STORTINGETS KONTROLLUTVALG
FOR ETTERRETNINGS-, OVERVÅKINGS- OG SIKKERHETSTJENESTE
EOS-UTVALGET

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 1 – 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.[1] 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

[1] 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.

POSTAL ADDRESS: P.O. Box 84 Sentrum, NO-0101 OSLO
OFFICE ADDRESS: Akersgata 8
TEL.: (+47) 23 31 09 30
EMAIL: post@eos-utvalget.no
WEBSITE: www.eos-utvalget.no

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'.[2] The Ministry refers to the fact that the oversight model was recently evaluated and upheld by the Storting.[3] Based on decisions made by the 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).[4] 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:[5]

> '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.[6]

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.[7] 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.[8]

---

[2] The Evaluation Report section 1.
[3] Consultation paper section 11.12.5.2.
[4] Consultation paper section 11.23.3.
[5] 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.
[6] *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).
[7] See the Evaluation Report sections 31 and 37.
[8] 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.[9] 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.[10]

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 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

[9] Consultation paper section 6.6.

[10] 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.

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'.[11]

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.[12] 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'.[13]

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.[14] 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:[15]

> 'NIS points out that the term "covert" in the prohibition refers to the actual collection of information, not subsequent searches and collation. The Committee does not agree with this interpretation. Active searches in and collation of information from selectors belonging to identified Norwegian legal persons obtained using covert collection capacities cannot be deemed to be anything other than targeted information collection targeting these persons, even if it is not done for the purpose of collecting information about the Norwegian legal persons in question. New information is always processed in connection with searches and analyses. This will apply regardless of NIS's expert assessment of relevance considered in isolation. The prohibition in the 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.'

[11] Consultation paper section 12.3.2.2.
[12] Consultation paper section 8.4.3.4.
[13] Consultation paper section 8.2.2.5 page 117.
[14] 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'.
[15] The 2016 special report, section 5.3.3.

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'.[16]

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'*.[17] 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[18] and continue to collect information through open sources belonging to the person who has returned.[19] 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.

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'.[20] 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

[16] The 2016 special report, section 5.2.3.2.
[17] Consultation paper section 8.4.3.4.
[18] Cf. the draft bill Section 4-2 seventh paragraph.
[19] Cf. the draft bill Section 4-2 final paragraph.
[20] The 2016 special report, section 1.5 on the Norwegian Intelligence Service's overriding considerations.

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*[21] 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'.[22] 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').

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.,[23] 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.

[21] 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').
[22] Cf. the Oversight Act Section 5 fifth paragraph.
[23] Document 7:1 (2013–2014), submitted on 16 December 2013.

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*[24] *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 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

[24] 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'.

In 2014, the Committee was made aware that the Norwegian Intelligence Service carries out searches in stored *metadata*[25] relating to Norwegian legal persons in Norway to find *selectors*[26] 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. [27]

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'.[28] 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.'

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',[29] it is difficult to see how collection from open sources would *not also* 'target' this person.

[25] 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.
[26] A selector can be a phone number, an email address, a Facebook username etc.
[27] The 2016 special report, section 6.
[28] Consultation paper section 9.5.6.3.
[29] Consultation paper section 8.8.2.

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',[30] 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'.[31] It will be an intelligence assessment to determine 'whether information can be collected at all' and 'how the information can be collected (methods)'.[32]

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, 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.'

[30] Consultation paper section 9.3.1.
[31] Consultation paper section 9.1.
[32] Consultation paper section 9.1.

The following is stated about preparatory measures in the consultation paper:[33]

> '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 Service's surveillance activities, and the Norwegian Police Security Service's remit and legal basis.[34]

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

[33] Consultation paper section 10.5.3.

[34] 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.

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'.[35]

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.*

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,[36] 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.[37] 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.

[35] Consultation paper section 10.6.2.
[36] Consultation paper section 11.12.3.8
[37] 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 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.

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.[38] 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

[38] The Evaluation Report pages 127 and 130.

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.

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,[39] the question is raised of whether the right to complain to the EOS Committee under Norwegian law is sufficiently broad.[40] After a discussion of the current right to complain,[41] 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.[42] As regards the Committee's oversight duties, the traditional interpretation will largely

[39] Consultation paper section 4.3.
[40] Consultation paper section 4.3.4.
[41] Consultation paper section 4.3.4.1.
[42] 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.'

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.[43] The Ministry concludes as follows:[44]

> '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 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'.[45]

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.[46]

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.

[43] The Ministry's discussion of jurisdiction is primarily found in section 4.1.3 of the consultation paper.
[44] Consultation paper section 4.1.3.
[45] The Ministry specifies that the Act will apply to all information collection due to practical considerations, not due to any legal obligations.
[46] 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.

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 in Norway on the sole condition that the complaint is against an EOS service.[47] 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:[48]

(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'.[49]

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.

[47] 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.

[48] 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.'

[49] 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.

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.

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.[50] 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.[51]

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

[50] 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.
[51] Recommendation No 418 to the Storting (2016–2017).

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.

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[52] 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 if 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,

Eldbjørg Løwer
Chair of the EOS Committee

[52] It is the Norwegian Police Security Service that has legal authority to do surveillance of persons in Norway.