Document 7:1

Special report from the Parliament Appointed Committee for Intelligence Oversight (the EOS Committee) on unlawful data storage in connection with the Norwegian Intelligence Service's use of the method facilitated bulk collection

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 EOS Committee hereby submits its report on unlawful data storage in connection with the Norwegian Intelligence Service's use of the method of facilitated bulk collection to the Storting.

The report is unclassified, cf. the Oversight Act Section 17 third paragraph. Pursuant to the Security Act, the issuer decides whether information is classified.
The report text has been submitted to the Norwegian Intelligence Service (NIS) for assessment. The NIS has also been given the opportunity to check that there are no factual errors or misunderstandings.

Oslo, 11 November 2025

Grete Faremo

Kristin Krohn Devold	Jan Arild Ellingsen	Olav Lysne
Hege Solbakken	Åsa Elvik	Geir Sunde Haugland
		Henrik Gudmestad Magnusson

1. The EOS Committee's review of the legality of the NIS' use of facilitated bulk collection

The EOS Committee conducts legality review of the intelligence, surveillance and security services, also known as the secret services. The purpose of the Committee's oversight is to ascertain whether the rights of any person are violated and to prevent such violations, to ensure that the services' activities do not unduly harm the interests of society, and that the services' activities are kept within the framework of statute law, directives and non-statutory law. This remit is set out in the Oversight Act.

The Storting has emphasised that the Committee has a distinct role in overseeing the NIS's facilitated bulk collection of cross-border electronic communication (facilitated bulk collection). This distinct role is described e.g. in the Act relating to the Norwegian Intelligence Service (the Intelligence Service Act) Section 7-11, in which the Committee is charged with the continuous oversight of the NIS's compliance with the provisions of the Intelligence Service Act's chapter on facilitated bulk collection.

The method means that the NIS can collect electronic communication, such as emails, telephone or internet traffic, that is transmitted across the Norwegian border through fibre-optic cables. Among other things, the Committee checks which information the NIS collects by this method, which searches the service carries out, and whether the service complies with the limitations imposed through court warrants.

The EOS Committee reports annually to the Storting in the form of an annual report.
The Committee may submit a special report to the Storting if 'matters are uncovered that should be made known to the Storting immediately', cf. the Oversight Act Section 17 third paragraph. It is established practice that the Committee also submits reports to the Storting on matters of a certain scope and importance. This is such a matter.

In October 2025, the EOS Committee decided to submit a special report on unlawful storage of data obtained through facilitated bulk collection.

2. Background to the special report

On 20 December 2024, as part of the Committee's oversight of facilitated bulk collection, the Committee asked the NIS about the service's metadata storage arrangements seen in relation to the Intelligence Service Act.

The Committee received a reply on 4 February 2025. The topic was brought up in several of the Committee's subsequent inspections of the NIS, where the NIS briefed the Committee about challenges relating to the storage of metadata. In early September 2025, the NIS informed the Committee that the service had decided to disable parts of the system for storage of metadata from facilitated bulk collection. The Committee asked some follow-up questions in a letter dated 11 September 2025, and it received a reply on 30 September 2025.

The Committee sent its concluding statement to the NIS on 14 October 2025. The service's response of 31 October 2025 regarding the question of classification, consisted of an unclassified document that the service wanted to have included as an appendix to the Committee's special report. The letter is enclosed as Appendix 1 to this report.

3. The applicable legal framework for the Committee's statement to the NIS

The Intelligence Service Act distinguishes between metadata and content data in the context of facilitated bulk collection. Metadata is defined in Section 7-7 of the Intelligence Service Act, which states that 'metadata refers to data which describes other data or which contains additional information linked to data, including data which describes the contents' format, the sender and recipient, or the communication's size, position, timestamp or duration.'

Content data is defined in Section 7-9 of the Act, which states that 'content data is data which is not metadata.'

This distinction has a bearing on the due process protections that apply. The court review for the two data types differ slightly. The Intelligence Service Act Section 7-7 allows the NIS to store metadata in bulk[1] subject to court authorisation for mirroring[2] pursuant to Section 7-3 of the Act. Searches in the stored metadata require additional court authorisation, cf. the Intelligence Service Act Section 7-8.

Storage of content data also requires court authorisation, cf. the Intelligence Service Act Section 7-9. Storage of content data must take place in a targeted manner within the scope of the court's authorisation, and content data may not be stored in bulk as is allowed for metadata.

4. The Committee's statement to the NIS

4.1 Regarding the distinction between metadata and content data

The Committee has experienced through oversight of the NIS's metadata storage that the definition of metadata set out in the Intelligence Service Act and the service's approach to this definition give rise to challenges for the oversight. One such challenge is that there will always be cases where a category of data that as a rule will constitute metadata, could in practice sometimes include content data. The Committee has also experienced challenges with the metadata list mandated by the Intelligence Service Act Section 7-7 second paragraph. In its current form, the list describes the metadata stored by the NIS at any time. The challenges associated with this list include the fact that it does not at present contain enough information to allow for proper assessments of all types of data on the list, its large volume, and the fact that regular changes are made to the list without being adequately documented.

In its statement to the NIS dated 14 October 2025, the Committee pointed out that the legislators have introduced a distinction between content data and metadata because collecting the content of people's communication is normally considered more intrusive, and such data is given a stronger protection. This is expressed by the more stringent regulation in the Act on content data, as well as by the additional due process protection provided by court review.

The Committee also stated that it is important that the NIS maintains the purpose of the distinction between metadata and content data when making concrete assessments about whether a given category of information constitutes metadata or content data. The Committee wanted to clarify the oversight challenges in this area, which are connected to both the wording of the Act and the NIS's practice. The Committee stated that it would address this issue in the time ahead and raise it with the Committee for the Evaluation of the Norwegian Intelligence Service Act.

Based on the above, the Committee also remarked to the NIS that unanswered questions remained regarding interpretation of the law concerning the storage of metadata by the NIS in the facilitated bulk collection system and the NIS practice, and that the Committee will continue its work with these questions.

4.2 Criticism of the NIS's storage of email subject fields

The Lysne II Committee discussed the distinction between metadata and content data in section 9.2.4 of its report on digital border defence, including how this distinction applies to emails. The report referred to the fact that emails contain a 'subject' field. Although this is a field that *describes* the email's content, the Lysne II Committee was of the opinion that it must be considered part of the content.

[1] The collection of large quantities of data where a significant proportion of the information is considered irrelevant for intelligence purposes.

[2] Mirroring entails the NIS receiving a copy of data in transit from the cross-border communication streams transmitted through the selected cables. The mirrored data are processed in accordance with the Intelligence Service Act, for example by storing metadata from the communication.

The NIS has identified email subject field data stored in its metadata storage. Such data are considered content data both by the Committee and by the service itself, and the storage is thus in breach of Section 7-7 of the Act.

In its statement to the NIS, the Committee stated that the storage of content data in the metadata storage constitutes a breach of the Intelligence Service Act Section 7-7, and that the distinction between storage of metadata in bulk and targeted storage of content data is fundamental to due process protection in that the law only permits content data to be stored based on targeted collection authorised in advance by a court. The Committee therefore criticised the NIS for unlawfully storing email subject fields, cf. the Intelligence Service Act Section 7-7, cf. Section 7-9.

The NIS has informed the Committee that the service did not retrieve statistics on the scope of 'email subject fields' storage before deleting the data in question.

4.3 Criticism of the Intelligence Service's work to prevent the storage of email subject fields

As referenced above, the Committee sent the NIS a letter, dated 20 December 2024, asking how the system takes account of the Intelligence Service Act's definition of metadata, how the service checks and ensures that the definition set out in the Act is complied with, and how the service checks the content of the metadata list against the legal definition.

The NIS disabled a module that stored data from email subject fields in January 2025. In an internal control report from April 2025, the service identified another two modules that also contained data of the email subject fields type. The NIS informed the Committee that it continued to store metadata during the period from May to August in an effort to identify potentially problematic data storage. The service found that data from email subject fields were still being stored and made further adjustments in late August/early September 2025 to disable the remaining functionality that caused this type of data to be stored.

In its statement of 14 October 2025, the Committee expressed its understanding that the implementation of the facilitated bulk collection system is a complex process and that knowledge of the tools must be gained through experience. The Committee also acknowledged that the NIS took action by deciding to partially discontinue storage and delete data that had already been stored in this area. However, the Committee nevertheless considered that the provisions of the Act that allow for storage of metadata and prohibit the storage of content data impose requirements regarding the procedures used by the NIS in its technical implementation of the permitted storage. The Committee also referred to the fact that the Intelligence Service Act Section 7-10 first paragraph requires the Intelligence Service to take systematic measures to ensure that activity pursuant to this chapter is conducted in compliance with the Act.

Parts of the metadata processing system are based on acquired software that was not originally tailored for the NIS's organisation, which requires special investigation and evaluation in relation to the processing and storage permitted under the Intelligence Service Act.

With reference to the issues highlighted in the service's internal control report in April, the Committee pointed out that the service could have been expected to consider the need for further action to be taken sooner.

Based on the above, the Committee's statement criticised the NIS for not having taken sufficient action to ensure compliance with the Intelligence Service Act when implementing and initiating metadata storage in the facilitated bulk collection system.

Appendix:
Letter from the Intelligence Service to the EOS Committee dated 31 October 2025

The EOS Committee – The Parliament Appointed
Committee for Intelligence Oversight
P.O. Box 84 Sentrum
NO-0101 OSLO

Date	Our ref.	Your/previous reference
31 October 2025		

Regarding criticism of production of metadata in the facilitated bulk collection system

1. Introduction

Based on its oversight of the NIS's production of metadata in the facilitated bulk collection system, the EOS Committee has concluded by expressing criticism against the service for two issues relating to this metadata production: for the unlawful storage of email subject fields in the metadata storage, and for not having taken sufficient action to ensure compliance with the Intelligence Service Act when implementing and initiating metadata storage in the facilitated bulk collection system.

2. General comments

I take the criticism seriously and take note of it, and I agree that the NIS has, objectively speaking, stored a type of data that we should not have stored. I agree with the EOS Committee that the service likely could have conducted further investigations and taken further measures before and during the testing and development phase.

However, I would like to emphasise the following:

- Statutory compliance has been a governing consideration in all our decisions and actions in the matter.
- Email subject fields have never been the subject of analysis or production for intelligence purposes. The problem relates exclusively to the storage.
- The storage of email subject fields was identified as a problem by the NIS itself based on internal control. The EOS Committee has been kept informed on a continuous basis.
- Preventive action was taken immediately upon discovery of potential non-conformities. This happened before the service had reached a conclusion regarding how to characterise email subject fields.

Postal address:
P.O. Box 193
Alnabru Bedriftssenter
NO-0614 OSLO

Office address:
Lutvannsveien 60
NO-0616 OSLO

Civilian phone/fax:
+47 23 09 40 00
+47 23 09 44 66

Email/Website:
post.etterretningstjenesten@mil.no
www.forsvaret.no

8090916cdb088a32c8418fc40ff50f42

- There was a need to keep the dataset for a while in order to conduct technical investigations to determine what had happened and whether other types of data had been stored unlawfully. Once the dataset was no longer needed for technical investigation, the entire dataset that included this type of data was deleted.

3. More about the central aspects of the case

I see a need to give a somewhat more detailed account of the facts of the case in order to ensure that the case is properly elucidated.

3.1. About the most important actions taken

The criticism expressed by the EOS Committee is based on the NIS's own findings and assessments related to the storage of email subject fields. It is thus the service's own assessment that this type of data does not fall within the Intelligence Service Act's definition of metadata and that it therefore cannot be stored. The fact that the storage that took place constitutes a non-conformity has not been disputed. The EOS Committee has been kept informed about the case throughout.

I consider this case to be a confirmation that the system set out by the legislators in the Intelligence Service Act functions as intended. The external oversight and the NIS's internal control are working. The EOS Committee's continuous oversight of facilitated bulk collection is working in that the Committee has been able to monitor and evaluate the service's work and actions in the case more or less in real time. The Committee and its secretariat have their own access cards to the NIS's premises and has a dedicated space at the NIS with several workstations from which they can access the NIS systems and the information within them.

The storage of email subject fields was identified as a potential issue through the NIS's internal control in January 2025. It has been crucial to the service that the system developed should be in keeping with the applicable statutory framework. In addition to considering which measures to take specifically in relation to the storage of email subject fields, the service therefore needed to look at this issue at a system level. Compliance with the legal requirements applicable to the facilitated bulk collection system has been a governing consideration for all actions and measures taken in this case.

I decided to implement internal measures without delay to ensure that the metadata production issues that were unresolved at the time would not, when seen in relation to the service's legal framework, give rise to consequential errors in other parts of the facilitated bulk collection system.

Preventive measures were implemented as soon as the storage of email subject fields was identified as a potential issue in order to prevent storage in violation of the Intelligence Service Act, and this was done before the service had concluded that the storage of this type of data was indeed problematic. These measures included disabling the functionality that produced this type of data. Once the NIS subsequently concluded that email subject fields were to be considered content data, further action was taken to prevent email subject fields from appearing in any results from operational queries in metadata based on court orders.

The service's subsequent investigations in the case found that further corrective action was needed in relation to storage of email subject fields in order to fully disable this production. As mentioned above, this should ideally have been identified at an earlier stage, but the internal measures implemented to isolate the problem and reduce the risk of consequential errors in the system were deemed to be adequate while work on the case was ongoing.

8090916cdb088a32c8418fc40ff50f42

The storage of email subject fields has now been discontinued, and the dataset in which this type of data might be stored was deleted in its entirety in mid-September 2025. In any case, this type of data was never the subject of any analysis or production for intelligence purposes. The reason why the entire dataset was not deleted immediately was that we needed to carry out technical analyses of the dataset to ensure that no other problematic types of data were being processed as metadata. The NIS has not found other data types stored in connection with metadata storage to constitute content data.

Considering the complexity of the case in question and the framework within which the NIS must resolve cases of doubt regarding the storage of metadata, I believe that this case has, despite the matters that warrant criticism, been handled with the appropriate measures – including by taking immediate action to isolate the effect of the problems identified.

3.2. Reasons for the non-conformity

3.2.1. Introduction

The facilitated bulk collection system is a complex system that remains under construction and development. The procurement is scheduled to be completed by 2026. It was to be expected that some challenges of the nature on which the Committee's criticism is based would be encountered. I agree with the Committee that when the service first identified the problem, it should have dedicated additional resources to investigating whether there could be other unidentified elements in the processing system that would result in this type of data still being stored.

In most cases, it is relatively simple for the NIS to determine which types of data to respectively categorise as metadata and content data. However, I would like to emphasise that there are no definitive answers to this question. As is generally the case with legislation, there is also room for interpretation in the definition of metadata found in the Intelligence Service Act Section 7-7. The Intelligence Service Act and its preparatory works include no detailed guidelines as to which specific types of data fall within the definition in the Act, although they do give some examples. The legislators have acknowledged that cases of doubt will arise, and the solution prescribed is that the NIS is obliged to keep a list of metadata. Such a list has been available to the EOS Committee for as long as data have been stored.

The NIS cannot assume that the way in which data behave in internet traffic will fit neatly with the legal framework that applies to the service. We found it to be a good starting point for this work to look to established standards that define how data occur in network communication, insofar as such standards exist. The basic functionality of the service's processing system is therefore based on such internationally recognised standards – specifically, the RFC standards[1] are the most relevant in this context. Such standards normally distinguish between the solutions that allow information to be sent and delivered to a recipient and standards for the actual information transmitted. By such standards, email subject fields will not be part of the content of the message, but accompany it. It will thus be a natural starting point for data processing systems based on such standards to categorise this datatype as metadata.

3.2.2. More about where to draw the line between metadata and content data

In principle, email subject fields can be considered data describing other data. The NIS has nevertheless concluded that email subject fields are to be considered content data.

[1] The IETF (Internet Engineering Task Force) is a major international collaboration that defines standards for the internet through Requests for Comment (RFCs). The RFCs are freely available numbered publications.

The core of the facilitated bulk collection system is based on the proposals made by the Lysne II Committee in its report, which assumes precisely that although a subject field can be said to describe the content, see the definition of metadata, it must nevertheless be considered content data. The NIS has found no grounds to dispute this view in its continued work on metadata based on the Intelligence Service Act and its preparatory works. However, arguments can be made in support of both views, and it is not a foregone conclusion. The Lysne II Committee's statement concerning email subject fields was not included in or referred to in the proposition to the Storting that formed the basis for the bill.

Viewed in relation to how data behave in network communication, this shows that where to draw a sensible distinction between metadata and content data on the basis of how data behave in a technological perspective does not necessarily correspond to where the legislators have chosen to draw the distinction from a legal perspective. The considerations that are of relevance in a legal context may differ from those that are relevant in a technological context.

Both technical standards and the Lysne II Committee's report use an envelope analogy in which the envelope represents metadata and the letter inside represents content data. Although the envelope analogy can be useful as a teaching tool to explain the subject, our experience suggests that it is probably not sufficiently timeless and precise to understand the overall complexity of such a system. The service will in any case have to adapt to technological developments and the use of data.

3.4. Consequences of the measures

The totality of measures that have been required in this case have been at the cost of the operationality and effectiveness of the system, and the system-oriented technical measures found to be necessary will also affect parts of the system that are unproblematic from a legal perspective. However, these considerations are of secondary importance compared with full compliance with the law.

It is important that the facilitated bulk collection system becomes fully operational as soon as possible, within the limits of the applicable statutory framework. We are now facing a threat situation that is more serious than it has been for several decades. Facilitated bulk collection can help to identify, combat and attribute cyber-espionage and cyberattacks targeting Norway, threat actors using Norwegian digital infrastructure against targets in other countries, terrorism plans, information influence operations by foreign states, foreign states' assassination plans , foreign military operations on Norwegian territory, online communication between foreign intelligence services and their agents and sources, circumvention of Norwegian export limitations, bring forth information about foreign investments and acquisitions in Norway that represent a security challenge, and uncover other development trends, events and circumstances in other states that could challenge our national security interests.

In particular, the introduction of facilitated bulk collection will help to significantly strengthen our national situational awareness within the cyber domain and cybersecurity and strengthen our counterterrorism and counterintelligence capabilities. This will in turn strengthen our ability to identify, monitor and counter new and unknown threat actors. The few queries conducted with court orders during the development phase have already demonstrated facilitated bulk collection's considerable potential to strengthen the security of Norway and its population. In one case, facilitated bulk collection helped to avert a serious terrorist threat against targets in Norway. However, I would like to emphasise once again that email subject fields have never been the subject of analysis or production for intelligence purposes.

8090916cdb088a32c8418fc40ff50f42

I have made it a priority to assign the resources required to find quick and satisfactory solutions to the challenges that emerged in this case that maintain the system's potential while being in full compliance with the law. This work will take some time, and I cannot rule out the possibility that legislative amendment may be required. However, it is my intention to keep to the progress schedule in all material respects.

3.5. The way forward

The overall processing systems used by the NIS are developed to accommodate differentiated processing rules, and the service is thus not at the mercy of its technological starting point. This nevertheless requires complex adaptations to be made to the processing systems when encountering a global telecommunications and internet landscape in a state of constant change. It is noted that this case concerns one type of data from one form of communication, namely emails, and that there are countless other forms of communication. This involves an enormous variation in terms of standards and protocols, and consequently also in how different types of data occur in communication.

The system has been under development over some time. However, the NIS can never consider this work to be completed. I expect to encounter other problems during the system's further development and operation as in other aspects of the NIS's activities. I will align the service's efforts towards continued work to identify and deal with any cases of doubt that come up, including those stemming from possible dissonance between technology and law. At the same time, I will strive to enable the service to highlight this dissonance in its communication with its superior authorities and the EOS Committee. If regulatory amendment is required, I will propose such amendments.

The reputation and credibility of the NIS is entirely dependent on effective democratic oversight. In my experience, the service's dialogue with the EOS Committee is constructive, which is important in enabling the service to properly accommodate the Committee's oversight requirements. I will facilitate the continuation of this good dialogue. We will continue our work to ensure that the facilitated bulk collection system functions as well as possible within the statutory requirements and to further facilitate effective external oversight.

4. Conclusion

In order to ensure that the case is as well elucidated as possible for the Storting, I request that the service's perspective on the case, as expressed in this letter, be included in or appended to the special report to the Storting.

Nils Andreas Stensønes
Vice-Admiral
Head of the Norwegian Intelligence Service

8090916cdb088a32c8418fc40ff50f42