under this provision requires a court decision, while the prosecuting authority can make decisions concerning audio surveillance under the Criminal Procedure Act Section 216 I. By using Section 216 I as a basis for collecting chat logs, PST can withhold this collection from statutory court control, which will weaken individuals’ due process protection.

*The Committee has criticised PST and urged the service to change its practice.*

PST later made it clear that the provision in question has only been used to collect chat logs in this one instance. PST underlined that the use of this provision was based on the service’s interpretation of the law and not motivated by a wish to evade court control.

*PST has confirmed to the Committee that the service will comply with the EOS Committee’s request and refrain from using the Criminal Procedure Act Section 216 I to collect chat logs in the future. The Committee is satisfied with this result.*

## 5.6 Non-conformity reports – PST’s use of coercive measures

In our annual report for 2017, we wrote that PST had, on its own initiative, informed us of a non-conformity relating to the service’s use of covert video surveillance. In 2018, the

Committee has been informed about PST’s follow-up of the non-conformity and changes in procedures following this error.

The Committee has in 2018 been informed of two more non-conformities in the service’s use of coercive measures. One non-conformity concerned the service’s lawful interception, which was not discontinued when the subscription was no longer in use. The second non-conformity concerned camera surveillance that was not discontinued when the court permission expired. The camera was turned off when the mistake was discovered nine days later. No recordings were made during these nine days.

We have been informed about how the service has followed up these non-conformities. The information has not given grounds for follow-up on our part.

*The Committee takes a positive view of the fact that PST reports on non-conformities to the Committee during its inspections. We assume that PST takes the non-conformities seriously and reviews its procedures to prevent recurrence of errors.*

## 5.7 Complaint cases considered by the Committee

The Committee received 6 complaints against PST in 2018, compared with 12 complaints in 2017. Some of these complaints were against several of the EOS services.

The Committee’s statements to complainants shall be unclassified. Information concerning whether or not a person has been subjected to surveillance shall be regarded as classified unless otherwise decided. This means that, in principle, a complainant cannot be told whether he or she is under surveillance by PST. The Oversight Act dictates that statements in response to complaints against the services concerning surveillance activities shall only state whether or not the complaint contained valid grounds for criticism.<sup>28</sup>

The Committee concluded 4 complaint cases against PST in 2018. No complaint cases concluded in 2018 has resulted in criticism of PST.

<sup>28</sup> Cf. the Oversight Act Section 15 first paragraph: ‘Statements to complainants should be as complete as possible without disclosing classified information. Information concerning whether or not a person has been subjected to surveillance activities shall be regarded as classified unless otherwise decided. Statements in response to complaints against the services concerning surveillance activities shall only state whether or not the complaint contained valid grounds for criticism. If the Committee holds the view that a complainant should be given a more detailed explanation, it shall propose this to the service or ministry concerned.’

### Lawful interception

A method that monitors a person’s communication – for example telephone surveillance or monitoring of meta-data about telephone and computer communication. PST can use this method subject to court approval.

6.

# The National Security Authority (NSM)

## 6.1 General information about the oversight

The Committee carried out two inspections of NSM in 2018, including one of NSM NorCERT. NSM NorCERT is Norway's national centre that has a coordinating role in preventative work and responses against IT security breaches aimed at vital infrastructure in Norway.<sup>29</sup> The Committee has also inspected NSM in its role as a party to the Joint Cyber Coordination Centre (FCKS).

NSM is a directorate and attends to the general functions in the protective security services pursuant to the Security Act. NSM is the security clearance authority for its own personnel in addition to being the appellate body for clearance decisions made by other security clearance authorities.

In our inspections of the service, we focus on the following:

- NSM's processing of cases where security clearance has been denied, reduced or suspended by the security clearance authority, and its processing of complaints in such cases.
- NSM's cooperation with other EOS services.
- NSM NorCERT's information processing.

During the inspections, we are routinely briefed about NSM's ongoing activities, including its cooperation cases with other EOS services and case processing times in security clearance cases. During the inspections, the Committee conducts searches directly in NSM's electronic systems. The Committee mostly selects the topics of the briefings, but the service is also asked to brief us on any other matters it deems relevant to the Committee's oversight. The Committee asks verbal questions during the briefings and sends written questions, if any, afterwards.

The function of the security clearance authority is to assess the reliability, loyalty and sound judgement of a person and determine whether he or she is fit to process classified information.<sup>30</sup> A security clearance decision can be decisive for a person's career, and strict requirements must therefore apply to the processing of such cases. The Committee maintains a particular focus on such cases for this reason, and because the processing of security clearance cases is a more closed process than case processing in relation to other administrative decisions.

## 6.2 Special report to the Storting on differing practices in the security clearance of persons with connections to other states

The Special report was delivered to the President of the Storting on 12 March.

The EOS Committee has reviewed security clearance cases where the person for whom security clearance is requested or their closely related persons have a connection to states other than Norway. We have identified several matters that warrant criticism. The National Security Authority (NSM) is the expert authority on for these matters. One of the main goals of this project has been to assess whether similar cases are treated in the same way.

- The Committee's investigation has uncovered unwarranted differential treatment of cases concerning security clearance cases of persons who are citizens both of Norway and of a foreign country. There were differences in both case processing and outcomes. Some persons with a connection to a country were denied security clearance despite other persons with a comparable connection to the same country being granted clearance.
- The investigation showed that several of the cases were not sufficiently well-informed and that the persons' connection to Norway had not been sufficiently well assessed.
- The Committee has concluded that the rights of individuals have been violated, cf. the Oversight Act Section 2.

The majority of the security clearance cases included in this investigation, were processed by the Norwegian Defence Security Department (FSA), the Norwegian Police Security Service (PST) and the Norwegian Intelligence Service (NIS). These security clearance authorities process a great number of cases. The Committee has no opinion about what the outcomes of the cases in questions should have been. Our concern is to ensure that all security clearance authorities process and assess cases with similar facts in a uniform manner. Variations between security clearance authorities in terms of case processing and outcomes is detrimental to the due process protection of the persons for whom security clearance is applied for.

The investigation of eight cases where persons were denied security clearance showed that six of them were denied clearance without the case having been sufficiently well-informed. These cases were decided by the FSA. The FSA has informed us that these negative security clearance decisions will be reconsidered.

### Protective security services

Planning, facilitating, implementing and overseeing protective security measures that aim to eliminate or reduce risks resulting from activity that poses a threat to security.

The Committee's investigation also uncovered unwarranted differential treatment in security clearance cases where there was insufficient information about the personal history of the spouse of the person concerned. Several cases were decided based on the assumption that the personal history requirement did not apply to the spouse, and security clearance was therefore granted, while NSM denied security clearance in comparable cases.

The reply received from NSM in this case supports the Committee's conclusions. NSM acknowledges that there is disproportionate and unwarranted variation in case processing as well as decisions in the cases that the Committee referred to. NSM pointed out as possible reasons that no traceable overview of practice exists, and that the security interview capacity situation is challenging.

Over several years, the Committee has emphasised the importance of NSM, as the expert authority for security clearance cases, putting in place an archive of experience and other tools to ensure that similar cases are treated in the same way. It is very important that NSM establishes solutions to ensure uniform practice. The Committee notes that such measures have not yet been implemented.

## 6.3 Complaint cases considered by the Committee

### 6.3.1 Introduction

The Committee received 11 complaints against NSM in 2018, compared with 3 complaints in 2017. Ten of the complaints concerned security clearance cases.

A decision in a security clearance case can be of vital importance to a person's life situation and future career. It is therefore essential that the security clearance authorities consider these cases in a fair manner that safeguards due process protection. In cases where the Committee expresses criticism, the complainant is given the reason for the Committee's decision.

The Committee concluded eight complaints against decisions to deny security clearance in 2018. Of the cases that we concluded in 2018, the following cases gave grounds for critical statements by the Committee:

### 6.3.2 Complaint case 1 – Person with no need for security clearance

In one complaint case, the complainant asked the Committee to investigate whether a security clearance was even necessary. The Committee asked the requesting authority (the employer) to document and give grounds for the need for security clearance for the position in question.<sup>31</sup> The employer's reply prompted us to ask further questions, and the statements made by the employer to the Committee were forwarded to NSM for assessment.

NSM concluded that the need for security clearance was not adequately documented. The inadequate documentation constituted a case processing error that made the NO CLEARANCE decision invalid.

*NSM should have dismissed the request for security clearance.*

When we concluded the case, we endorsed the directorate's assessment that the decision was invalid. There was no legal basis for a security clearance process in relation to the complainant. We also stated:

'The security clearance case without a legal basis has had actual negative consequences for [the complainant]. The Committee emphasises that a decision in a security clearance case can be of vital importance to a person's life situation and future career.

The Committee also remarks that a security clearance process without a legal basis is a clear interference with an individual's protection of privacy. The Committee has noted that information from the security clearance process is anonymised and access to it restricted.

It warrants strong criticism that the security clearance authority implemented an intrusive measure without there being a real need for security clearance.'

*The Committee is of the opinion that NSM have violated the complainant's rights in a manner that warrants strong criticism, cf. the Oversight Act Section 2 first paragraph (1) and (3).*

The Committee described a similar complaint in its annual report for 2017. We opened a case to consider general

29 NSM NorCERT (Norwegian Computer Emergency Response Team). NSM NorCERT is a function attended to by NSM's Department for ICT Security.

30 Cf. the Security Act 1998 Section 21 first paragraph.

31 Cf. the Security Act 1998 Section 19 and the Regulations concerning Personnel Security Section 3-1.

#### Requesting authority

A body that requests security clearance of personnel.

issues relating to documentation and grounds for a need for security clearance. This case is still under consideration by the Committee.

### 6.3.3 Complaint case 2 – inadequate access to information in a case where the Committee disagrees with the grounds given by NSM

In our annual report for 2017,<sup>32</sup> we discussed a case concerning revocation of security clearance that involved where to draw the line between disciplinary matters and security clearance cases. In the same case, the person concerned requested access to the correspondence between the EOS Committee and NSM. We therefore requested NSM to consider whether access could be granted.

NSM concluded that access to the information could be granted to the Committee's letter to NSM in its entirety, but exempted from access several paragraphs in some of NSM's letters to the Committee. The grounds given for denying access was that the paragraphs in question 'reflect NSM's work methods and assessments'. NSM was of the opinion that these paragraphs contain sensitive information that must remain classified pursuant to the Security Act Section 11.<sup>33</sup>

The Committee remarked to NSM that it was unclear which work methods and assessments are classified in this concrete case. We found it difficult to see a basis for exempting information in the paragraphs in question from access, as they contain descriptions of facts and regulations, legal and security assessments and a reproduction of the Committee's statements. Nor could we see how the information exempted from access in the case documents is classified; i.e. how it could harm the national security of Norway or our allies, relations with foreign powers or other vital national security interests if the person in question was given access to the information.

We therefore asked NSM to explain which work methods and assessments, if any, are classified. The authority was also requested to give grounds for this and be specific about why giving the person whom this case concerns access to the relevant paragraphs in these documents could harm national security.

After receiving a reply from NSM that it was still of the opinion that the information exempt from access should be classified, we made the following concluding statement:

'The Security Act Section 11 third paragraph second sentence states "Security classification shall not be carried out to a greater extent than is strictly necessary, and the

security classification used shall be no higher than necessary". This provision defines a duty to assess the value of information as regards whether it is classified and, if so, which security classification applies. If exemption from access is based on information being classified without a legal basis for classification, this will be in breach of the Security Act Section 11.

The Committee notes that NSM maintains that the information exempt from access should be classified "based on the considerable potential negative consequences for national security interests if the information is collated and used to manipulate future security clearance cases".

On a general basis, the Committee can agree that collation of detailed security assessments and methods could harm national security interests if they become known to unauthorised parties. However, we still found it difficult to see how all the information in the exempted paragraphs reflects NSM's security assessments or the methods used by the service, and thus contains classified information pursuant to Section 11 of the Security Act 1998.

We also referred to Official Norwegian Report NOU 2016:19 Chapter 8.2.1<sup>34</sup> on information security, which states that '[t]he threshold for classifying information must be such that the information has a certain potential for harm'.

It was not clear to us that all the information exempted is of such a nature that it has a certain potential for harm.

*The Committee finds it regrettable that the person in question was not granted full access to correspondence between NSM and the Committee in the case.*

### 6.3.4 Complaint case 3 – Inadequate grounds and information to the complainant and inadequate documentation

The Committee asked NSM about the processing of a complaint concerning a decision to deny security clearance. The body that made the initial decision has emphasised several factors mentioned in the Security Act 1998 Section 21 first paragraph:

- criminal acts (letter b),
- factors that may make person concerned susceptible to pressure (c),
- misrepresentation of or failure to present facts (d),
- failure to keep the person responsible for authorisation currently informed about personal matters (g), and
- other matters related to the complainant's manner and characteristics (l).

#### Internal grounds (ISB)

An internal document that security clearance authorities are obliged to prepare in connection with security clearance decisions. This document must deal with all the material factors in the case, including the provisions on which the decision is based, the matters to which importance has been attached pursuant to Section 21 of the Security Act, and which facts the decision is based on.

NSM's internal grounds (ISB) did not show how NSM had considered the above-mentioned factors when considering the appeal.

In a reply to us, NSM wrote that it had not considered all the factors that the body that made the initial decision had attached importance to. In NSM's opinion, the importance that the body that made the initial decision attached to criminal acts, basis for pressure and the complainant's characteristics or demeanour had no bearing on the outcome. Other factors provided sufficient grounds for denying security clearance. NSM admitted that this ought to have been described in the internal case documents and in the information communicated to the complainant.

It is very important to the complainant's due process protection and the Committee's opportunity to conduct subsequent oversight that the assessments made by the security clearance authority are described in the case documents.

*The Committee criticised NSM for inadequate written documentation in the case.*

NSM also failed to inform the complainant that it had not considered all the factors in the case. The body that made the initial decision had emphasised factors of a personal and highly sensitive nature in its assessment of the complainant. Among other things, it had attached importance to the fact that the complainant had been reported to the police for serious criminal acts, despite the fact that the case was dropped because no criminal offence had been proven.

*The Committee criticised NSM for not making it clear to the complainant that the sensitive circumstances were not part of the grounds for the decision to deny security clearance. It warrants criticism in itself that inadequate grounds were given, and the serious subject of assessment intensifies the Committee's criticism.<sup>32</sup>*

In its reply to us, NSM apologised for its decision appearing incomplete and being likely to cause frustration and misunderstandings. The Committee endorsed NSM's view of the wording of the decision.

*It is a condition for individuals being able to safeguard their own interests that the security clearance authority provides as comprehensive grounds as possible when security clearance is denied.*

### 6.3.5 Complaint case 4 – long case processing time

In one complaint case, the Committee criticised NSM for its long case processing time. When the complaint case was forwarded to NSM from the body that made the initial decision, that body made a mistake for which NSM as the appellate body cannot be blamed. When NSM became aware of the case, one and a half years had passed since the initial security clearance decision. NSM's case processing time was another nine months. In the Committee's concluding statement to NSM, we expressed the view that, considering the circumstances, NSM should have made a decision in the case without delay. In the Committee's opinion, the case processing time was therefore unreasonably long.

## 6.4 Case processing times in security clearance cases

The Committee has for many years been following the security clearance authorities' case processing time in security clearance cases. Below is an overview of the case processing times for 2018 as provided by NSM.

NSM has informed the Committee about the work to reduce the case processing time. The Committee will continue to be informed about the case processing times in security clearance cases in 2019.

CASE PROCESSING TIME NSM 2018	Average case processing time in total	Average case processing time positive decisions	Average case processing time negative decisions
Request for access to information	49 days		
Request for security clearance	76 days	74 days	189 days
Appeal 1. instance	74 days	N/A	74 days
Appeal 2. instance	75 days	152 days	65 days

32 Annual report for 2017 section 6.4.

33 Cf. the Security Act 1998 Section 25a second paragraph first sentence, cf. Section 25 third paragraph.

34 Official Norwegian Report NOU 2016:19 Chapter 8.2.1 page 150.

35 The requirement for grounds to be given follows from the Security Act Section 25 and NSM's guide to the Security Act Chapter 6 and the Regulations concerning Personnel Security, guidelines to Section 25.

7.

## The Norwegian Defence Security Department (FSA)

## 7.1 General information about the oversight

The Committee conducted two inspections of the FSA in 2018. In our inspections of the department, we focus on the following:

- The FSA's processing of cases where security clearance has been denied, reduced or suspended by the security clearance authorities.
- The FSA's protective security activities.
- The FSA's cooperation with other EOS services.

During the inspections, the Committee requests a briefing about the FSA's ongoing activities and about certain special topics of relevance to the Committee's oversight. The Committee mostly selects the topics of the briefings, but the service is also asked to brief us on any other matters it deems relevant to the Committee's oversight. The Committee asks verbal questions during the briefings and sends written questions, if any, afterwards.

The FSA's processing of security clearance cases is particularly important in the Committee's oversight of the department. The FSA is Norway's largest security clearance authority by far. With effect from 1 January 2017, the FSA became the security clearance authority for the entire defence sector, and it took over responsibility for security clearance cases from the Ministry of Defence and the Norwegian Defence Estates Agency. The Committee reviews most of the negative security clearance decisions made by the FSA, as well as appealed security clearance cases where it granted the appeal in part or in full.

We also oversee the FSA's protective security activities, carry out spot checks of investigations into activity that poses a threat to security targeting the Armed Forces (security investigations) and check operational cases that are part of the department's responsibility for military counterintelligence in Norway in peacetime. Another of our primary duties in this connection is to oversee the FSA's processing of personal data as part of its protective security activities.

The Committee received three complaints against the FSA in

2018, compared with one in 2017. These complaints were against several EOS services. We concluded two complaint cases in 2018. No complaint cases concluded in 2018 resulted in criticism of the FSA.

## 7.2 Use of vetting information for purposes other than security clearance assessments

The Committee asked the FSA whether personal data obtained in security clearance cases could be used for other purposes.

The FSA is charged with keeping an overview of the security risk situation of the Norwegian Armed Forces and Norway's military activities in Norway and abroad.<sup>36</sup> In order to prevent incidents that pose a threat to security, FSA processed information about a large number of persons affiliated to the Norwegian Armed Forces in a security investigation. An internal FSA memo from 2014 shows that the department had received the information that was to be used in the investigation in connection with vetting in security clearance cases. Pursuant to the Security Act 1998 Section 20 sixth paragraph, this information cannot be used for purposes other than such vetting. In 2018, the FSA informed the Committee that the investigation was not based on information from vetting.

*When we concluded the case, we reminded the FSA that information provided to a security clearance authority for vetting purposes shall not be used for purposes other than security clearance assessments.*

## 7.3 Case processing times in security clearance cases

The Committee has for many years been following the security clearance authorities' case processing time in security clearance cases. Below is an overview of the case processing times for 2018 as provided by FSA.

FSA has informed the Committee about the work to reduce the case processing time. The Committee will continue to be informed about the case processing times in security clearance cases in 2019.

CASE PROCESSING TIME FSA 2018	Average case processing time in total	Average case processing time positive decisions	Average case processing time negative decisions
Request for access to information	16 days		
Request for security clearance	25 days	21 days	151 days
Appeal 1. Instance	98 days	149 days	70 days

36 Cf. Instructions No 695 of 29 April 2010 for Defence Security Service Section 4 first paragraph letter e.

### Incident that poses a threat to security

Activity that poses a threat to security, sensitive information being compromised and serious security breaches.

8.

## The Norwegian Intelligence Service (NIS)

## 8.1 General information about the oversight

The Committee conducted two inspections of the NIS headquarters in 2018, in addition to inspections of the vessel Marjata and the Norwegian Armed Forces' Ringerike station at Eggemoen.

The Committee has also inspected the NIS in its role as a party to the Joint Cyber Coordination Centre (FCKS).

The oversight of the NIS focuses in particular on ensuring that the service does not violate the statutory prohibition against monitoring or in any other covert manner collecting information concerning persons on Norwegian territory.<sup>37</sup> Two other key oversight points for the Committee is to oversee that the service is subject to national control and that it complies with the Ministry of Defence's provisions regarding collection and/or sharing of information concerning Norwegian legal persons outside Norway.

The Committee is charged with ensuring that the NIS's activities are carried out within the framework of the service's established responsibilities.<sup>38</sup> The oversight is also intended to ensure that the NIS's activities do not violate the rights of any persons or unduly harm the interests of society and that the activities are kept within the framework of statute law, administrative or military directives and non-statutory law. Other important oversight points are to ascertain that the means of intervention employed do not exceed those required under the circumstances, and that the service respects human rights.<sup>39</sup>

Our oversight of the NIS shall cover the service's technical activities, including surveillance, information collection and processing of personal data. The Committee shall ensure that the cooperation and exchange of information between the NIS and domestic and foreign collaborative partners are kept within the framework of the applicable regulations, cf. the Oversight Act Section 6.

During our inspections of the NIS, we focus on the following:

- The service's technical information collection.
- The service's processing of information in its computer systems.
- The service's exchange of information with cooperating domestic and foreign services.

- Matters of particular importance or that raise questions of principle that have been submitted to the Ministry of Defence<sup>40</sup> and internal approval cases.

In connection with the inspections, the Committee requests information about the NIS's ongoing activities, including the service's cooperation cases with other EOS services, the threat situation, cases submitted to the Ministry of Defence and internal approvals. The topics of the briefings are mostly selected by the Committee, but the service is also asked to brief us on any other matters it deems relevant to the Committee's oversight. The Committee asks verbal questions during the briefings and sends written questions, if any, afterwards.

Internal approval cases can be permission to share information about Norwegian legal persons with cooperating foreign services or to do surveillance of Norwegian legal persons' communication when the persons are abroad. As the Committee has previously pointed out, the NIS is not required to obtain court permission to do surveillance of Norwegian persons' communication abroad. PST, on the other hand, needs a court ruling to carry out lawful interception in relation to persons in Norway.

The Committee received four complaints against the NIS in 2018, compared with six complaints in 2017. These complaints were against more than one of the EOS services. We concluded two complaint cases in 2018. No complaint cases concluded in 2018 has resulted in criticism of the NIS.

The Committee routinely requests that the NIS report any non-conformities it uncovers in the service's technical information collection. The NIS has not reported any non-conformities in 2018.

## 8.2 The NIS's collection of information from open sources about persons in Norway

The NIS is not allowed to do surveillance on or in any other covert manner collect information concerning persons on Norwegian territory.

Subject to certain conditions, the NIS can collect information

37 Cf. the Intelligence Service Act Section 4 first paragraph.

38 Cf. the Oversight Act Section 6 third paragraph (2).

39 Cf. the Oversight Act Section 2.

40 Cf. Royal Decree No 1012 of 31 August 2001 relating to Instructions for the Norwegian Intelligence Service Section 13 letter d.

### Legal person

Any person with rights and obligations. This includes not only people, but also legal persons such as associations, foundations, companies, municipalities, county authorities and the central government.

about Norwegian persons abroad. The Committee noted that the service's internal regulations allow the NIS to also collect information from open sources about persons in Norway – including Norwegian citizens. This is conditional on the purpose of the collection not being to collect information about domestic circumstances, and on the person in question being an approved target.

Based on the above, the Committee asked the service as a matter of principle about what limits Section 4 of the Intelligence Service Act sets for the NIS's collection of information from open sources concerning persons in Norway. The service replied that its collection should only target foreign circumstances within the scope of the NIS's area of responsibility and should not aim to produce information about domestic circumstances. Therefore, the collection activities do not really target persons in Norway. The NIS also claimed that the collection of publicly available information does not fall under the term 'covert' in the sense of the Intelligence Service Act Section 4, even if the service conceals its activities.

The prohibition in the Intelligence Service Act Section 4 is worded as follows:

'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 Committee has raised the question of how the word 'concerning' ('om' in Norwegian) in this provision is to be interpreted in a special report to the Storting.<sup>41</sup> The NIS is of the opinion that the word must be understood to mean targeting and must be interpreted to mean that there must be an intent to do surveillance. In the report, the Committee discussed the NIS's searches in stored metadata linked to persons in Norway to identify selectors of relevance to foreign intelligence activities.<sup>42</sup> We had doubts about whether this was permitted under the current regulatory framework.

The Committee is of the opinion that the service's collection of information from open sources targeting persons who are approved targets and who are in Norway must be subject to the same assessment as the above-mentioned searches.

We are concerned with when the NIS can collect information about persons in Norway. It is not evident from the wording of the prohibition that the *intent* of the service should be the factor that determines whether monitoring persons in Norway is unlawful. That the service's intention is only to monitor a person when he/she is outside Norway, but not when the

person in question is in Norway, is an artificial distinction that it is difficult for us to oversee.

*The Committee finds it difficult to see how the service can search for information of relevance to foreign circumstances by searching open sources for information about persons who are in Norway – and who are targets when they are abroad.*

*We stated to the NIS that there is reason to question whether the collection of information from open sources about Norwegian persons in Norway is lawful under the current regulatory framework. This illustrates that the scope of the prohibition in Section 4 of the Intelligence Service Act should be clarified by the Storting.*

The Committee has submitted comments to the Ministry's proposed draft bill for a new Intelligence Service Act in its consultation submission of 12 February, see section 4.1 and appendix 3.

### 8.3 The NIS's collection of content data about a Norwegian citizen

During an inspection, we found that the service had collected content data in the form of personal data about a Norwegian citizen in Norway. The information had been collected as a result of the service's collection of satellite content data.

The data were collected based on a search term that was within the service's mandate and legal basis. The collected material contained information that met the service's need for information – but also irrelevant information about a Norwegian citizen.

We therefore asked the service whether collection of information about the Norwegian citizen was in breach of the Intelligence Service Act Section 4. The NIS was not aware that it had collected the information about the Norwegian citizen until the Committee asked about it. The service replied that the collection of data was carried out in the course of its statutory duties. Moreover, the search term did not *target* Norwegian persons and was therefore not in breach of the prohibition as understood by the NIS.

As described in section 8.2, the Committee has in a special report to the Storting raised the matter of how the word 'concerning' ('om' in Norwegian) is to be interpreted in the wording of the law: '(...) collect information concerning Norwegian

#### Metadata

Information about data, such as times, duration, to/from identifiers and type of traffic, that describes a technical event that has taken place in a communication network. Information about a telephone call is one example of metadata.

#### Selector

In an intelligence context, a selector is a target from which information is collected, for example a telephone number or an email address.

physical or legal persons'. The NIS is of the opinion that the word must be understood to mean *targeting* and must be interpreted to mean that there must be an intent to do surveillance.

Targeted collection of content data based on a search term will naturally never target specific persons, and if the NIS's understanding of the prohibition is to be applied, such collection will *never* be in breach of the prohibition – despite content data about Norwegian citizens in Norway actually being collected along with other data.

On the other hand, we realise that an interpretation based on a purely linguistic understanding of the word 'concerning' would so severely restrict the service's possibility to collect content data that the service would be unable to perform its statutory duties.

*In our concluding statement to the NIS, we stated that there is reason to question whether the collection of information about a Norwegian person in Norway is lawful under the current regulatory framework – even if the collection was unintentional. In our opinion, this again illustrates that the scope of the prohibition in Section 4 of the Intelligence Service Act should be clarified by the Storting.*

The Committee has submitted comments to the Ministry's draft bill for a new Intelligence Service Act in its consultation submission of 12 February see section 4.1 and appendix 3.

The NIS has informed the Committee that the information about the Norwegian citizen has been deleted.

#### 8.4 The NIS is not permitted to go through content data collected in breach of the law

The Committee has asked the NIS to give an account of whether the service can go through content data collected in breach of the Intelligence Service Act Section 4 first paragraph:

'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 background to this question was that the Committee was under the impression that the NIS had listened to the content of the sound clips that were wrongfully collected in breach of the Intelligence Service Act Section 4 first paragraph. We gave an account of the wrongful collection in the annual report for 2017.<sup>43</sup>

The NIS reported that it had not listened to the sound clips. The Committee noted that the service argued on a general basis that 'the effect of information being acquired in breach of Section 4 (...) [will] not automatically be that the information cannot be processed for foreign intelligence purposes'.

The NIS referred to the European Court of Human Rights' case law specifying the application of ECHR Article 8 (the right to respect for privacy), Supreme Court case law on the use of unlawfully obtained evidence in criminal cases, and correspondingly for civil cases, cf. the Dispute Act Section 22-7.



Photo: Forsvaret / NTB scanpix

41 Document 7:2 (2015–2016) Special Report to the Storting concerning the legal basis for the Norwegian Intelligence Service's surveillance activities.

42 Special Report to the Storting concerning the legal basis for the Norwegian Intelligence Service's surveillance activities, section 5.3.3.

43 The annual report for 2017 section 8.3 under 'Non-conformity case 1'.

The Committee wrote in its concluding letter to the service that foreign intelligence services are fundamentally different from the purposes and activities of police bodies. The function of the Intelligence Service is to 'reduce uncertainty for important decision-makers with a particular focus on predicting the future. They are to evaluate foreign trends and actions of states, organisations and individuals, regardless of whether they intend to engage in criminal activity.'

In our opinion, further processing of such (wrongfully) collected material must still be deemed to constitute 'covert collection' of information about a Norwegian citizen on Norwegian territory. The prohibition against covert surveillance of Norwegian persons in Norway set out in Section 4 of the Intelligence Service Act is a key limitation on the activities of the Intelligence Service.

The Committee also stated the following when concluding the case:

'If the material collected in breach of the Intelligence Service Act Section 4 is reviewed by the NIS, this could constitute a repeated violation of the Intelligence Service Act Section 4, and constitute continued unlawful interference with the monitored person's privacy. The Committee remarks that the opposite conclusion would carry a high risk of undermining the prohibition against surveillance of Norwegian citizens on Norwegian territory set out in the Intelligence Service Act Section 4 first paragraph. This could make the prohibition in the Intelligence Service Act Section 4 illusory and would present a problem for the due process protection of Norwegian persons in Norway.'

*The Committee concluded that the NIS does not have legal authority to go through or otherwise process information originating from Norwegian communication in Norway that the service has collected in breach of the Intelligence Service Act Section 4 first paragraph.*

## 8.5 Collection of communication when one party is in Norway

The Committee has considered the legal basis for processing personal data about persons in Norway in intelligence reports concerning intelligence targets abroad.

Our view is that the service can report information that is necessary and relevant to foreign intelligence and that emerges via 'the Norwegian connection' during collection activities aimed at targets abroad. In other words, lawful collection of information about targets abroad can also include the target's communication with Norwegian persons in Norway. The question in the case was whether the service went too far in collating and continuing to process communication with the Norwegian connection, even though it had been lawfully collected. The Committee decided to let the matter rest after receiving the service's explanation.

*We stated that as part of the work on a new Intelligence Service Act, it must be clarified what limitations apply to the Intelligence Service's collation and further processing etc. of information originating from 'the Norwegian connection' seen in relation to the prohibition set out in Section 4.*

### Covert collection

Collection of information for intelligence purposes that is kept secret from the person about whom information is collected.

### Particularly sensitive information

The EOS Committee has limited access to data held by the NIS that is deemed to be particularly sensitive information. By 'particularly sensitive information', cf. the NIS's *Guidelines for the processing of particularly sensitive information*, is meant:

1. The identity of the human intelligence sources of the NIS and its foreign partners
2. The identity of foreign partners' specially protected civil servants
3. Persons with roles in and operational plans for occupational preparedness
4. The NIS's and/or foreign partners' particularly sensitive intelligence operations abroad\* which, if they were to be compromised,
  - a. could seriously damage the relationship with a foreign power due to the political risk involved in the operation, or
  - b. could lead to serious injury to or loss of life of own personnel or third parties.

\*By 'intelligence operations abroad' is meant operations targeting foreign parties (foreign states, organisations or individuals), including activities relating to such operations that are prepared and carried out on Norwegian territory.

## Oversight of other EOS services

## 9.1 General information about the oversight

The Committee oversees EOS services regardless of which part of the public administration carries out the service.<sup>44</sup> In other words, the oversight area is defined by function rather than being limited to certain organisations.

Following the 2017 amendment of the Oversight Act, the Committee shall carry out one inspection per year of the Army Intelligence Battalion<sup>45</sup> and one inspection per year of the Norwegian Special Operation Forces<sup>46</sup>, cf. the Oversight Act Section 7.

The Committee concluded one complaint case against the security clearance authority in the Norwegian Communications Authority in 2018. The case was concluded without criticism. The Norwegian Communications Authority is no longer a security clearance authority since the Storting's decision in 2016 to change the clearance authority structure from 2018.

## 9.2 The Joint Cyber Coordination Centre (FCKS)

The Joint Cyber Coordination Centre (FCKS) was established in 2017 and is a collaboration between NSM, the NIS, PST and the National Bureau of Crime Investigation (Kripos). The purpose of the centre is to improve Norway's capacity to effectively defend itself against and deal with serious incidents in cyberspace.

The Committee conducted an inspection of the centre in 2018. The inspection did not give grounds for follow-up.

For several years, we have focused on overseeing cooperation between the EOS services in their work in relation to digital threats. It is particularly important to us that cooperation is organised such that the regulatory framework governing the individual services is not circumvented. The Committee expects the services to document their cooperation to enable subsequent oversight by us.

*The Committee will continue its oversight of the cooperation taking place in FCKS.*

## 9.3 Inspection of the Army Intelligence Battalion

According to the Evaluation Committee for the EOS Committee,<sup>47</sup> the need for external oversight of the Army Intelligence Battalion relates to the risk of the tools and knowledge that the battalion possesses, being used in irregular ways.

The Committee inspected the Army Intelligence Battalion at Setermoen in 2018. During its inspection, the Committee was informed about changes in the Intelligence Battalion since the inspection in 2017, cooperation with other EOS services and ongoing cases and activities. The Committee



Photo: Anette Ask / Forsvaret

inspected the Army Intelligence Battalion's computer systems and selected documents based on the Secretariat's preparation for the inspection. The inspection did not give grounds for follow-up.

#### **9.4 Inspection of the Norwegian Special Forces Command**

According to the Evaluation Committee, the need for external oversight relates to the unit's capacity to engage in intelligence activities and the risk of this capacity being used in Norway in peacetime or in other irregular ways. It should also be subject to oversight that the cooperation with the NIS is kept within the framework of the applicable regulations.

We inspected the Norwegian Special Forces Command at Rena in 2018. The Committee was briefed about the organisation, tasks and capacities of the special operation forces. The inspection gave grounds for a written follow-up.

#### **9.5 Inspection of the Norwegian Communications Authority (Nkom)**

Pursuant to the Oversight Act Section 7 (8) that the Committee shall conduct inspections on its own initiative of bodies that assist the PST. The Committee inspected Nkom in 2018. The inspection did not give grounds for follow-up.

#### **9.6 Inspection of Telia Norge AS**

We conducted an inspection of Telia Norge AS in 2018. As an electronic communications network provider, Telia has a duty to facilitate PST's access to information in connection with lawful interception. The inspection did not give grounds for follow-up.

#### **9.7 The personnel security service of the Office of the Auditor General**

The Committee carried out an inspection of the personnel security service of the Office of the Auditor General of Norway in 2017. In a letter to the Office of the Auditor General, we questioned inadequate grounds given to people who were denied security clearance and raised some questions regarding the facts in one of the cases.

In cases where clearance had been denied on grounds of 'connections to other states', the persons were informed by the security clearance authority that the reason why they were not given information about the grounds for the decision was that the grounds were classified.

In its reply to the Committee, the Office of the Auditor General maintained that grounds could not be given and cited the Security Act 1998 Section 25 as the legal basis. According to the Security Act 1998 Section 25 third paragraph first sentence, the '[g]rounds for a decision shall be given at the same time as information about the outcome of the security clearance case'. NSM's guide to this provision states that in each case, grounds 'must be prepared on the basis of the security clearance authority's internal grounds'.

In our concluding statement we made reference to NSM's guide, which also states that the grounds must 'as a minimum mention the provisions and facts on which the decision is based'. It emerges from the wording of the Act that 'connection to other states' can be considered a negative factor – and that it cannot be considered classified information to make reference to it in the grounds. The Office of the Auditor General personnel had themselves provided information about their connections to other states and were thus aware of the facts of the case.

Only in extraordinary cases have the legislators accepted that grounds can be exempt from access, and no such considerations existed in the cases in question.

In the Committee's opinion, a decision to deny security clearance is so invasive that it strengthens the requirement

44 Cf. the Oversight Act Section 1 first paragraph.

45 The Oversight Act Section 7 second paragraph (5) requires the EOS Committee to carry out at least 'one inspection per year of the Army Intelligence Battalion'.

46 The Oversight Act Section 7 second paragraph (6) requires the EOS Committee to carry out at least 'one inspection per year of the Norwegian Special Operation Forces'.

47 On 27 March 2014, the Presidium of the Storting appointed a committee chaired by then Senior Presiding Court of Appeal Judge Bjørn Solbakken and tasked it with evaluating the EOS Committee's activities and framework conditions. The Evaluation Committee submitted its report to the Storting on 29 February 2016, Document 16 (2015–2016).

#### **Personnel security**

Measures, actions and assessments made to prevent persons who could constitute a security risk from gaining any access that could result in a security breach.

that the grounds given must be sufficiently precisely and clearly worded, so that they reflect the considerations that have been decisive in the case. If no grounds are given, that makes it difficult for the persons concerned to respond to the decision and weakens their due process protection. In its concluding letter to the Office of the Auditor General, the Committee remarked that none of the persons had appealed against the negative decisions.

*The EOS Committee criticised the Office of the Auditor General for not having given grounds for the negative decisions as required by the provisions of the Security Act. The Committee urged the Office of the Auditor General to bring its practice into compliance with the Security Act's requirements for notifications to give grounds for decisions and report back to the Committee on what measures it has implemented, cf. the Oversight Act Section 14 final paragraph.*

In one case, the Committee also questioned the basis for the decision to deny security clearance. The person in question was informed that the grounds were classified, and the internal case documents showed that the negative decision was based on connection to another state. In response to questions from the Committee, the Office of the Auditor General expressed that it was the person's reluctance to provide information to the security clearance authority that was decisive to the negative outcome. In our final letter to the Office of the Auditor General, we stated that the person should have been given grounds that reflected the real grounds for the outcome. We also pointed out to the Office of the Auditor General that documentation that the person in question had not provided the security clearance authority with desired information seemed to be lacking in the internal case documents. On the contrary, it was documented that the person in question had supplied several details about contact with citizens of another country to the Office of the Auditor General.

We therefore had grounds to question whether the case had been sufficiently well-informed and documented to enable the Committee to verify the decision.

*We have asked the Office of the Auditor General for feedback on what measures have been implemented based on our criticism, cf. the Oversight Act Section 14 final paragraph.*

## 9.8 Security interviews project

The Committee has for several years paid particular attention to the security interview as an instrument for security clearance authorities in its oversight of security clearance cases. According to the 2018 wording of the law,<sup>48</sup> a security interview shall be conducted in cases where it is not 'clearly unnecessary'. The purpose of the interview is for the security clearance authority to obtain information on which to base its assessment of whether the person concerned is suited for security clearance. According to the Security Act Section 8-4,<sup>49</sup> several matters may be relevant in the assessment of a person's suitability for security clearance.

In 2018, the Committee decided to conduct a systematic review of a large number of security interviews. The purpose of this review is to investigate whether security interviews are prepared and carried out in such a manner that information relevant to the security clearance authority emerges, and how the adversarial principle is safeguarded in relation to the person in question.

*The project is expected to be completed in 2019.*

## 9.9 Complaints against security clearance decisions made by the Ministry of Defence

In 2018, the Committee concluded two complaint cases against the security clearance authority in the Ministry of Defence, which was the appellate body in both cases. We asked the Ministry to document its assessments in the appeal cases. In the Committee's opinion, the Ministry's internal case documents did not show that the Ministry had carried out a concrete and individual assessment of the complainant's suitability for security clearance when considering the appeals. The Ministry stated that it agreed with the assessments and conclusion of the body that made the initial decision, but admitted that the assessments should have been better documented.

*We pointed out that it is very important to the complainants' due process protection and the Committee's opportunity to conduct real subsequent oversight that the assessments made by the security clearance authority are described in the case documents.*

48 See the Security Act 1998 Section 21 third paragraph.

49 See the Security Act 1998 Section 21 first paragraph.

A dark blue background featuring a faint world map. Overlaid on the map is a complex network of thin, light blue lines connecting various points, resembling a global communication or data network. The lines are more densely packed in some areas, particularly around the Atlantic and Indian Oceans.

10.

# Communication, external relations and the media in 2018

## 10.1 Publication of Committee statements via channels other than the annual report

In our public and unclassified reports to the Storting, we take account of both the EOS services' need for secrecy and the public's need for information. It is necessary for an informed debate that information about criticism of the EOS services is available to the general public. We note that the absence of criticism in an area is increasingly taken to mean that the Committee considers a service's activities to be within the applicable regulatory framework.

We believe that it could be a positive contribution to public debate if the Committee published some of its descriptions of concluded cases on a continuous basis modelled on the Parliamentary Ombudsman's practice. We believe that the Committee's consideration of cases that are of public interest, but that do not necessitate a special report to the Storting, can be published as statements during the year. It would also be an advantage in connection with cases that have been subject to publicity and public debate, if the Committee does not have to wait until the next annual report to make a statement. We expect such publication to be relevant only in a small number of cases.

The Committee's statements would be unclassified like its reports to the Storting. Before publishing such statements, we should give the services the opportunity to clarify whether the statement contains classified information and check that there are no errors or misunderstandings in the text. Such statements would only be published in digital form, but would be included in the next annual report.

## 10.2 External relations, annual conference and study trip to the USA

In recent years, the Committee has invested a lot of time and efforts in contact with external parties in Norway and abroad, both to disseminate information about our work and to learn from others.

We believe that making more information about the democratic oversight of the EOS services public will strengthen public confidence in and the legitimacy of the Committee as well as the services. It can also help to improve the services and the Committee.

Provided that we have the capacity and are not prevented by our duty of secrecy, we want to be available to answer questions from the media, researchers and others and to give talks if requested.

In 2018, the Secretariat has started to publish the media summaries that the Committee receives on news stories and reports of relevance to the EOS services – both on the

Committee's website and via our Twitter account. External parties can also receive these summaries via email.

The Committee and Secretariat has attended several conferences abroad in 2018 arranged by oversight bodies and civil society. Among other things, we attended a conference in Paris in December where representatives of 14 European oversight bodies were present with a view to achieving closer oversight cooperation in Europe. This issue is particularly relevant because cooperation between the services is increasing and more and more data are shared across borders.

We have also contributed to international publications, and we have published a joint statement with foreign oversight bodies for the first time. See section 3.2 and appendix 4 for more details about this work.

In April, we hosted our second annual conference for about 100 participants. The topics included transparency in the services, automated control and '5 years after Snowden'.

We will hold another annual conference in 2019 in connection with the publication of this annual report. The conference will be held annually as part of the Committee's work to make the oversight of the EOS services publicly known and contribute to debate on the oversight and its results. Based on the good feedback we have received about the conference in recent years, we feel confident that it is well worth the resources we put into organising it.

The EOS Committee is particularly interested in learning how oversight is organised in other countries in order to improve its own oversight work. For this purpose, the whole Committee and four secretariat employees visited Washington DC for a five-day study trip in September.

The USA has 17 intelligence services, and their combined budgets are many times bigger than the budgets of the Norwegian services. There are also more oversight bodies and more people working in oversight. Nonetheless, American oversight bodies and the EOS Committee have some common challenges.

Some of the people we met with in the USA were:

- Senator Ron Wyden (D), who is a member of the Senate Select Committee on Intelligence.
- The management of the Senate Select Committee on Intelligence's secretariat.
- NSA's Deputy Inspector General.
- The secretariat of the Privacy and Civil Liberties Oversight Boards.
- The Office of the Director of National Intelligence.
- The Department of Justice's Office of Intelligence.
- Representatives of the think tank New America and the NGOs Access Now and Center for Democracy and Technology.

The following were some of the issues we discussed:

- Good systems for whistle-blowers.
- Openness about the activities of the services and the oversight bodies.
- The relationship between internal control and independent external oversight.
- Direct access to the services' computer systems.
- How the courts oversee intelligence services.
- How highly polarised political debate affects oversight.
- Concrete methods and approaches to review of legality.

An overview of the meetings, visits and conferences that the Committee and the Secretariat have attended in 2018 is provided in Appendix 1.

### 10.3 The EOS Committee in the media in 2018

The EOS Committee makes itself available to the media when possible. We would also like to draw the media's attention to our reports to the Storting. The media attention helps to increase knowledge and transparency regarding the oversight of the EOS services.

In March, the Norwegian Broadcasting Corporation (NRK) ran several stories about the Intelligence Service's station at Eggemoen and the satellite communications surveillance that takes place there. The stories were partially based on documents from the 2013 Snowden leak. In interviews with NRK, committee chair Løwer referred to our 2016 special report in which we questioned the legal basis for some of the Intelligence Service's surveillance activities – which was relevant to the issues NRK raised.

In connection with this matter, Løwer also responded to Minister of Defence Frank Bakke Jensen in the newspaper *Dagbladet*, stating that 'he is hiding behind us', when the Minister according to *Dagbladet* claimed that 'the EOS Committee has concluded that the activities are in compliance with Norwegian law'. We never issued that conclusion.

The matters that attracted particular attention from several media following the publication of the annual report for 2017 in April were:

- That PST had on a couple of occasions done surveillance on individuals for longer than the court had permitted.
- NSM and a security clearance authority were strongly criticised for having conducted a security clearance

process when there was no reason to initiate such a process. This had considerable personal, professional and financial consequences for the person in question.

Furthermore, NRK wrote about PST's changed transparency about international cooperation that had a bearing on the joint statement issued by us and four other oversight bodies. See section 3.2 and appendix 4 for more details. This statement was also mentioned in an editorial in November in the weekly newspaper *Morgenbladet* on the draft bill for a new Intelligence Service Act.

The website ABC Nyheter published a story about the different ways in which PST uses surplus information. The Committee pointed out that it is doubtful whether the right to use surplus information from lawful interception should differ depending on whether audio surveillance has taken place as part of an investigation case or a prevention case.

In April, committee chair Løwer also wrote a reply to Kjetil Stormark, editor of the online newspaper *aldrimer.no*, in which she emphasised that we do everything in our power to protect the anonymity of whistle-blowers who contact the EOS Committee, see section 3.3.

### 10.4 Administrative matters

The Committee's expenses amounted to NOK 18,951,810 in 2018, compared with a budget of NOK 19,550,000, including transferred funds. The main reasons for the underspending were leaves of absence in the Committee Secretariat and the fact that it has taken time to recruit new staff – particularly technological advisers. This has resulted in unused payroll funds. The Committee has applied for permission to transfer NOK 598,089 in unused funds to its budget for 2019.

In decision number 305 of 18 December 2018, the Storting allocated NOK 29,000,000 for new premises over the national budget for 2019. We are pleased with the Storting's allocation. A lot of time has been spent on the planning of new premises in 2018. The Committee expects to be able to move into its new premises in spring 2019.

There is still a need to expand the Secretariat by hiring more staff. The Committee will return to this matter in connection with the budget process for 2020.

#### Review of legality

Review that rules of law are complied with.

#### Surplus information

Information that has been obtained by means of e.g. covert coercive measures and is relevant to criminal offences other than that which formed the basis for the use of coercive measures, or information that is not relevant to the criminal offence at all.

**11.**

## Appendices



## APPENDIX 1 – Meetings, visits, lectures and participation in conferences etc.

### Meeting with the Norwegian Board of Technology's secretariat

A secretariat employee visited the Norwegian Board of Technology in January to explain how the EOS Committee conducts its oversight.

### Meeting with the head of the secretariat of the Lawful interception commission

Three secretariat employees met with the new head of the secretariat of the Lawful interception commission in January. The commission's remit has been expanded to include over-seeing equipment interference conducted by the ordinary police. The purpose of the meeting was to share experience with a commission whose remit is in many ways related to that of the EOS Committee.

### Participation in the Lawful interception commission's seminar

A committee member and two secretariat employees took part in the Lawful interception commission's seminar in February. We informed them about the EOS Committee's functions and discussed common issues and the possibility of cooperating.

### Meeting with journalists

In February, nine journalists visited the committee chair and two secretariat employees after the EOS Committee had invited journalists who are interested in 'EOS matters'. The purpose of the meeting was to establish contact with interested journalists and provide them with information intended to help to improve understanding of our oversight responsibility.

### Presentation for Norwegian PEN

In March, Norwegian PEN's surveillance committee invited the committee chair to give a presentation on the EOS Committee's work.

### Conference hosted by the Bundestag in Berlin

A committee member and one secretariat employee attended a conference in March on the topic of intelligence services in a state based on the rule of law.

### Meeting with the Norwegian Civil Security Clearance Authority

Two secretariat employees met with the new head of the newly established Norwegian Civil Security Clearance Authority in April.

### Presentation at Nasjonal beredskapskonferanse

In April, the committee chair gave a talk about the EOS Committee's activities and issues related to surveillance and protection of privacy at the national preparedness conference 2018.

### The EOS Committee's annual conference

The Committee held its annual conference on 11 April. The 2018 conference had more than 100 participants, and, in addition to the annual report for 2017, topics included transparency in the services, '5 years after Snowden' and smart intelligence and automated oversight.

### Security conference in Trondheim

A committee member attended the information security conference *Sikkerhet og Sårbarhet* in Trondheim.

### Participation in debate about transparency in the Norwegian Armed Forces

In May, the committee chair was invited to speak at a conference on transparency and academic freedom in the defence sector under the auspices of the Norwegian Institute for Defence Studies (IFS) and the Centre for Integrity in the Defence Sector (CIDS).

### Participation in workshop in Berlin

A secretariat employee went to Berlin in May to take part in a workshop organised by the German think tank Stiftung Neue Verantwortung, which brought together representatives of several oversight bodies and experts to exchange best practices. This workshop formed part of the basis for the think tank's publication *Upping the ante on bulk surveillance – An international compendium of good legal safeguards and oversight innovations*.

### Presentation in Ukraine

The deputy chair visited Kiev in May to attend a seminar for Ukrainian members of parliament about a new act relating to the security services and oversight of the services. The deputy chair gave a lecture on the Norwegian oversight model for the secret services. The seminar was organised by the Ukrainian parliament, NATO, the EU and DCAF.

### Visit from the Norwegian Data Protection Authority

The head of the Data Protection Authority and a senior adviser visited in June to tell the EOS Committee about issues relating to artificial intelligence and protection of privacy.

### Meetings with other oversight bodies concerning a common project

In June (Copenhagen) and October (Bern), secretariat employees and the committee chair (Bern) met with the oversight bodies of Denmark, Switzerland, Belgium and the Netherlands in connection with the project the five bodies have been engaged in since 2015. This resulted in a joint statement published in November – *Strengthening oversight of international data exchange between intelligence and security services*. Read more about this in section 3.2 and appendix 4.

### Workshop and presentation in the UK

In July, a secretariat employee took part in a workshop on oversight of secret services in Colchester. The event was organised by the University of Essex and the UK oversight body IPCO. Representatives of the UK, Israel, Norway and the Netherlands attended the workshop.

### Presentation for an Armenian delegation

In September, the deputy chair gave a talk on the EOS Committee's work for a delegation from Armenia. The delegation was visiting the Ombudsman for the Armed Forces.

### Conference on oversight cooperation in Berlin

A secretariat employee attended a conference on possibilities for cooperation between European oversight bodies in September. The conference was organised by three German civil society organisations.

### Study trip to the USA

The whole Committee and four secretariat employees visited Washington DC for a five-day study trip in September to learn more about the USA and the oversight of its intelligence services. Read more about this study trip in section 10.2.

### Meeting with the Ombudsman for the Armed Forces

In October, the committee chair and representatives of the Secretariat met with the Ombudsman for the Armed Forces to discuss methods and common challenges.

### Launch of book with foreword by the EOS Committee

The committee chair gave a talk at the Norwegian Institute of International Affairs (NUPI) in October in connection with the launch of the book *Intelligence oversight in the twenty-first century*. The committee chair wrote the foreword to the book. The book is partly based on presentations from the conference that was held to celebrate the EOS Committee's 20th anniversary in 2016.

### Meeting with the Norwegian Bar Association

In October, the committee chair and two secretariat employees met with the president and secretary general and other representatives of the Norwegian Bar Association. The parties discussed the work of the EOS Committee in general and consideration of complaint cases in particular.

### Lecture for the Storting's administration

The head of the secretariat gave a talk on the activities of the EOS Committee in November.

### Participation in the *Nasjonalt internetforum* conference

In November, a secretariat employee took part in a conference on the internet in Norway under the auspices of the Norwegian Communications Authority and Norid.

### Lecture at the Norwegian Defence University College

The committee chair and the head of the Secretariat's technology unit both gave talks for students on the intelligence course at the Norwegian Defence University College in November.

### Meeting of the Norwegian Information Security Forum (ISF)

In November, a secretariat employee attended the Christmas meeting of ISF, of which the EOS Committee is a member.

### International oversight conference in Malta

A secretariat employee participated in the third International Intelligence Oversight Forum in November. The event was organised by the UN Special Rapporteur on the right to privacy, Joe Cannataci. The secretariat employee also gave a talk on the EOS Committee's oversight function. The 2018 conference was held in Malta, and was attended by people from more than 20 countries. All continents except South America were represented. Cooperation between oversight bodies was one of the key topics of the conference. In addition to oversight bodies, representatives of academia, civil society, prosecuting authorities, data protection authorities, parliamentary committees and public administration also attended.

### Meeting of oversight bodies in Paris

Under the auspices of the French and Belgian oversight bodies, the committee chair and the head of the Secretariat's technology unit went to Paris in December together with representatives of 13 other European countries. The goal of the conference was to promote closer cooperation and more meetings between European oversight bodies.

*Events for which no other location is specified have taken place in Oslo.*

The EOS Committee's annual conference welcomes both domestic and foreign speakers.

From left: Journalist Ryan Gallagher (The Intercept), former head of the NIS, Kjell Grandhagen, head of PST, Benedicte Bjørnland, Gerald Folkvord from Amnesty International, professor Iain Cameron and moderator Anne Grosvold.

Photo: EOS-utvalget



## APPENDIX 2 – News from foreign oversight bodies

### Denmark

In one in five spot checks, the Danish Intelligence Oversight Board found that searches in raw data about Danish people had been conducted without a legal basis. Among other things, the Danish Security and Intelligence Service was criticised for not complying with deadlines for deletion.

### The Netherlands

A new intelligence services act that grants the services wider authorities, including a form of digital border defence, was implemented in 2019.

The Review Committee for the Intelligence and Security Services (CTIVD) has looked at how the country's two services have implemented the new act and has criticised them for lacking both good internal control systems and systems for ensuring that they do not store more data than is necessary.

CTIVD has also prepared a report in which it investigates multilateral collaboration in the Counter-Terrorism Group (CTG, a European collaboration based in the Netherlands). The committee identified several possibilities for improvement and found the possibilities of exercising oversight to be inadequate.

In CTIVD's annual report for 2017, the committee identified breaches of the law in connection with the services' use of equipment interference/hacking. The committee also oversaw bulk collection of data from open internet sources. CTIVD checked four bulk data sets. Two of them contained personal data such as names, email addresses, postal addresses and passwords. CTIVD believed one of the data sets to be unlawfully collected because sufficient political authorisation had not been obtained.

### The UK

The Intelligence and Security Committee of Parliament described in two reports how the UK intelligence services

contributed to the torture and rendition of suspected terrorists after the attacks on the USA on 11 September 2001.

### New Zealand

In its annual report for 2017/2018, the Inspector-General for Intelligence and Security writes that they have looked into all complaints received from people who suspect that they are under surveillance by New Zealand's secret services. The Inspector-General states that she has received confirmation that the services held no information about the persons concerned. To compare this to the situation in Norway: the EOS Committee is in principle only permitted to say whether or not it found reason to criticise the service.

### Finland

A law that will give the intelligence services more powers is under consideration by the Finnish parliament. The draft bill also includes a proposal to establish the country's first independent specialised oversight body for the secret services.

### USA

The Office of the Inspector General at the National Security Agency published a public version of its semi-annual report for the first time. Among other things, the Inspector General writes that only 12 out of 72 intelligence oversight recommendations made had been implemented at the time of the report's submission. Half of the recommendations had not been addressed by the NSA despite being made at least one year ago.

### Canada

A draft bill considered by the Canadian parliament has proposed establishing a single oversight body – the National Security and Intelligence Review Agency (NSIRA) – to oversee all the services. At present, each service has its own oversight body. The NSIRA will probably be the world's largest independent oversight body. A separate parliamentary committee has also been established to oversee the secret services.

The Committee was in September in Washington DC to learn more about the US system for oversight with their intelligence services. This photo is taken from our visit at the United States Department of Justice.

Photo: EOS-utvalget



## APPENDIX 3 – Consultation concerning a draft bill for a new Intelligence Service Act

The Ministry of Defence  
P.O. Box 8126 Dep.  
NO-0032 OSLO

12 February 2019

### Consultation submission from the EOS Committee – consultation on the draft bill for a new Intelligence Service Act

#### Part I – Introduction and general remarks

##### 1. Introduction

The EOS Committee refers to the Ministry of Defence's consultation letter of 12 November 2018 on the draft bill for a new Intelligence Service Act and hereby submits our consultation statement.

It has been the EOS Committee's practice to have a high threshold for submitting consultation statements. It does not fall within the Committee's remit to have opinions about which surveillance methods the Storting as the legislative body should permit the Norwegian Intelligence Service to use. However, this draft bill directly affects the EOS Committee's oversight and gives grounds for some comments. Moreover, the Committee believes that this draft bill would have consequences that the Storting should be made aware of before considering it.

The Committee has noted that the consultation paper consistently refers to the EOS Committee as a security mechanism. It is important to underline that the EOS Committee is no guarantee that errors are not made or cannot be made in the EOS services. Our oversight is based on spot checks and is not intended as a complete review of all surveillance activities carried out by the EOS services. The Committee's right of access to information is a fundamental precondition for our oversight, and it probably has a strong disciplinary and thus preventive effect.

The Committee's capacity is currently being fully utilised.<sup>50</sup> More oversight duties will necessitate further prioritisation for the committee members. As a minimum, the Secretariat should be significantly strengthened to allow the Committee to meet the expectations made of its oversight. An overall review of the oversight model may therefore be in order, see section 2 below.

##### 2. Oversight as a precondition for lawfulness

The Evaluation Committee concluded that 'the Norwegian model of democratic oversight of the EOS services grounded in parliament is internationally acknowledged as a good one'.<sup>51</sup> The Ministry refers to the fact that the oversight model was recently evaluated and upheld by the Storting.<sup>52</sup> Based on decisions made by the

<sup>50</sup> On 27 March 2014, the Presidium of the Storting appointed a committee tasked with evaluating the EOS Committee (the Evaluation Committee). The Evaluation Committee submitted its report to the Storting on 29 February 2016: *Report to the Storting from the Evaluation Committee for the Norwegian Parliamentary Intelligence Oversight Committee*, Document 16 (2015–2016) ('the Evaluation Report'). See the Evaluation Report section 31.2 for information about the Committee's capacity.

<sup>51</sup> The Evaluation Report section 1.

<sup>52</sup> Consultation paper section 11.12.5.2.

European Court of Human Rights (ECtHR), the Ministry finds the oversight mechanisms to be among the preconditions for bulk collection being in accordance with the European Convention on Human Rights (ECHR).<sup>53</sup> The Ministry goes on to discuss the quality requirements that must be defined for the oversight and which oversight tasks it must be possible to carry out.

In light of this, the Committee would like to highlight the Storting's previous expectations concerning an examination of the oversight model. The following is quoted from the Standing Committee on Scrutiny and Constitutional Affairs' recommendation to the Evaluation Report:<sup>54</sup>

'The rapidly accelerating technological development, increased globalisation and an increasingly complex threat situation changes the conditions for surveillance and thus for the EOS Committee's oversight of the methods. The Committee has noted that the Evaluation Committee points to the probability of the oversight tasks increasing in complexity and scope, among other things with reference to potential consequences of "digital border defence" that the Ministry of Defence has announced will be reviewed. The Committee notes that the Evaluation Committee finds that it would be **difficult to expand the scope of parliamentary oversight of the secret services without an overall review of the oversight model.**

The Committee also notes that the Evaluation Committee has not conducted such a review, but limited itself to pointing out the need for fresh thinking. In light of the trends described by the Evaluation Committee, **the Committee is of the opinion that the oversight model should have been included in the Evaluation Committee's work, but takes note of the fact that the Storting will have to return to this matter at a later time**' (the Committee's boldface).

Since the standing committee submitted these remarks on 15 December 2016, a 'digital border defence' (now known as facilitated bulk collection) has been examined and distributed for consultation. Furthermore, the ECtHR has emphasised oversight mechanisms as a precondition for the lawfulness of surveillance measures.<sup>55</sup>

The Committee's view is that several aspects of the oversight model can be evaluated on a continuous basis without impacting the fundamental strength of the model, which it derives from its parliamentary basis, independence, right of inspection and the composition of the Committee.

Otherwise, reference is made to the Evaluation Committee's evaluation of the committee model and its relationship to the overall oversight system.<sup>56</sup> The Committee bases its work on the constitutional framework for the Committee's oversight as described by the Evaluation Committee. Among other things, this entails that the purpose of its activities is purely to oversee.<sup>57</sup>

53 Consultation paper section 11.23.3.

54 The Standing Committee on Scrutiny and Constitutional Affairs' recommendation concerning the Report from the Evaluation Committee for the Norwegian Parliamentary Intelligence Oversight Committee (EOS Committee) on the evaluation of the EOS Committee, Recommendation No 146 to the Storting (Resolution) (2016–2017) p. 47.

55 *Centrum for rättvisa v. Sweden* pronounced on 19 June 2018 (not final) and *Big Brother Watch and others v. the United Kingdom* pronounced on 13 September 2018 (not final).

56 See the Evaluation Report sections 31 and 37.

57 See the Evaluation Report sections 1, 10 and 29. In section 10, the Evaluation Committee wrote: 'The fact that the EOS Committee is appointed by the Storting is crucial to understanding the Committee's role, duties and scope of action. It is a constitutional consequence of this fact that the Committee is really independent of the services it oversees. On the other hand, it also limits the Committee's authority in relation to the services, among other things in that it can point out and criticise matters that warrant criticism, but cannot issue instructions to the services or take on an advisory role in relation to them.'

*In light of the legal basis that the draft bill proposes to grant for the Norwegian Intelligence Service's activities, the Committee questions whether a broad consideration of the oversight model, which the Storting seems to expect, has been carried out.*

## Part II – Comments on the draft bill for a new Intelligence Service Act

- On a general level, we would like to point out that the draft bill does not resolve important ambiguities relating to the Norwegian Intelligence Service's surveillance of persons in Norway. Moreover, several of the Committee's critical remarks have been incorporated in the draft bill as exceptions from the prohibition against surveillance of persons in Norway. The consequence will be that the Norwegian Intelligence Service will be granted extended powers in Norway.
- We would particularly like to draw attention to the proposal that the Norwegian Intelligence Service's *intent* should be the factor determining whether the service can collect information about persons in Norway. Firstly, this criterion is unsuitable for use in real subsequent oversight by the Committee. Secondly, the criterion seems to obscure the fact that the Norwegian Intelligence Service can use methods against persons in Norway – provided, that is, that the 'intent' is aimed at other persons.

### 3. Comments on Section 2-8 of the draft bill – Duty of facilitation and access

The consultation paper raises the need for rules of law to facilitate effective oversight of the Norwegian Intelligence Service's activities.<sup>58</sup> This is reflected in the proposed provision relating to the purpose of the Act, Section 1-1 b, where it is stated that *the purpose of this Act is to contribute to safeguarding confidence in and securing the basis for oversight of the activities of the Norwegian Intelligence Service.*

The Committee believes that a provision that imposes on the Norwegian Intelligence Service a *duty to facilitate* the EOS Committee's work should be included, for example in Section 2-8 of the draft bill. This would clarify the service's duty to contribute to ensuring a basis for effective oversight of its activities. The Committee must be allowed to play an active role in the development of oversight facilitation. The Committee is of the opinion that it is a precondition for effective oversight, particularly any future control of facilitated bulk collection, that the Committee be given its own tools for use in oversight of the service's systems.

Moreover, the Committee thinks that it should be considered whether the exception from the Committee's right of access for information that the Norwegian Intelligence Service has deemed to be particularly sensitive information should be included in the proposed Section 2-8, and possibly also in the Oversight Act Section 8.<sup>59</sup>

### 4. Comments on Section 2-10 of the draft bill – Processing of personal data

The Ministry writes in the consultation paper that the proposed continuation of the current rule exempting

<sup>58</sup> Consultation paper section 6.6.

<sup>59</sup> The Storting made a plenary decision in 1999 stating that a special procedure shall apply in disputes about access to NIS documents. The decision did not lead to any amendments being made to the Act or Directive governing the Committee's oversight activities, see Document No 16 (1998–1999), Recommendation No 232 to the Storting (1998–1999) and minutes and decisions by the Storting from 15 June 1999. The Storting's 1999 decision was based on the particular sensitivity associated with some of the Norwegian Intelligence Service's sources, the identity of persons with roles in occupation preparedness and particularly sensitive information received from cooperating foreign services. In 2013, the EOS Committee asked the Storting to clarify whether the Committee's right of inspection as enshrined in the Act and Directive shall apply in full also in relation to the Norwegian Intelligence Service, or if the Storting's decision from 1999 shall be upheld. At the request of the Storting, this matter was considered in the report of the Evaluation Committee for the EOS Committee, submitted to the Storting on 29 February 2016, see Document 16 (2015–2016). When the Evaluation Committee's report was considered in 2017, the limitation on access to 'particularly sensitive information' was upheld, but without the wording of the Act being amended.

the Norwegian Intelligence Service from oversight by the Norwegian Data Protection Authority and the Privacy Appeals Board, regardless of the purpose of the processing, ‘is also based on considerations for a uniform oversight regime, which means that the EOS Committee also oversees the Norwegian Intelligence Service’s processing of personal data regardless of purpose’.<sup>60</sup>

*The EOS Committee would like to make clear that the Committee only oversees the processing of personal data that fall within its area of oversight: intelligence, surveillance and security services. The wording of the act should reflect this.*

## **5. Comments on Section 4-1 of the draft bill – Issues relating to intelligence activities and relations with persons and enterprises in Norway**

### **5.1 Territorial limitation – background**

In the current Intelligence Service Act, the prohibition is worded as follows:

‘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 Ministry refers to the draft being based on the current principle that, as a rule, the Norwegian Intelligence Service is not to engage in collection activities targeting persons and enterprises in Norway.<sup>61</sup> The Ministry makes reference to the fact that ‘[t]he prevailing view is currently that the prohibition against covert collection of information “concerning” Norwegian persons in the Norwegian Intelligence Service Act Section 4 first paragraph must be understood to mean covert collection “targeting” Norwegian persons’, and that ‘[t]he 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’.<sup>62</sup>

The Committee disagrees that the prohibition against covert collection of information ‘concerning’ (‘om’ in Norwegian) Norwegian persons in the Norwegian Intelligence Service Act Section 4 first paragraph must be understood to mean covert collection ‘targeting’ Norwegian persons. We have previously raised the question of how the word ‘concerning’ in the current Section 4 is to be interpreted. In its Special report to the Storting concerning the legal basis for the Norwegian Intelligence Service’s surveillance activities, the Committee discussed searches conducted by the Norwegian Intelligence Service in stored metadata relating to Norwegian legal persons in Norway to find selectors for purposes relevant to foreign intelligence.<sup>63</sup> The Committee’s opinion was that it was difficult to find support for such a method in the present regulatory framework. The Committee did *not* agree that ‘the term covert’ relates to the collection method and focus of the collection activity, and not to the subsequent analysis and collation of information that has already been collected. The Committee stated:<sup>64</sup>

‘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

60 Consultation paper section 12.3.2.2.

61 Consultation paper section 8.4.3.4.

62 Consultation paper section 8.2.2.5 page 117.

63 Document 7:2 (2015–2016) *Special Report to the Storting concerning the legal basis for the Norwegian Intelligence Service’s surveillance activities*, section 5.3.3. The report will hereinafter be referred to as ‘the 2016 special report’.

64 The 2016 special report, section 5.3.3.

analyses. This will apply regardless of NIS's expert assessment of relevance considered in isolation. The prohibition in the Norwegian 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.'

*The Committee notes that our comments on how the word 'concerning' in the current Section 4 is to be interpreted have not been taken into consideration in the consultation paper.*

The Committee is still of the opinion that the current prohibition in the Norwegian Intelligence Service Act Section 4 limits the service's possibility to collect information relevant to foreign intelligence in Norway. The Committee notes that the draft bill does not set out such a limitation when the provision is interpreted to contain a limitation on collection activities with the intent to do surveillance.

*In the Committee's opinion, the regulation entails broadening the Norwegian Intelligence Service's right to collect information relevant to foreign intelligence in Norway compared with current law. Whether restrictions on the right to collect information relevant to foreign intelligence in Norway should or should not be imposed on the Norwegian Intelligence Service, is for the Storting as the legislative body to decide.*

## 5.2 More about 'intent to do surveillance'

The proposed territorial limitation in the new Section 4-1 concerns use of the Norwegian Intelligence Service's methods 'targeting' persons in Norway. The use of the word 'targeting' is interpreted as introducing an *intent to do surveillance*.

As the Committee stated in the 2016 special report, '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'.<sup>65</sup>

The prohibition on collection in the current Intelligence Service Act prohibits 'all collection, including from open sources and covert collection disciplines, of information targeting persons or enterprises in Norway'.<sup>66</sup> In the Committee's opinion, it is not evident that the wording of the prohibition in the current Section 4 can be interpreted to mean that the *intent* of the service determines whether surveillance of persons in Norway violates the prohibition or not. The Committee also remarks that it could be difficult to check the Norwegian Intelligence Service's *intent* in each case, which can be illustrated by means of the following hypothetical example:

A person returns to Norway after having been an intelligence target for the Norwegian Intelligence Service's collection of information abroad. As a consequence of the prohibition against collection in the proposed Section 4-1, all collection activities in relation to the person must stop when he or she is in Norway. However, since the draft bill assumes that the prohibition against collection is only applicable when the Norwegian Intelligence Service acts with the *intention to do surveillance*, the service can continue to conduct searches in raw data based on the person's personal selectors<sup>67</sup> and continue to collect information through open sources belonging to the person who has returned.<sup>68</sup> The condition for such further use of methods/collection is that the activities are not 'targeting' the person who has returned, but 'targets circumstances or persons abroad'. It will be difficult for the Committee to examine.

<sup>65</sup> The 2016 special report, section 5.2.3.2.

<sup>66</sup> Consultation paper section 8.4.3.4.

<sup>67</sup> Cf. the draft bill Section 4-2 seventh paragraph.

<sup>68</sup> Cf. the draft bill Section 4-2 final paragraph.

In connection with the 2016 special report, the Norwegian Intelligence Service itself wrote that its '[f]ocus is on information, not individuals, and there is in principle no stigma attached to being of interest to NIS'.<sup>69</sup> In the Committee's opinion, this indicates that *intent to do surveillance* is not a suitable criterion for a territorial prohibition against collection. The word 'target' might obscure the fact that the Norwegian Intelligence Service's methods can actually be used for intelligence purposes with regards to the communication of persons in Norway.

If 'intent to do surveillance' is to become the criterion for determining whether or not the service can use its methods in relation to persons in Norway, this would in principle open up the possibility of all the service's methods, including covert collection disciplines, being used with regards to the communication of persons in Norway as long as the collection is deemed to 'target circumstances or persons abroad'. Changing times, new challenges facing society and unexpected threats can all change the need to collect information relevant to foreign intelligence in Norway. Making the intent to do surveillance a criterion for the collection of the communication of persons in Norway will therefore entail a risk of undermining the proposed 'territorial limitation' on the Norwegian Intelligence Service's surveillance activities.

*If there are to be no limitations on the information that the Norwegian Intelligence Service can collect about Norwegian communication relevant to foreign intelligence in Norway, then this should be clearly stated in the Act.*

### 5.3 Conclusion

In the Committee's opinion, *intent to do surveillance* ('targeting') is not a suitable criterion for a territorial prohibition against collection. The Committee's view is that the prohibition against the Norwegian Intelligence Service engaging in collection on Norwegian territory must be clarified in the further work on the new Intelligence Service Act.

## 6. Comments on Section 4-2 of the draft bill – Exceptions from and clarification of the prohibition in Section 4-1

### 6.1 Comments on the draft bill Section 4-2 first paragraph – Collection of information concerning foreign intelligence activities in Norway

The Committee takes note of the Ministry's assessment that collection targeting *Norwegian citizens*<sup>70</sup> in Norway who are engaged in foreign intelligence activities shall no longer be part of the Norwegian Intelligence Service's duties.

The Committee's oversight responsibility does currently not cover activities 'which concern foreigners whose stay in Norway is in the service of a foreign state'.<sup>71</sup> Given that this limitation is removed in the proposed new Oversight Act Section 5 fifth paragraph, the Committee suggests considering the introduction of an explicit *duty to notify* the EOS Committee when the Norwegian Police Security Service has granted consent to the Norwegian Intelligence Service engaging in intelligence activities in Norway under the exception provision in the draft bill Section 4-2 first paragraph final sentence. The same duty should also apply if the Norwegian Intelligence Service initiates collection without the consent of the Norwegian Police Security Service with regards to persons acting on behalf of a foreign power or activities carried out by a foreign power in Norway (other 'foreign activity').

69 The 2016 special report, section 1.5 on the Norwegian Intelligence Service's overriding considerations.

70 See the Committee's annual report for 2017 section 8.2 pages 41–43, cf. Recommendation No 389 to the Storting (2017–2018) – 2. Komiteens merknader ('The Committee's comments').

71 Cf. the Oversight Act Section 5 fifth paragraph.

### 6.2 Comments on the draft bill Section 4-2 second and third paragraph – sources and source verification

In its special report about its investigation into information about the Norwegian Intelligence Service's sources etc.,<sup>72</sup> one of the Committee's conclusions was that it had not found examples of the service violating the prohibition in the Intelligence Service Act Section 4 against surveillance or in any other covert manner collecting information concerning Norwegian physical or legal persons on Norwegian territory.

The Committee notes that the proposed Section 4-2 second paragraph sets out exceptions from the prohibition against collection that applies to the Norwegian Intelligence Service. Legal basis for covert collection of information about potential sources and for source verification purposes is proposed. The Committee notes with particular interest that the Norwegian Intelligence Service will be able to initiate covert human intelligence operations in relation to such sources in Norway for a limited period of time if 'weighty security reasons' exist. Such operations 'may include infiltration and provocation', as well as covert 'systematic collection of information by means of interaction with people', cf. Sections 6-3 and 6-4.

The draft bill appears to entail an expansion of the activities authorised by law compared with prevailing law. It is up to the legislators to decide which intelligence methods the service should be permitted to use *in Norway* to 'obtain relevant information to find potential sources or for source verification purposes'. It will be a challenge for the Committee to oversee the distinctly discretionary assessments that this section sets out, among other things in terms of what constitutes 'strictly necessary' information and when 'weighty security reasons' exist to indicate the use of intrusive methods for the above-mentioned purposes in relation to the service's sources and potential sources.

### 6.3 Comments on the draft bill Section 4-2 sixth paragraph – Collection of bulk raw data that contain information about persons and enterprises in Norway

The 2016 special report questioned the Norwegian Intelligence Service's current legal basis for collection of metadata that may include communication to and from Norwegian legal persons in Norway. The questions particularly concerned the service's collection of metadata from satellite communication, where communication signals are intercepted in transit between a sender and a recipient through what is known as midpoint collection, cf. the draft bill Section 6-7. The Committee concluded that there is some uncertainty as to the legality of collection of metadata that may contain information about Norwegian citizens in Norway.

*The Committee notes that our remarks regarding the Norwegian Intelligence Service's practice of collecting bulk metadata that may include communication to and from Norwegian legal persons in Norway have been incorporated in the draft bill as exceptions from the prohibition against collection that applies to the Norwegian Intelligence Service in the draft bill Section 4-2 sixth paragraph.*

The Committee notes that the proposed exception from the prohibition against the collection of *raw data*<sup>73</sup> *in bulk* does not appear to be limited to metadata or to the collection of communication signals in transit between a sender and a recipient. The Committee also notes that the Ministry writes that raw data in bulk can be collected '*using any collection method*', including collecting information from open sources. Whether bulk collection '*using any collection method*' will be a proportional measure in each individual case, could depend on the collection method used.

*It is important to also strengthen the Committee's subsequent oversight of the Norwegian Intelligence*

<sup>72</sup> Document 7:1 (2013–2014), submitted on 16 December 2013.

<sup>73</sup> In the proposed Section 1-4 (13), 'raw data' are defined as 'any form of unprocessed or automatically processed information whose intelligence value has not been assessed'.

*Service's bulk collection of raw data, among other things by giving the Committee its own tools for use in oversight of the service's systems.*

#### **6.4 Comments on the draft bill Section 4-2 seventh paragraph – Searches in raw data based on a personal selector that can be linked to a person in Norway**

In 2014, the Committee was made aware that the Norwegian Intelligence Service carries out searches in stored *metadata*<sup>74</sup> relating to Norwegian legal persons in Norway to find *selectors*<sup>75</sup> relevant to the performance of the service's tasks. The Committee stated in its 2016 special report that these searches were problematic in relation to Section 4 of the Intelligence Service Act.<sup>76</sup>

*The Committee notes that our critical remarks regarding the Norwegian Intelligence Service's practice of conducting searches in stored metadata linked to Norwegian legal persons in Norway have been incorporated as exceptions from the prohibition against collection that applies to the Norwegian Intelligence Service in the draft bill Section 4-2 seventh paragraph.*

The proposed territorial limitations means that the Norwegian Intelligence Service has to stop all collection 'targeting' persons in Norway. However, the regulatory framework would permit the Norwegian Intelligence Service to continue to search for personal selectors belonging to persons in Norway, provided that the service does not have an 'intent to do surveillance' the persons in Norway. These raw data are covertly collected by means of the service's technical collection systems. The Committee therefore finds it difficult to see how these searches do not also 'target' the person in question while he or she is in Norway. Even though it is claimed that searches conducted in such raw data do not 'target' the person in Norway, the person's communication will in any case be the subject of the Norwegian Intelligence Service's active intelligence work.

*As mentioned in section 5, it will be difficult for the Committee to examine if the searches are not in reality 'targeting' persons in Norway ('intent to do surveillance').*

#### **6.5 Comments on the draft bill Section 4-2 eighth paragraph – Collection from open sources**

The legal basis for collection from open sources is provided in the draft bill Section 6-2. The Ministry proposes an exception in Section 4-2 final paragraph on the collection of information from open sources belonging to persons *in Norway*. The draft bill also allows for collection of information from open sources *in bulk*; cf. the draft bill Section 4-2 sixth paragraph above. The Ministry refers to the fact that bulk collection can in principle take place '*using any collection method*', '[f]or example, collection from open sources can also entail bulk collection'.<sup>77</sup> The Ministry writes as follows:

'Collection from open sources has traditionally not been considered a "covert" intelligence discipline, and the method has not required any explicit authority in Norwegian law pursuant to the principle of legal basis. This is because the information collected will typically be freely shared on the internet or another publicly available medium, and the persons who have shared the information have no reasonable expectations that the information will be protected. However, collection of information from open sources of a certain scope or intensity may be considered interference pursuant to ECHR Article 8 on the right to privacy. In these cases, collection must be warranted by law and deemed necessary in a democratic society out of consideration for a legitimate purpose.'

74 Metadata are 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.

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

76 The 2016 special report, section 6.

77 Consultation paper section 9.5.6.3.

The proposal would mean that the Norwegian Intelligence Service could collect information from open sources, for example social media platforms, about persons *in Norway* to find information about foreign circumstances or persons abroad. As part of these intelligence activities, information can be collected that the person in question has not shared openly.

If, for example, a person in Norway has ‘contact with terrorist networks abroad’,<sup>78</sup> it is difficult to see how collection from open sources would *not also* ‘target’ this person.

In 2018, the Committee questioned the Norwegian Intelligence Service’s legal authority for collecting information from open sources belonging to persons who were approved targets abroad, but who are in Norway. In the Committee’s opinion, the collection of information about such persons must be subject to the same assessment as searches conducted by the Norwegian Intelligence Service in stored metadata relating to Norwegian legal persons in Norway to find selectors for purposes relevant to foreign intelligence, cf. section 6.4.

Moreover, the EOS Committee does not agree with the Norwegian Intelligence Service’s interpretation of the term covert. As long as the Norwegian Intelligence Service collects information secretly, the collection must be considered to be ‘covert’.

*The Committee notes that our critical remarks regarding the Norwegian Intelligence Service’s practice of collecting information from open sources linked to Norwegian legal persons in Norway have been incorporated as an exception from the prohibition against collection that applies to the Norwegian Intelligence Service in the draft bill Section 4-2 eighth paragraph.*

## 6.6 Conclusion

*The Committee is of the opinion that the prohibition is not sufficiently clear to form a basis for oversight.*

## 7. Comments on chapter 5 of the draft bill – Fundamental conditions for information collection

The fundamental conditions for target identification and targeted collection follow from the draft bill Sections 5-1 and 5-2, whose criteria are mainly for intelligence professionals to assess. Target identification and targeted collection both involve collecting information about persons using the same intelligence methods. The blurred distinction between target identification and targeted collection, including that ‘both forms of collection are carried out as searches in metadata or content data, or both’,<sup>79</sup> means that it may be challenging to oversee whether the fundamental conditions are met.

The requirement for proportionality, cf. Section 5-4 of the draft bill, will ‘apply to the question of whether information can be collected at all, to how the information can be collected (methods), and to whether the information collected can be disclosed to others’.<sup>80</sup> It will be an intelligence assessment to determine ‘whether information can be collected at all’ and ‘how the information can be collected (methods)’.<sup>81</sup>

The Committee takes a positive view of enshrining in law the fundamental conditions for collection of and searches in raw data in bulk (Section 5-3 of the draft bill) and for target identification and targeted collection,

<sup>78</sup> Consultation paper section 8.8.2.

<sup>79</sup> Consultation paper section 9.3.1.

<sup>80</sup> Consultation paper section 9.1.

<sup>81</sup> Consultation paper section 9.1.

and the proportionality requirement for the collection. The service must be able to document to the Committee that the fundamental conditions are met and that the methods are used in such a way as to minimise their intrusiveness in relation to the individuals subject to the service's methods. This is something the Committee will be able to oversee.

## 8. Comments on Section 6-9 of the draft bill – Preparatory measures

The following provision is proposed in Section 6-9 of the draft bill:

### *'Section 6-9 Preparatory measures*

The Norwegian Intelligence Service can implement preparatory measures necessary in order to use methods as described in this chapter, including overcoming or bypassing actual and technical obstacles, installing, searching or acquiring technical devices and software, and taking control over, modifying or setting up electronic or other forms of technical equipment.'

The following is stated about preparatory measures in the consultation paper:<sup>82</sup>

'A general provision is proposed, see Section 6-9 of the draft bill, that the Norwegian Intelligence Service can implement preparatory measures necessary to carry out the collection, including overcoming or bypassing actual and technical obstacles, installing, searching or acquiring technical devices and software, and taking control over, modifying or setting up electronic or other forms of technical equipment. This does not represent an independent legal basis for using these methods, but is simply intended to highlight in law that the use of these methods requires several preceding actions. The draft bill codifies and specifies current practice, and such measures will generally be an obvious precondition for the Norwegian Intelligence Service being able to obtain physical or logical access and thus have the possibility to use the collection methods regulated. This provision must also be seen in conjunction with Section 11-5 of the draft bill, which deals with measures to safeguard the security of the services' own personnel, sources and operations.'

In the Committee's opinion, such preparatory measures will constitute intelligence activities because they take place as *part* of the Norwegian Intelligence Service's active information collection/surveillance activities. The Committee notes that the consultation paper contains no assessment of whether, and if so, to what extent, such 'preparatory measures' can be implemented in relation to physical or legal persons and their property *in Norway*. This means that the measures have also not been discussed in relation to the proposed territorial limitation of the Norwegian Intelligence Service's surveillance activities.

Moreover, it is unclear whether any 'preparatory measures' *in Norway* to prepare for collection targeting a person *abroad* can include e.g. secret searches, breaking into buildings, intrusion into a computer system, disrupting signals/communication, manipulating persons, third persons or their electronic equipment and other technical equipment.

If the intent is to allow such and other forms of 'preparatory measures' to be implemented *in Norway*, and this means that the Norwegian Intelligence Service is granted legal authority to implement measures for which the Norwegian Police Security Service would need a court's permission, these measures should be considered in relation to the principle of legal basis, the above-mentioned territorial limitations on the Norwegian Intelligence

<sup>82</sup> Consultation paper section 10.5.3.

Service's surveillance activities, and the Norwegian Police Security Service's remit and legal basis.<sup>83</sup>

*The Committee is of the opinion that these circumstances should be further clarified before legal basis for 'preparatory measures' is granted.*

### **9. Collation and further processing of collected information about communication originating from 'the Norwegian connection'**

The Norwegian Intelligence Service's lawful collection in relation to intelligence targets abroad can also cover the target's communication with persons in Norway ('the Norwegian connection'). In 2018, the Committee considered the Norwegian Intelligence Service's legal basis for processing information that originated *exclusively* from the communication's 'Norwegian connection', i.e. exclusively from the person *in Norway*. The Committee was of the opinion that the service can report information that is necessary and relevant to foreign intelligence when the information is obtained through 'the Norwegian connection' in connection with the *lawful* collection of information concerning targets abroad. The question was whether the service went too far in collating and further processing communication with the Norwegian connection even though it had been lawfully collected. The Committee is of the opinion that it must be clarified further in the work on the new Intelligence Service Act what limits, if any, should apply to the Norwegian Intelligence Service's collation and further processing of information originating from 'the Norwegian connection', cf. the prohibition in Section 4, including what is to be considered 'surplus information' for the Norwegian Intelligence Service in this context.

*The Committee would like the Ministry's assessment of these matters.*

### **10. Comments on the consultation paper's discussion of pre-authorization/approval**

The Ministry writes that it 'has considered whether a general mechanism for pre-authorization/approval for the use of methods by an independent body outside the Norwegian Intelligence Service (court of law or independent administrative body) should be established, but has concluded that this is neither possible, necessary nor desirable'.<sup>84</sup>

The Committee has previously referred to the fact that the legislation that governs the Norwegian Intelligence Service for example does not require a court's permission for intercepting a Norwegian person's means of communication abroad. This differs from the situation of the Norwegian Police Security Service, which will need the court's permission for lawful interception of communication to/from the same person's phone number in Norway. The Committee makes particular reference to the counterterrorism field, where close and extensive cooperation is already taking place between the Norwegian Police Security Service and the Norwegian Intelligence Service on persons with connections to Norway.

*The Committee's opinion is that the possibility of pre-authorization/approval of information collection abroad targeting persons with connections to Norway can be examined.*

<sup>83</sup> Annual report for 2009, chapter VI section 2 page 37. The Committee refers to the annual reports for the years 2007–2009, in which we criticised aspects of a joint operation carried out in Norway by the Norwegian Police Security Service and the Norwegian Intelligence Service. Among other things, the Committee remarked that several circumstances indicated that some of the measures that the Norwegian Intelligence Service implemented in Norway were questionable in relation to the principle of legal basis.

<sup>84</sup> Consultation paper section 10.6.2.

## **11. Comments on chapters 7 and 8 of the draft bill – Facilitated bulk collection of transboundary electronic communication**

### **11.1 Introduction**

The EOS Committee has no opinion about whether the Norwegian Intelligence Service should be granted access to transboundary electronic communication as described in chapters 7 and 8 of the draft bill, nor on the conditions for using this method. The Committee's comments relate to the oversight of the collection and the oversight function assigned to the EOS Committee in the draft bill.

### **11.2 The Norwegian Intelligence Service's internal control**

In the consultation paper,<sup>85</sup> the Ministry writes that strict internal control rules apply in the service and that reporting non-conformities is already an established practice in the Norwegian Intelligence Service.

The Committee endorses the Ministry's view that the service should be instructed to report non-conformities in its own facilitated bulk collection systems to the EOS Committee.

The Ministry has not specified in more detail how the Norwegian Intelligence Service's own control of facilitated bulk collection should be organised and which aspects of the collection should be subject to internal control. The Committee assumes that a number of facilitated bulk collection activities can be subject to different internal control procedures. For example, reference is made to the fact that one court ruling can authorise an unknown number of searches in stored data without the searches having been individually assessed by the court.<sup>86</sup> The Committee's opinion is that it would be natural for the different searches to be subjected to some form of internal control procedure, and for the service to establish special procedures to uncover non-conformities itself.

The Committee emphasises the importance of organising a control system comprising several elements. The internal control system should identify errors and shortcomings at the earliest possible stage and the lowest possible level. The service must establish sound control mechanisms to ensure that it complies with the conditions for using facilitated bulk collection.

*The Committee would like a closer examination of the service's internal control and the possibility of having it enshrined in law.*

### **11.3 Comments on Section 7-11 of the draft bill – The EOS Committee's oversight of facilitated bulk collection**

The draft bill proposes that the EOS Committee practise 'enhanced' oversight of this part of the Norwegian Intelligence Service's collection. The Committee is to have unrestricted access to all information and equipment used in the collection. According to the Ministry, this oversight would be 'continuous' and should take place 'relatively frequently' and at the Committee's 'own initiative'.

The Committee understands this proposal to mean that 'enhanced' oversight would entail a more intensive form of oversight than the Committee's regular oversight of the Norwegian Intelligence Service's other intelligence activities. It will otherwise be left up to the Committee to determine how intensive the oversight should be.

<sup>85</sup> Consultation paper section 11.12.3.8

<sup>86</sup> The Ministry proposes that petitions to the court should not have to be individually specified, but may cover 'a set of related cases', cf. the consultation paper section 11.11.4.4.

The EOS Committee's oversight of the EOS services, including the Norwegian Intelligence Service, is not organised as complete oversight of every aspect of the services' intelligence, surveillance, and security activities. Complete oversight would be too great a task for the Committee, and it is questionable whether such oversight is even possible or desirable. The Committee chooses which of the services' activities to take a closer look at based on, among other things, criteria set out in the Oversight Act and the Committee's assessments of where the risk of violation of rights and regulations with serious consequences is greatest. Even though the Committee has full right of inspection in the Norwegian Intelligence Service, with an exception for access to particularly sensitive information, not all the service's activities will be subject to oversight activities.

The evaluation of the EOS Committee conducted in 2016 showed that the Committee's capacity was already stretched. The committee model limits the Committee's capacity and thus also the scope of its oversight activities.<sup>87</sup> Expanding the scope of its control function to include enhanced oversight of facilitated bulk collection would add to the Committee's range of oversight duties. This will reduce the capacity available for oversight of the other EOS services and other aspects of the Norwegian Intelligence Service's activities.

*The Committee is of the opinion that it will be essential to incorporate oversight mechanisms into the data collection systems already during their development.*

It is also a necessary condition for oversight that sufficient computing power and other resources are dedicated to oversight functions in systems developed by the service. The facilitation of oversight helps to make the oversight easier and ensures that it can be carried out in as efficient a manner as possible.

#### **11.4 Comments on Section 8-1 of the draft bill – Rulings authorising facilitated bulk collection**

The draft bill Section 8-1 fifth paragraph states that the court's ruling shall be communicated to the Norwegian Intelligence Service, which shall then make it available to the EOS Committee. The EOS Committee proposes that the ruling and the petition on which it is based shall be *communicated* to the Committee. In order to be capable of exercising effective oversight of whether the service's searches are in accordance with the content of the ruling, the Committee has to be aware of the assumptions on which it is based. Practical facilitation on the part of the service enables the Committee to exercise closer oversight.

The Committee proposes the following adjustment to Section 8-1 fifth paragraph:

*'Section 8-1 Rulings authorising facilitated bulk collection*

*(...)*

*The ruling shall be communicated to the Norwegian Intelligence Service. The service shall communicate the ruling and the petition on which it is based to the EOS Committee.'*

#### **11.5 Administrative and financial consequences for the EOS Committee**

The Committee agrees with the Ministry that the draft bill will necessitate adding to the technological and legal expertise of the Committee Secretariat. The Committee also believes that it is important, as pointed out by the Ministry, to strengthen the Secretariat with dedicated capacity already at the development stage. The Committee would like to remark that the additional technological expertise recently employed in the Secretariat and the further recruitment planned for 2020, has been based on the current need to strengthen the Committee's ordinary oversight. Any needs arising as a result of a system for facilitated bulk collection being adopted will come in addition to this.

<sup>87</sup> The Evaluation Report pages 127 and 130.

The Ministry estimates that four full-time equivalents should be sufficient to attend to the oversight function. It is difficult to give a concrete estimate of the financial and administrative impact of the introduction of this method on the Committee's work. The consultation paper does not provide a concrete description of the scope of use of this new collection capacity. The scope of the activities to be overseen is therefore unknown.

The description of the resource requirements of advance oversight provides an indication. The Ministry estimates that the court will consider one or two cases per week. This estimate is based on the service's petitions to the court potentially covering a set of related cases rather than being individually specified, and on searches based on personal selectors being regulated in a manner that will 'help to keep the number of court decisions at a manageable level'. The Committee therefore assumes that the number of searches etc. that could potentially be subject to oversight may be high. In addition, the Committee's oversight will also cover other aspects of the system for facilitated bulk collection, for example the use of the short-term storage, activity logs and how filters are set up.

Based on the above, the Committee finds the Ministry's estimate of four full-time equivalents to be too low. The Committee's view is that oversight of facilitated bulk collection can be attended to if at least six full-time equivalents are added to the Committee Secretariat as soon as possible should facilitated bulk collection be adopted. The Secretariat's resource requirements must then be continuously assessed. The Committee cannot disregard the possibility that considerable further resources in addition to the above-mentioned six full-time equivalents could be required to strengthen the expertise and capacity for such oversight. The Committee assumes that the majority of these resources will be persons with technological expertise. However, it will also be necessary to strengthen the Secretariat's legal expertise and add some administrative resources. The extra resources must be put in place as soon as possible if the new Intelligence Service Act is adopted and allows for facilitated bulk collection.

The technological expertise of the committee members should also be strengthened. Even though some of the routine oversight activities can be performed by the Secretariat, it is the Committee that decides whether to criticise the service. It is crucial to the Committee's ability to exercise effective and real oversight that its members are capable of assessing the technical documentation that forms the basis for the service's use of facilitated bulk collection. The Committee's overall technological expertise can be strengthened by making such expertise a factor when new members are appointed, or by offering the committee members a possibility to improve their competence in this area.. Reference is made to the question of a review of the oversight model as discussed in section 2 above.

When considering the financial and administrative costs for the Norwegian Intelligence Service, reference is made to the fact that the proposal will bring a need for administrative procedures relating to the EOS Committee's enhanced oversight of facilitated bulk collection. The Committee assumes that development costs relating to incorporating oversight mechanisms into the data collection systems will also be borne by the service.

In order to safeguard the Committee's independent position in relation to the service, the Committee proposes taking steps to enable as much as possible of the continuous (enhanced) oversight to be performed from the Committee's own premises. The Committee is of the opinion that it would be possible to achieve this in its new premises from 2019, considering the available space and security and technical factors. The costs of facilitating system access from the Committee's premises must also be borne by the service.

## Part III – Comments on proposed amendments to the Oversight Act

- The consultation paper proposes two amendments to the Oversight Act. In our opinion, the proposed amendments creates a need to clarify their consequences for the Committee's activities.

### 12 Comments on the Oversight Act Section 5 – Jurisdiction as a criteria for the EOS Committee's oversight duties

#### 12.1 The condition' for the jurisdiction's bearing on the Committee's oversight duties

At present, the EOS Committee's oversight duties activities do not include 'activities which concern persons or organisations not domiciled in Norway (...)', cf. the Oversight Act Section 5 fifth paragraph. The Committee can, 'however', exercise such oversight 'when special reasons so indicate'.

As part of the Ministry's consideration of the ECHR requirement for an effective remedy,<sup>88</sup> the question is raised of whether the right to complain to the EOS Committee under Norwegian law is sufficiently broad.<sup>89</sup> After a discussion of the current right to complain,<sup>90</sup> it is proposed that the current territorial limitation of the Committee's oversight duties be replaced by a limitation based on jurisdiction.

The Ministry proposes that the Oversight Act Section 5 fifth paragraph be amended to the following wording:

'The oversight duties cover all persons, regardless of domicile or citizenship, who are subject to Norwegian jurisdiction.'

The concept of jurisdiction has traditionally been linked to a country's physical control over an area.<sup>91</sup> As regards the Committee's oversight duties, the traditional interpretation will largely correspond to the condition set out in the current Oversight Act that the person must be 'domiciled in Norway'.

It is more unclear to the Committee what consequences the Ministry envisages for oversight, when it discusses whether the Norwegian Intelligence Service surveillance of persons abroad can be deemed to constitute exercise of authority and control over persons, so that *extraterritorial jurisdiction* must be deemed to have been established and thus trigger obligations pursuant to ECHR.<sup>92</sup> The Ministry concludes as follows:<sup>93</sup>

'Until other evidence becomes available, it must be concluded that the legal situation is uncertain as regards ECHR's scope of application in relation to information collection targeting persons abroad by a foreign intelligence service.'

It is precisely jurisdiction that is proposed as a condition for the EOS Committee's oversight duties – while, pursuant to the Ministry's own assessment, the legal situation is uncertain as regards ECHR's scope of

88 Consultation paper section 4.3.

89 Consultation paper section 4.3.4.

90 Consultation paper section 4.3.4.1.

91 The Ministry writes in the consultation paper section 4.1.3 that '[it] follows from the European Court of Human Rights' (ECtHR) case law that a state's jurisdiction pursuant to the European Convention on Human Rights (ECHR) Article 1 is primarily territorial, and that acts that are committed by a state party outside that state's territory or that have effects outside that state's territory, can only in exceptional circumstances constitute exercise of jurisdiction under ECHR Article 1.'

92 The Ministry's discussion of jurisdiction is primarily found in section 4.1.3 of the consultation paper.

93 Consultation paper section 4.1.3.

application to foreign intelligence services' surveillance of persons abroad. For the Norwegian Intelligence Service, the problem is resolved in that the draft bill is 'generic and does not entail differentiated standardisation based on where or in relation to whom an activity takes place'.<sup>94</sup>

Until the question of jurisdiction is decided by a court of law (a national court or the ECtHR), the draft bill will leave it up to the Committee to determine whether surveillance of persons abroad by the Norwegian Intelligence Service triggers obligations pursuant to ECHR, and conduct its oversight accordingly.<sup>95</sup>

**Based on the above, the Committee requests the Ministry to clarify the consequences of the proposed amendment to the Oversight Act Section 5:**

- Clarification is requested of whether the Ministry proposes that the EOS Committee should on its own initiative oversee the Norwegian Intelligence Service's surveillance of persons (both with and without connections to Norway) abroad.
- Clarification is requested of whether the Ministry proposes that the EOS Committee should consider complaints from persons (both with and without connections to Norway) abroad who claim that the Norwegian Intelligence Service has violated their rights.

If the intent is for the EOS Committee to oversee the Norwegian Intelligence Service's surveillance of all persons abroad, this will entail a significant expansion of the scope of its oversight duties. This will in turn put the oversight model under pressure, cf. section 2 above.

At present, the Committee bases its work on the assumption that if the Norwegian Intelligence Service is surveilling persons abroad with connections to Norway, that constitutes 'special reasons' and the surveillance becomes subject to oversight. If the Ministry's interpretation is that the Norwegian Intelligence Service's information collection abroad is *not* subject to oversight under the draft bill, then the service's surveillance abroad of persons with connections to Norway will fall outside the Committee's area of oversight. It is not evident from the consultation paper whether this consequence is intended by the Ministry. In the Committee's opinion, there are good arguments against excluding the Norwegian Intelligence Service's surveillance abroad of persons with connections to Norway from the Committee's oversight.

*The Committee is of the opinion that the Storting should have as concrete and comprehensive an overview as possible of the oversight duties assigned to its oversight body, also in light of section 2 above. Based on the above, we request the Ministry to clarify the consequences of its proposal to make jurisdiction a condition for the Committee's oversight activities.*

## **12.2 The condition of jurisdiction's bearing on the Committee's consideration of complaint cases**

The Committee would like to draw attention to the potential consequences the condition of jurisdiction could have for the Committee's consideration of complaint cases. These consequences are related to and may in part no longer be relevant depending on the clarification requested from the Ministry in section 12.1 above.

The Committee's present practice is to accept for consideration any complaint received from persons domiciled

<sup>94</sup> The Ministry specifies that the Act will apply to all information collection due to practical considerations, not due to any legal obligations.

<sup>95</sup> The 2016 special report, section 3, quotes the Norwegian Intelligence Service pointing 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'. The Committee commented that this should be done as part of a legislative review process.

in Norway on the sole condition that the complaint is against an EOS service.<sup>96</sup> For persons with connections to Norway who are domiciled abroad, the Committee requires grounds to be given for the complaint (cf. the requirement for 'special reasons' in the Oversight Act Section 5 fifth paragraph).

It is emphasised that the Committee accepts complaints for consideration *without first conducting investigation activities in relation to the service*. The EOS Committee's decision to accept or refuse to consider a complaint will never be based on a preceding investigation of what information may exist or not exist about the complainant in the service(s). The reason for this is that *any* outcome of the Committee's investigations in relation to the services is considered classified information.<sup>97</sup>

**(I) It is classified information that a person is unknown to the service.**

In such cases, the Committee will inform the complainant that the complaint has been investigated and that the Committee has not found that the service has broken the law or acted in a manner that warrants criticism. The complainant is *not* informed that he or she is unknown to the service.

**(II) It is classified information that a person has been subjected to lawful surveillance activities by the service.**

In such cases, the Committee will inform the complainant that the complaint has been investigated and that the Committee has not found that the service has broken the law or acted in a manner that warrants criticism. The complainant is *not* informed that he or she has been subjected to *lawful* surveillance.

Only in cases where the Committee's investigation shows that the complainant's rights have been violated can the Committee confirm to the complainant that he or she is known to the service – in that the Oversight Act allows the Committee to state that it found grounds for 'criticism'.<sup>98</sup>

The Ministry's proposal that the Committee can consider complaints *if* the person is subject to 'Norwegian jurisdiction' appears to be in conflict with the security classification condition on which the Oversight Act is based, cf. sections (i) and (ii) above.

Whether or not a person abroad is to be considered to be subject to Norwegian jurisdiction as a result of surveillance by the Norwegian Intelligence Service or the absence thereof – will make it necessary for the Committee to conduct investigation activities in relation to the Norwegian Intelligence Service and draw a conclusion based on its findings *before accepting the complaint for consideration*.

The Committee requests the Ministry to clarify whether a conclusion from the Committee that a person abroad is subject to Norwegian jurisdiction (after which the person in question will be informed that the complaint is accepted for consideration) could be deemed to constitute confirmation of classified information. Such a conclusion can hardly be understood as anything but a confirmation of the Norwegian Intelligence Service's presence or interest in an area, country or person. If the Ministry is of the opinion that the outcome of the Committee's assessment of jurisdiction in a complaint case can disclose classified information, the Committee's view is that a jurisdiction condition should not be included in the Oversight Act as a condition for the Committee's remit, or that the right to complain must be safeguarded by other means.

96 The Committee practises a low threshold for considering complaints. Complainants cannot be expected to hit the nail on the head when they have no access to information about any surveillance measures against them by the EOS services. If a complainant who is resident in Norway (or who cites 'special reasons') claims that an EOS service has committed an injustice against him or her, the Committee will accept the complaint for consideration.

97 The Oversight Act Section 15 first paragraph second sentence reads as follows: 'Information concerning whether or not a person has been subjected to surveillance activities shall be regarded as classified unless otherwise decided.'

98 The Committee has previously stated that this can be demanding, see section 38.6 of the Evaluation Committee's report. The Committee stated in the annual report for 2017 that it is challenging that the Committee is legally prevented from providing further information about the grounds for criticism in complaint cases, see section 3.

If the Ministry is of the opinion that the Committee can inform a complainant abroad of the outcome of its assessment of jurisdiction without coming into conflict with the prohibition against sharing classified information, then the Committee has no objections against jurisdiction being made a condition for accepting *complaints* from persons abroad.<sup>99</sup> In the Committee's opinion, it is formally possible to establish such a right to complain without at the same time expanding the scope of the Committee's other oversight duties.

*The Committee requests the Ministry to clarify the consequence of the jurisdiction condition for the Committee's consideration of complaint cases.*

### **13. Comments on the Oversight Act Section 15 – The Committee's possibility to make statements about the public administration's liability in damages**

In its annual report for 2016, the Committee requested that the Storting consider whether the Committee can make statements about the public administration's liability in damages. The Committee's account and request were based on its oversight of security clearance cases. The Standing Committee on Scrutiny and Constitutional Affairs expressed in its recommendation to the Storting that the Committee's proposal should be examined more closely and asked the Government to get back to the Storting with an assessment.<sup>100</sup>

With reference to the above-mentioned annual report, among other things, the Ministry has proposed the following amendment to the Oversight Act Section 15 first paragraph third sentence:

'Statements in response to complaints against the services concerning surveillance activities shall only state whether or not the complaint contained valid grounds for criticism, and whether the Committee is of the opinion that there is a basis for liability in damages on the part of the public administration in relation to the complainant.'

Firstly, the proposed wording seems to exclude the Committee's consideration of complaints concerning security clearance cases, as it only refers to 'surveillance activities'. Even though the consultation paper seems to assume that security clearance cases are also covered, this should be included in the wording of the act.

Secondly, the request that the Committee made to the Storting in 2016 did not cover surveillance cases, but was limited to security clearance cases. The limitation of the request to security clearance cases was an intentional decision on the part of the Committee and was based on the challenges the Committee has experienced in its efforts to be able to give any *grounds* at all in complaint cases concerning surveillance that resulted in criticism.

The Committee's statements to complainants in surveillance cases, and the challenges it gives rise to that the Committee can only state whether 'criticism has been expressed', is a matter that the Committee has raised for some time. The consultation paper has not examined how the Committee can make a statement concerning 'basis for liability in damages', given its lack of opportunity to give grounds for the criticism expressed in complaint cases concerning surveillance. Based on the proposed wording, a complainant can be informed that 'criticism has been expressed' and that there is a 'basis for liability in damages' without being told *anything* else.

<sup>99</sup> Complaints received from persons domiciled in Norway can be considered in the same manner as today, as there can be no doubt that a state has jurisdiction on its own territory.

<sup>100</sup> Recommendation No 418 to the Storting (2016–2017).

In principle, the Committee takes a positive view of being given the opportunity to make statements on liability in damages in response to complaints concerning surveillance, but emphasises that such an arrangement must be thoroughly examined and probably also enshrined in regulations in more detail. It can be mentioned<sup>101</sup> that more complaints concerning surveillance are related to the Committee's oversight of the Norwegian Police Security Service than to its oversight of the Norwegian Intelligence Service.

*The Committee is of the opinion that the Committee's right to make statements about the public administration's liability in damages in surveillance cases must be examined further.*

Yours sincerely,

A handwritten signature in blue ink, appearing to read 'Eldbjørg Løwer', is centered on the page.

Eldbjørg Løwer  
Chair of the EOS Committee

---

<sup>101</sup> It is the Norwegian Police Security Service that has legal authority to do surveillance of persons in Norway.

## APPENDIX 4 – Joint statement with four other oversight bodies: Strengthening oversight of international data exchange between intelligence and security services

# Strengthening oversight of international data exchange between intelligence and security services

*Written in cooperation between:*

### Belgian Standing Intelligence Agencies Review Committee

(Comité permanent de contrôle des services de renseignements et de sécurité / Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten)

[www.comiteri.be](http://www.comiteri.be)

### Danish Intelligence Oversight Board

(Tilsynet med Efterretningstjenesterne)

[www.tet.dk](http://www.tet.dk)

### Review Committee on the Intelligence and Security Services – The Netherlands

(Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten)

[www.ctivd.nl](http://www.ctivd.nl)

### EOS Committee – The Norwegian Parliamentary Intelligence Oversight Committee

(EOS-utvalget)

[www.eos-utvalget.no](http://www.eos-utvalget.no)

### Independent Oversight Authority for Intelligence Activities (OA-IA)

(Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND)

[www.ab-nd.admin.ch](http://www.ab-nd.admin.ch)



Belgian Standing Intelligence Agencies Review Committee



Danish Intelligence Oversight Board



Review Committee on the Intelligence and Security Services



NORWEGIAN PARLIAMENTARY OVERSIGHT COMMITTEE ON INTELLIGENCE AND SECURITY SERVICES



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

# 1. Content

Five European intelligence oversight bodies have begun a new form of cooperation. In this statement, we will:

Describe our project, which entailed each of us conducting an investigation into our respective countries' services' use of information regarding foreign terrorist fighters and sharing our methods, best practices and experiences.

- Address the challenges we met when overseeing international data exchange, including the risk of an oversight gap when intelligence and security services cooperate internationally.
- Identify ways to move forward towards strengthening oversight cooperation, for example through minimizing secrecy between oversight bodies so that certain information can be shared, in order to improve our oversight of international data exchange.

## 2. Introduction

Recent terrorist attacks, such as in Paris, Brussels and London, were carried out by persons directed, encouraged or inspired by ISIS, Al-Qaeda or similar terrorist groups. To identify and investigate the threat of homegrown and returning foreign terrorist fighters is an important task for intelligence and security services across Europe.

The threat of jihadist terrorism has become more complex and widespread in recent years. Investigating this threat requires international cooperation between intelligence and security services, either bilaterally or multilaterally. Such cooperation exists within Europe and with other countries. As this cooperation has intensified, the exchange of personal data between services has increased. The exchange of data with foreign services is part of the intelligence and security services' day-to-day activities. Data may be exchanged in various ways, either orally or in writing.

The oversight bodies have naturally followed the development of international cooperation between intelligence and security services. As our respective oversight mandate is strictly national, we have been concerned with the risk of an "oversight gap" occurring. In an ideal situation, the national systems of oversight would be complementary to each other: where one oversight body reaches the boundaries of its national mandate, the other is competent to effectively oversee. However, national legislation regarding exchange of data and the oversight of such exchanges may not meet these requirements. Moreover, international cooperation between intelligence services could develop in such a way, that national oversight can no longer keep up. Then an "accountability deficit" or "oversight gap" could emerge.

In light of this, the five oversight bodies from Belgium, Denmark, the Netherlands, Norway and Switzerland decided to start a joint project to exchange experiences and methods. Each of the oversight bodies conducted a national investigation into the international exchange of data on foreign terrorist fighters by the intelligence and security services they oversee.<sup>1</sup>

We conducted the national investigations more or less at the same time, each from our national context and within the framework of our national mandate. We have met regularly to compare investigation methods, interpret legal frameworks, discuss legal and practical problems and to collate our findings and conclusions. Classified information was not exchanged.

---

<sup>1</sup> The report from CTIVD (The Netherlands) about the investigation in English – <https://english.ctivd.nl/latest/news/2018/04/26/index>  
The annual reports from the Danish Intelligence Oversight Board in English – <http://www.tet.dk/redegorelser/?lang=en>

### 3. Current practices in oversight of data exchange

The participating oversight bodies oversee data exchange between intelligence and security services in several ways. We may

- assess cooperative relations or arrangements between intelligence and security services,
- assess the legitimacy and quality of specific data exchanges with foreign services,
- review the system of data exchange as a whole, including the safeguards,
- be involved in procedures concerning individual remedies and complaints.

Although the mandates of the oversight bodies are different, we all have a diverse range of instruments for overseeing international data exchange.

#### Assessment of the cooperative relationship

Oversight bodies may assess whether or not the cooperative relationship between their country's service and partner services in other countries meets certain criteria. Legislation governing the intelligence and security services may specifically state criteria for cooperation. Typically, criteria include the necessity for cooperation, the respect for human rights, the existence of legislation on data protection and/or reliability. The threshold for cooperating with services that do not meet the criteria should be high. The oversight bodies of Belgium, the Netherlands, Norway and Switzerland review the considerations made in that respect by their national services.

Cooperative relationships between the services can be based on agreements, for example letters of intent or memorandums of understanding. Such agreements are usually not legally enforceable but offer a practical framework on the exchange of data by services. Even the existence of some of these agreements is classified. Other agreements are made public by governments or the services. Nevertheless, they may draw the outline of the cooperative relationship by addressing issues like the purpose of the cooperation, how the cooperation is expected to function, limitations concerning disclosure to third parties or procedural aspects of the cooperation. The oversight bodies of all five countries may either review or report on whether these agreements comply with national laws and regulations.

#### Assessment of the legitimacy of specific data exchanges

Oversight bodies may assess whether individual data exchanges meet the legal requirements imposed by national laws and regulations.

The national legislations of our countries share certain characteristics, most notably the principles of necessity and proportionality. These shared principles originate from international legal frameworks such as the European Convention on Human Rights. The principle of necessity includes the requirement of a clear and legal purpose for the data exchange and the reasonable expectation that this purpose will be

met by exchanging the data. The principle of proportionality requires the service to balance the purpose of the exchange against the gravity of the infringement of fundamental rights. Most national legislation contains other requirements as well, such as the reasonableness, correctness, effectiveness and reliability of data exchange.

The internal policy of the services may provide additional rules for data exchange. Such policy may, for example, further specify which type of data exchange is allowed under which circumstances, which authorisation level is required and which use may be made of data received. When national law or bilateral and multilateral agreements are absent or silent on a specific matter, internal policy can provide additional safeguards.

### Assessment of the quality of specific data exchanges

Quality may relate to the content of the data or the format of the data. When it comes to content, quality means the data is correct, sufficiently clear and precise in its wording, confirmed by underlying data, up to date and with an indication of probability or reliability. As for format, quality aspects relate to the inclusion of a classification level, the date of exchange, the designated receiving partner service(s) and caveats regarding further use of data. All five oversight bodies can review the quality of data exchange in this respect.

Quality may also have a different meaning. It may relate to efficiency or effectiveness, that is whether the data exchange is relevant, whether the exchange happened in a timely manner and whether it fulfilled its purpose. This type of quality review is less common for oversight bodies. The oversight bodies of Belgium and Switzerland are expressly authorised to review whether data exchange has been effective and efficient.

### Review of the system of data exchange as a whole

Oversight bodies may adopt a broader approach when reviewing the legitimacy of data exchange. In reviewing certain multilateral cooperative frameworks, the oversight body in the Netherlands expressly looks at the system of data exchange as a whole and at the protection of individual rights within that system. Even though certain specific data exchanges may be legitimate, there can still be insufficient safeguards in the system to ensure the legitimacy of data exchange in the longer run. This type of review may help prevent unlawful data exchange between intelligence and security services.

One could take a similar approach when reviewing the quality of data exchange. When the purpose of exchanging data is to counter jihadism, the general quality of data exchange could be measured by investigating the amount of shared information that led to prosecution and conviction, or even to a direct prevention of a terrorist attack. However, measuring the usefulness of exchanged data in this way can be challenging. Such reviews are often initiated after a terrorist attack has occurred. Then the oversight body assesses if the relevant data had sufficiently and adequately been exchanged with national and international partners. The oversight body of Belgium has been involved in this type of review.

### Involvement in individual remedies and complaints

In general, oversight bodies in all five countries can receive complaints from individuals regarding the activities of the national intelligence and security services. Usually oversight bodies may offer non-legally binding opinions or recommendations to the intelligence and security services and/or the ministers who are politically responsible. The services usually comply with such opinions or recommendations. A

new law was adopted in the Netherlands in 2017, granting the oversight body the power to take binding decisions on complaints. This may also include ordering the exercise of a power to be terminated or the destruction or removal of processed data.

The secrecy that is necessary for the intelligence and security services to conduct their activities usually limits the right of the individual to access personal data. Some countries explicitly afford individuals the right to request the national oversight body to review the personal data their services have processed about them. In Denmark, any person may ask the Danish oversight body to investigate whether the security service is unlawfully processing personal data about them. In case of the military intelligence service, this review is limited to residents of Denmark. In both cases, the Danish oversight body may order the deletion of personal data regarding the applicant.

In Belgium the oversight body has an obligation to investigate all complaints that are not manifestly unfounded. The complainant will receive the findings of the investigation in general terms. The complainant then has the possibility to use these findings before the court or an administrative authority. In some specific cases the oversight body must give an official advice to a criminal court following a complaint and regarding two other topics of complaint (use of special methods and data protection), the committee may take binding decisions.

In Norway, residents have the same right to complain to the oversight body if a citizen suspects that he/she is subject to unlawful surveillance. However, the Norwegian oversight body does not have the authority to order deletion of data. In Switzerland, the Federal Data Protection and Information Commissioner (FDPIC) handles individual requests on data processing.

## 4. Challenges for oversight of international data exchange

In the course of our project we have found that the increased cooperation between intelligence and security services and the exchange of data between these services, especially on the multilateral level, may pose legal and practical challenges to the oversight bodies.

### Oversight does not cross national borders

National legislation often promotes the cooperation and exchange of information between intelligence and security services, both bilaterally and multilaterally. However, it usually does not provide a specific legal basis for oversight bodies to cooperate or exchange information on individuals. None of the five oversight bodies working together in the context of this common publication has an explicit legal basis to exchange data with another oversight body, certainly not when this information is classified.

Where intelligence and security services cross national borders, oversight bodies cannot. Oversight is limited to national mandates. This reflects one side of data exchange: either oversight will focus on the provision of data and its prior collection, or it will focus on the reception of data and its use. National oversight bodies will not independently be able to acquire a full picture of personal data exchange, let alone review the lawfulness of the entire process of exchange.

Such a limit to national oversight does not necessarily constitute an oversight gap. When oversight is exhaustive and effective on both sides of the border, no gap exists between the mandates of the oversight bodies. However, when it comes to cooperation between intelligence and security services - predominantly multilateral cooperation - the cooperation of oversight bodies is only as strong as its weakest link.

### The challenge of cooperation in the face of secrecy

Oversight bodies are limited to national rules on secrecy and cannot share and discuss the substance of their investigations beyond what is designated as public information. In practice, this means that oversight bodies have very limited insight into whether 'the other side' of data exchange is effectively overseen or whether an oversight gap exists. Therefore, oversight activities are not only unable to cross borders; they are also largely unable to share with other oversight bodies what occurs within their borders.

As the joint project between the five oversight bodies progressed, we found ourselves on numerous occasions aware of the fact that we were not even in a position to discuss matters known to us all, e.g. the content of agreements between the services we oversee. In addition, we became aware that what is public information in one country might be deemed confidential in another. This has led to difficulties for this project, limiting the possibility to reach substantial discussion on the matter in question.

## Assessment of necessity and proportionality

As mentioned above, oversight bodies continuously assess whether the exchange of data is necessary for a specific purpose and proportionate to the aim pursued. This requires that oversight bodies consider the level of protection of individual rights provided by the receiving service. As the volume of data exchanges and the number of foreign services with which the data is shared increase, this will be more and more challenging for oversight bodies. This test of necessity and proportionality can become more abstract and can lose value as the data exchanged is less specific or if it is exchanged within a larger group of intelligence and security services.

Different national legal regimes may include different legitimacy and quality standards for data collection, processing, retention and exchange. The level of protection of individual rights afforded by the service receiving the data is an important element in assessing the proportionality of a particular data exchange. This is not always easy to determine as intelligence and security services may not be open about all aspects of the legal framework in place and the standards they apply.

In the context of multilateral data exchange, common standards and definitions could help define under which circumstances data exchange is regarded as necessary and proportionate, and which minimum level of data protection needs to be in place to sufficiently safeguard individual rights. There is a common interest of all parties – intelligence and security services and oversight bodies – in having such common standards and a common interpretation of existing legal safeguards. This may also add to the legitimacy of the multilateral exchange in question.

## Some countries differentiate between citizens and foreigners

Some national legal frameworks offer nationals or residents a higher level of protection and more privileged access to individual remedies than foreigners or non-residents. The distinction between these groups may result in limited or no access to individual remedies for foreigners or non-residents whose data has been exchanged by the respective intelligence or security service.

A similar distinction may determine the mandate of the oversight body. Some oversight bodies only have the mandate to review data exchange with regard to nationals or residents. The provision of data with regard to other persons may lie beyond their reach. If no other oversight body may effectively review this part of the data exchange, an oversight gap exists.

## Means and methods of data exchange

Intelligence and security services exchange data in various ways. Some means and methods of data exchange pose further challenges for oversight bodies. An example of such a challenge is the informal exchange of data, and how to provide efficient oversight of data exchanged during conferences and meetings, by phone and so on. The increase in international data exchange may require oversight bodies to come up with more advanced methods of oversight, as it is no longer feasible to review each exchange of data. With regard to data protection, developments in multilateral data exchange may invoke responsibilities for each of the participating services as well as the oversight bodies. To safeguard individual rights adequately, it may be required that intelligence and security services discuss the standards they apply and work towards an equal minimum level of protection offered by all participating services.

## 5. Oversight of international data exchange – moving forward

Our project has shown us that the efforts of the intelligence and security services to find new ways to exchange data effectively, especially on a multilateral level, and the large increase in the volume of data exchanged, have in turn led to new challenges for the oversight bodies. This applies both to the limits of the oversight bodies' national mandates, their inability to adequately discuss international data exchange with other oversight bodies as well as to their own efforts to innovate their procedures and methods to ensure effective oversight.

National sovereignty and interests dictate the international cooperation between intelligence and security services. It is to be expected that, unlike other areas of international cooperation, oversight of the intelligence and security services will continue to be carried out by national oversight bodies. However, where intelligence and security services cross national borders, oversight bodies cannot. Consequently, oversight always reflects on one side of data exchange. Moreover, oversight bodies are largely unable to share with other oversight bodies their review of a particular data exchange. Because of these limits to national oversight, there is a risk of an oversight gap with regard to international data exchange by intelligence and security services. The question remains how to tackle such a risk.

By exchanging knowledge, experience and investigation methods, and by comparing their findings, conclusions and recommendations, oversight bodies may come closer together. Our experience is that this is precisely what this common project has accomplished. We have learned from each other's best practices, developed more understanding of each other's legal systems and we have built a level of trust. In order for oversight bodies to keep up with developments in international cooperation between intelligence and security services, we need to do just that: intensify our cooperation.

A valuable and necessary step towards closer cooperation is to minimize secrecy when sharing information between oversight bodies. At the minimum, oversight bodies could be able to discuss concrete bilateral and multilateral cooperative arrangements between the intelligence and security services they oversee. A logical additional step could be to share information with other oversight bodies that has already been shared by the intelligence and security services themselves. Once data has been exchanged, there is no need for oversight to lag behind. We do not suggest that all national secrecy limitations should be set aside, to the contrary. Cooperation between oversight bodies should take place within the limits and according to the standards set by national legislators.

Being able to discuss international cooperative arrangements and data exchange with other oversight bodies also comes with certain responsibilities. Adequately safeguarding individual rights while cooperating internationally, not only requires that intelligence and security services discuss the standards they apply and work towards an equal minimum level of protection offered by all participating services. It also requires oversight bodies to uphold such a minimum level of data protection and try to find common ground in interpreting existing legal safeguards.


Due to technological development and increased cooperation, the data exchange between intelligence and security services is intensifying, resulting in an increase of the number of individual data exchanges. The sheer volume of data exchanged may become a challenge in itself. To assess the legitimacy and quality of each individual exchange can become an overwhelming task for the oversight bodies. In addition to

conducting spot checks, it is becoming increasingly important to assess the system and framework for data exchange and the existence and functioning of safeguards for the protection of fundamental rights.

To do this effectively, oversight bodies will need to develop new methods. One way forward may be to increasingly use computerized automation and tools developed for conducting oversight of large volumes of data. In order to achieve this, oversight bodies need to expand their IT expertise and knowledge of the services' systems. Another way to facilitate a more effective oversight would be to take the needs of the oversight bodies into account when the services implement new systems and to strengthen mechanisms of internal and external control.

The oversight bodies of Belgium, Denmark, the Netherlands, Norway and Switzerland will continue to exchange methods and best practices, as well as discuss international challenges to oversight, and the best approaches to overcoming these challenges. We invite oversight bodies from other countries to join us in our efforts to limit the risk of an oversight gap and to improve oversight of international data exchange between intelligence and security services.

Signed in Bern on 22 October 2018,



**Mr. Serge Lipszyc**, Chair of the Belgian Standing Intelligence Agencies Review Committee



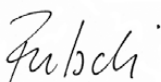
**Mr. Michael Kistrup**, Chair of the Danish Intelligence Oversight Board



**Mr. Harm Brouwer**, Chair of the Dutch Review Committee on the Intelligence and Security Services



**Mrs. Eldbjørg Løwer**, Chair of the EOS Committee – The Norwegian Parliamentary Intelligence Oversight Committee



**Mr. Thomas Fritschi**, Director of the Independent Oversight Authority for Intelligence Activities



*From left to right: Harm Brouwer (chair CTIVD, the Netherlands), Thomas Fritschi (director OA-IA, Switzerland), Eldbjorg Lower (chair EOS Committee, Norway), Serge Lypszyc (chair Comité I, Belgium). Michael Kistrup, chair of the Danish oversight board, could not be present when this photo was taken.*

## APPENDIX 5 – Act relating to oversight of intelligence, surveillance and security services<sup>102</sup>

### Section 1. The oversight area

The Storting shall elect a committee for the oversight of intelligence, surveillance and security services (the services) carried out by, under the control of or on the authority of the public administration (the EOS Committee). The oversight is carried out within the framework of Sections 5, 6 and 7. Such oversight shall not apply to any superior prosecuting authority.

The Freedom of Information Act and the Public Administration Act, with the exception of the provisions concerning disqualification, shall not apply to the activities of the Committee.

The Storting can issue instructions concerning the activities of the Committee within the framework of this Act and lay down provisions concerning its composition, period of office and secretariat.

The Committee exercises its mandate independently, outside the direct control of the Storting, but within the framework of this Act. The Storting in plenary session may, however, order the Committee to undertake specified investigations within the oversight mandate of the Committee, and observing the rules and framework which otherwise govern the Committee's activities.

### Section 2. Purpose

The purpose of the Committee's oversight is:

1. to ascertain whether the rights of any person are violated and to prevent such violations, 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 unduly harm the interests of society.
3. to ensure that the activities are kept within the framework of statute law, administrative or military directives and non-statutory law.

The Committee shall show consideration for national security and relations with foreign powers. The oversight activities should be exercised so that they pose the least possible disadvantage for the ongoing activities of the services.

The purpose is purely to oversee. The Committee shall adhere to the principle of subsequent oversight. The Committee may not instruct the bodies it oversees or be used by them for consultations. The Committee may, however, demand access to and make statements about ongoing cases.

### Section 3. The composition of the Committee

The Committee shall have seven members including the

chair and deputy chair, all elected by the Storting, on the recommendation of the Presidium of the Storting, for a period of no more than five years. A member may be re-appointed once and hold office for a maximum of ten years. Steps should be taken to avoid replacing more than four members at a time. Persons who have previously functioned in the services may not be elected as members of the Committee.

Remuneration to the Committee's members shall be determined by the Presidium of the Storting.

### Section 4. The Committee's secretariat

The head of the Committee's secretariat shall be appointed by the Presidium of the Storting on the basis of a recommendation from the Committee. Appointment of the other secretariat members shall be made by the Committee. More detailed rules on the appointment procedure and the right to delegate the Committee's authority will be stipulated in personnel regulations approved by the Presidium of the Storting.

### Section 5. The responsibilities of the Committee

The Committee shall oversee and conduct regular inspections of the practice of intelligence, surveillance and security services in public and military administration pursuant to Sections 6 and 7.

The Committee receives complaints from individuals and organisations. On receipt of a complaint, the Committee shall decide whether the complaint gives grounds for action and, if so, conduct such investigations as are appropriate in relation to the complaint.

The Committee shall on its own initiative deal with all matters and cases that it finds appropriate to its purpose, and particularly matters that have been subject to public criticism. Factors shall here be understood to include regulations, directives and established practice.

When this serves the clarification of matters or factors that the Committee investigates by virtue of its mandate, the Committee's investigations may exceed the framework defined in Section 1, first subsection, cf. Section 5.

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. The Committee can, however, exercise oversight in cases as mentioned in the first sentence when special reasons so indicate.

The ministry appointed by the King can, in times of crisis and war, suspend the oversight activities in whole or in part until the Storting decides otherwise. The Storting shall be notified of such suspension immediately.

<sup>102</sup> The EOS Committee's reference: 2016/147-6. The law was last changed in June 2017.

### Section 6. The Committee's oversight

The Committee shall oversee the services in accordance with the purpose set out in Section 2 of this Act.

The oversight shall cover the services' technical activities, including surveillance and collection of information and processing of personal data.

The Committee shall ensure that the cooperation and exchange of information between the services and with domestic and foreign collaborative partners is kept within the framework of service needs and the applicable regulations.

The Committee shall:

1. for the Police Security Service: ensure that activities are carried out within the framework of the service's established responsibilities and oversee the service's handling of prevention cases and investigations, its use of covert coercive measures and other covert information collection methods.
2. for the Intelligence Service: ensure that activities are carried out within the framework of the service's established responsibilities.
3. for the National Security Authority: ensure that activities are carried out within the framework of the service's established responsibilities, oversee clearance matters in relation to persons and enterprises for which clearance has been denied, revoked, reduced or suspended by the clearance authorities.
4. for the Norwegian Defence Security Department: oversee that the department's exercise of personnel security clearance activities and other security clearance activities are kept within the framework of laws and regulations and the department's established responsibilities, and also ensure that no one's rights are violated.

The oversight shall involve accounts of current activities and such inspection as is found necessary.

### Section 7. Inspections

Inspection activities shall take place in accordance with the purpose set out in Section 2 of this Act.

Inspections shall be conducted as necessary and, as a minimum, involve:

1. several inspections per year of the Intelligence Service's headquarters.
2. several inspections per year of the National Security Authority.
3. several inspections per year of the Central Unit of the Police Security Service.
4. several inspections per year of the Norwegian Defence Security Department.
5. one inspection per year of The Army intelligence battalion.
6. one inspection per year of the Norwegian Special Operation Forces.
7. one inspection per year of the PST entities in at least two police districts and of at least one Intelligence Service unit or the intelligence/security services at a military staff/unit.

8. inspections on its own initiative of the remainder of the police force and other bodies or institutions that assist the Police Security Service.
9. other inspections as indicated by the purpose of the Act.

### Section 8. Right of inspection, etc.

In pursuing its duties, the Committee may demand access to the administration's archives and registers, premises, installations and facilities of all kinds. Establishments, etc. that are more than 50 per cent publicly owned shall be subject to the same right of inspection. The Committee's right of inspection and access pursuant to the first sentence shall apply correspondingly in relation to enterprises that assist in the performance of intelligence, surveillance, and security services.

All employees of the administration shall on request procure all materials, equipment, etc. that may have significance for effectuation of the inspection. Other persons shall have the same duty with regard to materials, equipment, etc. that they have received from public bodies.

The Committee shall not seek more extensive access to classified information than warranted by its oversight purposes. Insofar as possible, the Committee shall show consideration for the protection of sources and safeguarding of information received from abroad.

The decisions of the Committee concerning what it shall seek access to and concerning the scope and extent of the oversight shall be binding on the administration. The responsible personnel at the service location concerned may demand that a reasoned protest against such decisions be recorded in the minutes. The head of the respective service and the Chief of Defence may submit protests following such decisions. Protests as mentioned here shall be included in or enclosed with the Committee's annual report.

Information received shall not be communicated to other authorised personnel or to other public bodies, which are not already privy to them unless there is an official need for this, and it is necessary as a result of the oversight purposes or results from case processing provisions in Section 12. If in doubt, the provider of the information should be consulted.

### Section 9. Statements, obligation to appear, etc.

All persons summoned to appear before the Committee are obliged to do so.

Persons making complaints and other private persons treated as parties to the case may at each stage of the proceedings be assisted by a lawyer or other representative to the extent that this may be done without classified information thereby becoming known to the representative. Employees and former employees of the administration shall have the same right in matters that may result in criticism being levied at them.

All persons who are or have been in the employ of the administration are obliged to give evidence to the Committee concerning all matters experienced in the course

of their duties.

An obligatory statement must not be used against any person or be produced in court without his or her consent in criminal proceedings against the person giving such statements.

The Committee may apply for a judicial recording of evidence pursuant to Section 43, second subsection, of the Courts of Justice Act. Sections 22-1 and 22-3 of the Civil Procedure Act shall not apply. Court hearings shall be held in camera and the proceedings shall be kept secret. The proceedings shall be kept secret until the Committee or the competent ministry decides otherwise, cf. Sections 11 and 16.

### Section 10. Ministers and ministries

The provisions laid down in Sections 8 and 9 do not apply to Ministers, ministries, or their civil servants and senior officials, except in connection with the clearance and authorisation of persons and enterprises for handling classified information.

The Committee cannot demand access to the ministries' internal documents.

Should the EOS Committee desire information or statements from a ministry or its personnel in other cases than those which concern the ministry's handling of clearance and authorisation of persons and enterprises, these shall be obtained in writing from the ministry.

### Section 11. Duty of secrecy, etc.

With the exception of matters provided for in Sections 14 to 16, the Committee and its secretariat are bound to observe a duty of secrecy.

The Committee's members and secretariat are bound by regulations concerning the handling of documents, etc. that must be protected for security reasons. They shall have the highest level of security clearance and authorisation, both nationally and according to treaties to which Norway is a signatory. The Presidium of the Storting is the security clearance authority for the Committee members. Background checks will be performed by the National Security Authority.

Should the Committee be in doubt as to the classification of information in statements or reports, or be of the opinion that certain information should be declassified or given a lower classification, the issue shall be put before the competent agency or ministry. The administration's decision is binding on the Committee.

### Section 12. Procedures

Conversations with private individuals shall be in the form of an examination unless they are merely intended to brief the individual. Conversations with administration personnel shall be in the form of an examination when the Committee sees reason for doing so or the civil servant so requests. In cases which may result in criticism being levied at individual civil servants, the examination form should generally be used.

The person who is being examined shall be informed of

his or her rights and obligations cf. Section 9. In connection with examinations in cases that may result in criticism being levied at the administration's personnel and former employees, said individuals may also receive the assistance of an elected union representative who has been authorised according to the Security Act with pertinent regulations. The statement shall be read aloud before being approved and signed.

Individuals who may become subject to criticism from the Committee should be notified if they are not already familiar with the case. They are entitled to familiarise themselves with the Committee's unclassified material and with any classified material they are authorised to access, insofar as this does not impede the investigations.

Anyone who submits a statement shall be presented with evidence and claims, which do not correlate with their own evidence and claims, insofar as the evidence and claims are unclassified, or the person has authorised access.

### Section 13. Quorum and working procedures

The Committee has a quorum when five members are present.

The Committee shall form a quorum during inspections of the services' headquarters as mentioned in Section 7, but may be represented by a smaller number of members in connection with other inspections or inspections of local units. At least two committee members must be present at all inspections.

In connection with particularly extensive investigations, the procurement of statements, inspections of premises, etc. may be carried out by the secretariat and one or more members. The same applies in cases where such procurement by the full Committee would require excessive work or expense. In connection with examinations as mentioned in this Section, the Committee may engage assistance.

### Section 14. On the oversight and statements in general

The EOS Committee is entitled to express its opinion on matters within the oversight area.

The Committee may call attention to errors that have been committed or negligence that has been shown in the public administration. If the Committee concludes that a decision must be considered invalid or clearly unreasonable or that it clearly conflicts with good administrative practice, it may express this opinion. If the Committee believes that there is reasonable doubt relating to factors of importance in the case, it may make the service concerned aware of this.

If the Committee becomes aware of shortcomings in acts, regulations or administrative practice, it may notify the ministry concerned to this effect. The Committee may also propose improvements in administrative and organisational arrangements and procedures where these can make oversight easier or safeguard against violation of someone's rights.

Before making a statement in cases, which may result in criticism or opinions, directed at the administration, the

head of the service in question shall be given the opportunity to make a statement on the issues raised by the case.

Statements to the administration shall be directed to the head of the service or body in question, or to the Chief of Defence or the competent ministry if the statement relates to matters they should be informed of as the commanding and supervisory authorities.

In connection with statements which contain requests to implement measures or make decisions, the recipient shall be asked to report on any measures taken.

### **Section 15. Statements to complainants and the public administration**

Statements to complainants should be as complete as possible without disclosing classified information. Information concerning whether or not a person has been subjected to surveillance activities shall be regarded as classified unless otherwise decided. Statements in response to complaints against the services concerning surveillance activities shall only state whether or not the complaint contained valid grounds for criticism. If the Committee holds the view that a complainant should be given a more detailed explanation, it shall propose this to the service or ministry concerned.

If a complaint contains valid grounds for criticism or other comments, a reasoned statement shall be addressed to the head of the service concerned or to the ministry concerned. Otherwise, statements concerning complaints shall always be sent to the head of the service against which the complaint is made.

Statements to the administration shall be classified according to their contents.

### **Section 16. Information to the public**

The Committee shall decide the extent to which its unclassified statements or unclassified parts of statements shall be made public.

If it must be assumed that making a statement public will result in the identity of the complainant becoming known, the consent of this person shall first be obtained. When mentioning specific persons, consideration shall be given to protection of privacy, including that of persons not issuing complaints. Civil servants shall not be named or in any other way identified except by approval of the ministry concerned.

In addition, the chair or whoever the Committee authorises can inform the public of whether a case is being investigated and if the processing has been completed, or when it will be completed.

Public access to case documents that are prepared by or for the EOS Committee in cases that the Committee is considering submitting to the Storting as part of the constitutional oversight shall not be granted until the case has been received by the Storting. The EOS Committee will notify the relevant administrative body that the case is of such a nature. If such a case is closed without it being submitted to the Storting, it will be subject to public disclosure when the Committee has notified the relevant administrative body that the case has been closed.

### **Section 17. Relationship to the Storting**

The provision in Section 16, first and second subsections, correspondingly applies to the Committee's notifications and annual reports to the Storting.

Should the Committee find that consideration for the Storting's supervision of the administration dictates that the Storting should familiarise itself with classified information in a case or a matter the Committee has investigated, the Committee must notify the Storting specifically or in the annual report. The same applies to any need for further investigation into matters which the Committee itself cannot pursue further.

The Committee submits annual reports to the Storting about its activities. Reports may also be submitted if matters are uncovered that should be made known to the Storting immediately. Such reports and their annexes shall be unclassified. The annual report shall be submitted by 1 April every year.

The annual report should include:

1. an overview of the composition of the Committee, its meeting activities and expenses.
2. a statement concerning inspections conducted and their results.
3. an overview of complaints by type and service branch, indicating what the complaints resulted in.
4. a statement concerning cases and matters raised on the Committee's own initiative.
5. a statement concerning any measures the Committee has requested be implemented and what these measures led to, cf. Section 14, sixth subsection.
6. a statement concerning any protests pursuant to Section 8 fourth subsection.
7. a statement concerning any cases or matters which should be put before the Storting.
8. the Committee's general experience from the oversight activities and the regulations and any need for changes.

### **Section 18. Procedure regulations**

The secretariat keeps a case journal and minute book. Decisions and dissenting opinions shall appear from the minute book.

Statements and notes, which appear or are entered in the minutes during oversight activities are not considered to have been submitted by the Committee unless communicated in writing.

### **Section 19. Assistance etc.**

The Committee may engage assistance.

The provisions of the Act shall apply correspondingly to persons who assist the Committee. However, such persons shall only be authorised for a level of security classification appropriate to the assignment concerned.

Persons who are employed by the services may not be engaged to provide assistance.

**Section 20. Financial management, expense reimbursement for persons summoned before the Committee and experts**

The Committee is responsible for the financial management of the Committee's activities, and stipulates its own financial management directive. The directive shall be approved by the Presidium of the Storting.

Anyone summoned before the Committee is entitled to reimbursement of any travel expenses in accordance with the State travel allowance scale. Loss of income is reimbursed in accordance with Act No 2 of 21 July 1916 on the Remuneration of Witnesses and Experts.

Experts receive remuneration in accordance with the fee regulations. Other rates can be agreed.

**Section 21. Penalties**

Wilful or grossly negligent infringements of the first and second subsections of Section 8, first and third subsections of Section 9, first and second subsections of Section 11 and the second subsection of Section 19 of this Act shall render a person liable to fines or imprisonment for a term not exceeding one year, unless stricter penal provisions apply.





NORWEGIAN PARLIAMENTARY  
OVERSIGHT COMMITTEE  
ON INTELLIGENCE AND SECURITY SERVICES



tdesign.no

**Contact information**

Telephone: +47 23 31 09 30

Email: [post@eos-utvalget.no](mailto:post@eos-utvalget.no)

[www.eos-utvalget.no](http://www.eos-utvalget.no)