Registered at the EFTA Court under NºE-5/26-01 on 23 day of March 2026.

BORGARTING LAGMANNSRETT

Dok 134

EFTA Court
1 rue du Fort Thüngen
L-1499 Luxemburg
Luxembourg

Deres referanse	Vår referanse	Dato
	25-099380ASD-BORG/01	23.03.2026

Request for an Advisory Opinion in Case No 25-099380ASD-BORG/01, civil case, appeal against judgment: The Tinius Trust Foundation and Tom Erik Thorsen – The Norwegian Government, represented by the Ministry of Defence

1. Introduction

Borgarting Court of Appeal (Borgarting lagmannsrett) hereby requests an Advisory Opinion from the EFTA Court in Case No. 25-099380ASD-BORG/01, pursuant to Section 51a of the Norwegian Courts of Justice Act (domstolloven) and Article 34 of the Agreement between the EFTA States on the Establishment of a Surveillance Authority and a Court of Justice.

The case currently pending before the Court of Appeal concerns, inter alia, the legality of Chapters 7 and 8 of the Act of 19 June 2020 No. 77 relating to the Norwegian Intelligence Service (the Intelligence Service Act), which govern the facilitated collection of cross-border electronic communications. The principal question under EEA law is whether these provisions fall within the scope of application of Articles 5 and 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive 2002/58/EC).

Central to the case and the parties' submissions is the preliminary ruling of the Court of Justice of the European Union (CJEU) of 6 October 2020 in Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others* (EU:C:2020:791) (*La Quadrature du Net)* (LQN), which clarified the interpretation of Article 15(1) of Directive 2002/58/EC.

The parties disagree on the scope of application and interpretation of Article 15(1), as elucidated by the CJEU in *La Quadrature du Net.*

The request seeks clarification on the following issues:

Postadresse	Sentralbord	Saksbehandler	Bankgiro	Organisasjonsnummer
Postboks 2107 Vika, 0125 Oslo	21 55 80 00	Terje Jørgensen		926721356
Kontoradresse	**Telefaks**	**Telefon**	**Ekspedisjonstid**	**Internett/E-post**
Keysers gate 13, 0165 Oslo		21558574	0800-1545 (1500)	http://domstol.no/borgarting borgpost@domstol.no

- Whether the scope of application of the EEA Agreement and Directive 2002/58/EC encompasses national legislation in the defence sector adopted for the purpose of safeguarding national security interests.

- If the above mentioned national legislation falls within that scope; the relevance of the LQN-criteria to national legislation authorising the facilitated collection of cross-border electronic communications for foreign intelligence purposes.

- If the LQN- criteria are applicable; whether they must be expressly laid down in national legislation (statutory law) to satisfy the proportionality requirement in Article 15(1) of Directive 2002/58/EC, as interpreted by the CJEU in *La Quadrature du Net*

2. Parties to the case

The parties to the case before the Borgarting Court of Appeal are:

Appellant 1:	The Tinius Trust Foundation (Stiftelsen Tinius) Olav Vs gate 5, 0161 Oslo
Appellant 2:	Tom Erik Thorsen Dalsbottenlia 8, 3726 Skien
Third Party Interveners:	1. Norwegian Editor's Association 2. Norwegian Press Association 3. Norwegian Journalist Union 4. Media Companies' Association 5. The Norwegian Publishers' Association 6. Norwegian PEN 7. Norwegian Non-fiction Writers and Translators Association
Counsel:	Advocate Jon Wessel-Aas and advocate Emanuel Feinberg Advokatfirmaet Glittertind AS Dronning Mauds gate 15, 0250 Oslo
Respondent:	The Norwegian Government, represented by the Ministry of Defence (staten ved Forsvarsdepartementet) Po.box 8005 Dep, 0030 Oslo
Councel:	Advocate Ida Thue Office of the Attorney General (Civil Affairs) P.O. Box 8012 Dep, 0030 OSLO

3. Facts of the case

3.1 The current proceedings before the Norwegian courts

In March 2024 The Tinius Trust Foundation («The Foundation») and Tom Erik Thorsen («Thorsen») took legal action against the Government before the Oslo District Court. The Norwegian Editor's Association, The Norwegian Press Association, The Norwegian Journalist Union, The Media Companies' Association, The Norwegian Publishers' Association, Norwegian PEN and Norwegian Non-fiction Writers and Translators Association declared third party intervention.

The case concerned the legality of Sections 6-9 and 6-10 and Chapter 7 of the Norwegian Intelligence Service Act. The Foundation and Thorsen submitted the following claim before the District Court:

1. The Government, represented by the Ministry of Defence, is not entitled to collect, store or process electronic communications through facilitated collection pursuant to Chapter 7 of the Intelligence Service Act.
2. The Government, represented by the Ministry of Defence, is not entitled to collect, store or process electronic communications collected in bulk through midpoint collection and endpoint collection pursuant to Sections 6-9 and 6-10, respectively, of the Intelligence Service Act..

The Government, as its principal submission, moved for dismissal of the appellants' claim under item 2. In all other respects, the Government submitted that it should be acquitted.

By judgment of 26 March 2025, the Oslo District Court dismissed the appellants' claim under item 2. Otherwise, the Government was acquitted.

The Foundation and Thorsen have appealed the judgment to Borgarting Court of Appeal. The Court of Appeal decided the appeal against the District Court's dismissal ruling on the basis of written proceedings. In its ruling of 16 February 2026 Borgarting Court of Appeal decided that the Foundation's claim shall be brought before Oslo District Court and heard on its merits. Thorsen's appeal was dismissed. The Foundation's claim under item 2 of its submission is not part of this request for an advisory opinion.

The request for an advisory opinion concerns the Foundation's and Thorsen's claim under item 1 relating to Chapter 7 of the Norwegian Intelligence Service Act.

3.2 The background of the Norwegian Intelligence Service Act

The Norwegian Intelligence Service Act of 19 June 2020 no. 77 applies to the Norwegian Intelligence Service, cf. section 1-1. The Norwegian Intelligence Service is the national foreign intelligence service and forms part of the Norwegian Armed Forces, cf. Section 2-1. Its mandate is to collect and analyse information on foreign affairs which, in brief, may

contribute to safeguarding national security interests, cf. Chapter 3 on the tasks of the Norwegian Intelligence Service.

The new Norwegian Intelligence Service Act (2020) replaced the previous Intelligence Service Act of 20 March 1998 No. 11.

The preparatory works include, inter alia, Prop. 80 L (2019–2020), Prop. 92 L (2022–2023) and the Report of 26 August 2016 *Digital Border Defence (Digitalt grenseforsvar)* prepared by the Government-appointed Lysne II Committee. To a large extent, the 2020 Act continued and codified the previous legal framework. However, the methods for information collection were not regulated under the 1998 Act. This raised the question of whether Norwegian legislation complied with the requirement under the European Convention on Human Rights that interferences with human rights by public authorities must be "in accordance with the law". Against this background, the Government proposed new legislation in which methods for information collection were explicitly and exhaustively regulated.

The provisions relating to general methods of information collection are set out in Chapter 6 of the Intelligence Service Act. Under these provisions, the Norwegian Intelligence Service is not authorised to require electronic communications providers to facilitate the collection of information. As mentioned above, the request for an advisory opinion does not concern these provisions.

The 2020 Act introduced new provisions in Chapters 7 and 8 concerning the facilitated collection of cross-border electronic communications. These provisions authorise the Norwegian Intelligence Service to order electronic communications providers to facilitate the collection and subsequent processing of information. This extended the authority of the Norwegian Intelligence Service compared to previous law.

Under the previous law, the Norwegian Intelligence Service was not authorised to issue facilitation orders to electronic communications providers. Consequently, the Service did not have access to cross-border internet communications transmitted via fibre-optic cables, as such access - due to technological constraints - requires provider facilitation. Since the predominant share of cross-border communications to and from Norway is transmitted via fibre-optic cables, this meant that the Intelligence Service lacked access to an important source of information.

The collection of cross-border electronic communications is subject to special regulation because of the need for provider facilitation and because such collection will, to a large extent, include communications between persons located in Norway. This is due to the fact that domestic internet traffic in general is routed via servers abroad. Hence, purely domestic communications will be included in the collection of cross-border communications.

The new Norwegian Intelligence Service Act entered into force on 1 January 2021.

Shortly before this, on 6 October 2020, the CJEU delivered its judgments in *La Quadrature du Net* and Case C-623/17 (*Privacy International*), concerning the interpretation of Directive 2002/58/EC.

At the same time, the Grand Chamber of the European Court of Human Rights (ECtHR) had two pending cases concerning Swedish and British legislation authorising bulk interception of electronic communications for foreign intelligence purposes.

Following the CJEU judgments and pending the Grand Chamber judgments of the ECtHR, the Norwegian Government decided to postpone the entry into force of Chapters 7 and 8 of the Intelligence Service Act.

On 25 May 2025, the ECtHR delivered two Grand Chamber judgments concerning bulk interception regimes: Case 35252/08 *Centrum för Rättvisa v. Sweden* and Joined cases 58170/13, 62322/14 and 24960/15 *Big Brother Watch and Others v. the United Kingdom*.

On the basis of the judgments from the CJEU and ECtHR, the Norwegian Government assessed the need for revisions to Chapters 7 and 8. Following a legislative process, the Government submitted a proposal with revised provisions to the Norwegian Parliament (Prop. 92 L (2022–2023). The revisions included, inter alia, special conditions for the facilitated collection of cross-border electronic communications in Section 7-3 and provisions on judicial oversight in Chapter 8.

The current provisions on the facilitated collection of cross-border electronic communications entered into force on 1 October 2023.

4. Relevant Norwegian law; The Intelligence Service Act

As explained above, the facilitated collection in bulk of cross border electronic communications is regulated in the Norwegian Intelligence Service Act, which relates to the Norwegian Foreign Intelligence Service.

An official English translation of the Intelligence Service Act is to be found on https://eos-utvalget.no/wp-content/uploads/2021/06/Official-translation-of-the-Act-relating-to-the-Norwegian-intelligence-service.pdf. This translation is used in the following. The official translation has not been updated after the revisions of the act in 2023. Hence, the revisions of Sections 7-2 and 7-3 are translated by the court and the parties. Also the statements from the preparatory works which are quoted below, are translated by the court and the parties.

The specific regulation of facilitated collection in bulk of cross-border electronic communications, is found in Chapter 7 (and Chapter 8) of the act. However, also other parts of the act are relevant in the context of this referral, and the most relevant parts will, therefore, be presented below.

The purpose of the Intelligence Service Act, as stated in its Section 1-1, is to:

(a) contribute to safeguarding Norway's sovereignty, territorial integrity, democratic form of government and other national security interests, including preventing, uncovering and counteracting foreign threats to Norway and Norwegian interests
(b) contribute to safeguarding confidence in and secure the basis for control of the activities of the Norwegian Intelligence Service
(c) ensure that the activities of the Norwegian Intelligence Service are conducted in accordance with human rights and other fundamental values of a democratic society.

The tasks of the Intelligence Service – for which purpose facilitated collection in bulk of cross-border electronic communications serves as one of the information collection methods – are defined in Chapter 3 of the act. The relevant sections in this context are:

Section 3-1 Information collection on foreign threats

The Norwegian Intelligence Service shall collect and analyse information on foreign matters which can contribute to uncovering and counteracting

(a) threats to Norway's independence and security, territorial integrity and political and economic freedom of action
(b) serious threats to public security in Norway
(c) serious threats to Norwegian interests abroad
(d) foreign intelligence activity
(e) foreign sabotage and influence operations
(f) cross-border terrorism
(g) proliferation of weapons of mass destruction and equipment and material that can be used to manufacture such weapons
(h) international arms trade that could constitute a serious security threat
(i) export of sanctioned, listed or sensitive goods or services.

Section 3-2 Information collection on other foreign matters

The Norwegian Intelligence Service shall collect and analyse information on foreign matters which can contribute to

(a) safeguarding prioritised foreign, defence or security policy interests vis-a-vis matters and trends in other states and regions
(b) national emergency preparedness planning
(c) incident and crisis management
(d) planning and conducting national or international military operations.

Chapter 4 of the act, entitled “Ban on collection in Norway and other specific bans”, sets out various general restrictions on the use of covert collection methods. Section 4-1 imposes a ban on use of covert collection methods aimed at any person who at the time of collection is physically located in Norway:

The Norwegian Intelligence Service shall not use collection methods pursuant to chapter 6 against any person in Norway.

If there is doubt as to whether a person is located in Norway or abroad, the Norwegian Intelligence Service shall seek to clarify the matter. For this purpose, only information from Norwegian authorities, foreign partners, open sources or own collection abroad shall be used.

This ban is modified in Section 4-7, entitled “Accessory information regarding individuals in Norway”, in which the second paragraph is relevant with regard to facilitated collection of cross-border electronic communications:

The Norwegian Intelligence Service may use collection methods pursuant to chapter 6 against persons abroad even though information regarding persons in Norway may also be included.

The Norwegian Intelligence Service may collect raw data in bulk regardless of whether information regarding persons in Norway is included.

Chapter 7 is entitled “Facilitated Collection of Cross-border Communications”.

Section 7-1 of the Intelligence Service Act sets out the general conditions and scope of facilitated collection in bulk of cross-border electronic communications:

> The Norwegian Intelligence Service may, for intelligence purposes, collect electronic communication being transported across the Norwegian border provided that the basic conditions pursuant to Chapter 5 are met, the provisions of chapters 7 and 8 are being obeyed and the collection does not contravene other provisions of the Act.
>
> The provisions of chapters 7 and 8 only apply when it is necessary for providers pursuant to section 7-2 to facilitate the collection.

Electronic communication providers shall, subject to certain specified conditions, be obliged, to facilitate the collection of cross-border communications. The scope of their obligations is set out in Section 7-2 first paragraph:

> Pursuant to an order issued under Section 7-3 providers covered by section 1-5 of the Electronic Communications Act and providers of internet-based communications or messaging services available to the public shall mirror and make available to the Norwegian Intelligence Service selected communication streams and otherwise facilitate selection, filtering, testing, collection, storage and queries as described in this chapter, for instance by
>
> (a) providing information on signal environments, data formats, technical devices and methods
> (b) allowing the Service to install equipment and establish a temporary or permanent presence in order to operate equipment in locations controlled by the provider
> (c) assisting in the technical operation and maintenance of established solutions
> (d) helping to enable the Service to conduct test collection and test analyses of network and service traffic
> (e) ensuring access to communication without obstacles such as link encryption or equivalent encryption controlled by the provider
> (t) contributing to secure solutions.

The specific conditions for the facilitated collection of cross-border electronic communications are set out in Section 7-3. The first paragraph states:

> Electronic communications being transported across the Norwegian border may be mirrored as a basis for searches in stored metadata pursuant to Section 7-8 and for targeted collection and storage of content data pursuant to Section 7-9, when necessary to establish an information basis for intelligence purposes. Permission to issue an order for such mirroring is granted by the court by decision pursuant to the rules in Chapter 8. The order is issued by the Director of the Norwegian Intelligence Service.

It follows from this paragraph that the Intelligence Service must obtain a court order before issuing an order for the mirroring of cross-border electronic communications.

The condition is that such mirroring is “necessary to establish an information basis for intelligence purposes”.

The term “intelligence purposes” refers to all of the tasks of the Intelligence Service, as set out in Sections 3-1 and 3-2 (presented above).

According to the preparatory works of the Intelligence Service Act, the term “necessary” encompasses requirements of suitability, relevance, and proportionality, cf. Prop. 92 L (2022–

2023) p. 57, second column. The criterion is described as follows in Prop. 92 L (2022–2023) p. 53:

> The question of whether it is necessary to mirror cross-border electronic communications must be answered based on the circumstances at the time the request is made. Which circumstances may justify mirroring depends on the foreign - or security policy situation when the request is submitted, or on other information which, following a more detailed intelligence-professional analysis, indicates that national security interests render mirroring necessary. This may, for example, be that a given situation constitutes a threat or a potential threat to national security. Another example may be circumstances related to developments in other states or regions which, based on a professional assessment, are considered relevant for the Norwegian foreign intelligence service to monitor. The Intelligence Service must inform the court of the circumstances and other relevant factors that justify mirroring at the time of the request. What is to be regarded as relevant factors must be assessed in conjunction with the tasks of the Intelligence Service, which include the timely detection of threats or situations that may develop into threats—that is at a point in time when it is still unknown to others that there are circumstances abroad that constitute a threat or have a threat potential as mentioned. The level of specificity with which the threat or potential threat can be described may therefore be limited. For example, it must be accepted that the Intelligence Service justifies a mirroring request by stating that there is a general threat related to cyber espionage or influence operations by foreign states, without this being linked to a known target. It will not be necessary to document that a threat actor is conducting ongoing threat activity against Norway or Norwegian interests at the time of the request, provided that the Intelligence Service's professional assessments and analyses support that the circumstances may develop in such direction.

The court's authorization shall not be granted for a longer period that necessary and shall not exceed two years, cf. Section 8-6.

For each mirroring of communications, the mirrored communications must be filtered pursuant to Section 7-6 before being stored in bulk in a metadata repository:

> Section 7-6 Selection and filtering
>
> The Norwegian Intelligence Service shall, through selection and filtering, seek to prevent storage pursuant to section 7-7 of metadata regarding communication between senders and recipients who are both located in Norway, unless one of them is covered by section 4-2 subsection 1.

The obligation in Section 7-6 concerning filtering is deliberately formulated as an obligation to "seek to prevent storage […]" (as underscored here). It is stated in Proposition 80 L (2019–2020) point 11.8.2.3 that a more ambitious obligation was considered impractical:

> In the current technological situation, it will not be possible to prevent the storage of large amounts of metadata concerning Norwegian domestic communications.

Collection and storage of metadata in bulk is regulated in Section 7-7:

Following selection and filtering pursuant to section 7-6, the Intelligence Service may collect and store metadata in bulk on electronic communications being transported across the Norwegian border. 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.

In order to prevent storage of content data, the Norwegian Intelligence Service shall establish and maintain a list of which types of metadata may be stored. The list shall be made available to the EOS Committee and the Norwegian Communications Authority.

Stored metadata shall be deleted after 18 months at the latest.

In respect of technical analysis, troubleshooting and updating of stored metadata for the purpose of enabling queries, section 7-5 subsection 5 sentence 1 shall apply correspondingly.

5. Relevant EEA law

5.1 The EEA Agreement and Directive 2002/58/EC

Article 4(2) of the Treaty on European Union (TEU) provides that national security remains the sole responsibility of each member state. A corresponding provision is not included in the EEA Agreement. International cooperation in the defence sector and harmonisation of national rules on national security do not, however, fall within the scope of the EEA Agreement.

Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector is incorporated into the EEA Agreement and therefore legally binding on Norway.

Recitals 2 and 3 of Directive 2002/58/EC state:

> (2)This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.
> (3) Confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights, in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms, and the constitutions of the Member States.

Article 1, entitled “scope and aim”, provides:

> 1. This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

[…]

3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.

Article 3, entitled "Services concerned", provides:

This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices.

The principle of confidentiality of communications is guaranteed in Article 5 of Directive 2002/58/EC.

Restrictions in the rights and obligations provided for in Article 5 and other articles of Directive 2002/58/EC may only be adopted by national law and in accordance with Article 15(1).

Article 15(1) of Directive 2002/58/EC, provides:

1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

It follows that the objective of safeguarding national security is expressly mentioned in Article 15(1).

As the Charter of Fundamental rights is not incorporated into the EEA Agreement, the wording of Article 15(1) was changed when Directive 2002/58/EC was incorporated into the EEA Agreement, cf. the EEA Committee's decision no 80/2003 of 20 July 2003. The phrase "the general principles of Community law, including those referred to

in Article 6(1) and 29 of the Treaty on European Union" was changed to "the general principles of EEA law".

5.2 Case Law of the CJEU concerning Article 15 (1) of Directive 2002/58/EC

The question of whether Directive 2002/58/EC applies to national legislation enacted for the protection of national security was examined by the CJEU in two Grand Chamber judgments delivered on 6 October 2020;

- C-623/17 *Privacy International* (EU: C: 2020:790)

- Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others* (EU:C:2020:791)

The CJEU held that Article 1(3) and Article 15(1) of Directive 2002/58/EC is to be interpreted as meaning that national legislation which requires providers of electronic communications services to retain and forward traffic data and location data for the purpose of safeguarding national security, falls within the scope of that directive. (*Privacy International*, articles 30 – 49. *La Quadrature du Net*, articles 87 – 104). In reaching that conclusion, the Court relied, inter alia, on the wording of Article 15(1) of Directive 2002/58/EC read in light of Articles 1 and 3 and the rights to privacy and data protection enshrined in Articles 7 and 8 of the Charter of Fundamental Rights.

In *La Quadrature du Net*, the CJEU proceeded to interpret Article 15(1) in light of the Charter and laid down the conditions that national legislation requiring the retention of data must meet to satisfy the requirement of proportionality.

In paragraph 132 the CJEU set out requirements regarding the formulation of national legislation:

> In order to satisfy the requirement of proportionality, the legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subjected to automated processing, particularly where there is a significant risk of unlawful access to that data. Those considerations apply especially where the protection of the particular category of personal data that is sensitive data is at stake […]

In paragraphs 134–139, the CJEU established objective criteria that legislation providing for the preventive retention of personal data for the purpose of safeguarding national security must meet in order to comply with the proportionality requirement.

The disagreement between the parties in the present case particularly concerns the implications of paragraph 137, read in conjunction with paragraphs 135 and 136. Paragraphs 135 – 137 read:

135 In that regard, it should be noted, at the outset, that Article 4(2) TEU provides that national security remains the sole responsibility of each Member State. That responsibility corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities.

136 The importance of the objective of safeguarding national security, read in the light of Article 4(2) TEU, goes beyond that of the other objectives referred to in Article 15(1) of Directive 2002/58, inter alia the objectives of combating crime in general, even serious crime, and of safeguarding public security. Threats such as those referred to in the preceding paragraph can be distinguished, by their nature and particular seriousness, from the general risk that tensions or disturbances, even of a serious nature, affecting public security will arise. Subject to meeting the other requirements laid down in Article 52(1) of the Charter, the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives.

137 Thus, in situations such as those described in paragraphs 135 and 136 of the present judgment, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not, in principle, preclude a legislative measure which permits the competent authorities to order providers of electronic communications services to retain traffic and location data of all users of electronic communications systems for a limited period of time, as long as there are sufficiently solid grounds for considering that the Member State concerned is confronted with a serious threat, as referred to in paragraphs 135 and 136 of the present judgment, to national security which is shown to be genuine and present or foreseeable. Even if such a measure is applied indiscriminately to all users of electronic communications systems, without there being at first sight any connection, within the meaning of the case-law cited in paragraph 133 of the present judgment, with a threat to the national security of that Member State, it must nevertheless be considered that the existence of that threat is, in itself, capable of establishing that connection.

6. Submissions by the Parties

6.1 The Appellants

6.1.1 Introductory Remarks

The Appellants submit that the present case concerns the constitutional limits, under the EEA legal order, of general and indiscriminate bulk collection of electronic communications metadata by State authorities, through imposing on providers of electronic communication services an obligation to facilitate such collection.

In its Grand Chamber case-law (*Digital Rights Ireland* (C-293/12 and C-594/12), *Tele2 Sverige/Watson* (C-203/15 and C-698/15) and *La Quadrature du Net* (C-511/18, C-512/18 and C-510/18), the CJEU has consistently emphasized that such bulk retention or collection

constitutes a particularly serious interference with fundamental rights, including freedom of expression and information. The Court has underlined the chilling effect that surveillance regimes of this nature may cause in a democratic society. Although the Court in *La Quadrature du Net* accepted in principle that general and indiscriminate retention may exceptionally be permissible for the purpose of safeguarding national security, this was subject to strict and narrowly defined conditions.

6.1.2 The First Question – Scope of Application

The Appellants submit that the contested legislation falls within the scope of the EEA Agreement and Directive 2002/58/EC. The decisive criterion is not the objective invoked by the State, but whether the legislation regulates an activity harmonized by EEA law. Directive 2002/58/EC governs the processing of traffic and location data by providers of publicly available electronic communications services.

The Norwegian regime imposes obligations on such providers to facilitate the States' collection, retention and storage of communications data. It therefore regulates the processing of data in a harmonized sector of the internal market.

Article 15(1) of Directive 2002/58/EC expressly provides that Member States may introduce restrictions for national security purposes within the framework of the Directive. In LQN, the CJEU expressly rejected the argument that national security measures fall outside the scope of the Directive as such.

A different conclusion under the EEA Agreement would undermine the principle of homogeneity.

6.1.3 The Second Question – The Cross-Border Character

The Appellants submit that the fact that the regime is formally limited to cross-border communications does not affect the applicability of the criteria established in LQN.

Modern electronic communications between persons located in Norway are frequently routed via infrastructure abroad. Messages sent through global platforms, email services, VoIP calls and ordinary web searches will typically and regularly cross national borders in transit. The same pertains to any use of cloud based global services (such as, for instance, Microsoft Office 365). The regime will therefore in practice encompass a substantial volume of communications between persons located in Norway, as well as communications between Norway and other EEA States – and data concerning the population's daily digital activities in general. No distinction is made between communications involving other EEA States and communications involving third countries.

Directive 2002/58/EC does not condition its applicability on the technical routing of data, and the CJEU did not introduce such a territorial distinction in *La Quadrature du Net*. The relevant assessment concerns the nature and scope of interference, not the physical transmission path of the communication (where national borders are irrelevant in today's digital communications).

6.1.4 The Third Question – Threshold and Clarity Requirements

The "serious threat" requirement is a threshold condition
The Appellants submit that the requirement identified in LQN — that a Member State must be confronted with a serious threat to national security that is genuine and present or foreseeable — constitutes a legal threshold, a *prerequisite* condition.

The threshold identified in LQN constitutes a narrow and exceptional basis for permitting measures of such intensity.

It is not sufficient that the seriousness of the threat be treated as one of several factors within a general necessity assessment. General and indiscriminate collection may only be permitted where the specific threshold identified in LQN is met. It is not sufficient that the requirements identified in LQN is part of a global assessment.

The essential limits must be clearly laid down in statutory law
The Court of Justice has required that national legislation lays down clear and precise rules governing the scope and application of such measures.

This requirement is particularly important in the context of secret bulk surveillance. Individuals are not notified that their data is collected and cannot in practice assess or challenge the legality of interference. Therefore, clear and binding statutory limits constitute the primary safeguard.

It is not sufficient in this context that the relevant conditions emerge through (secret) administrative practice or (secret) court decisions. The essential limits, including the prerequisite conditions, must be expressly and clearly reflected in the statutory law..

6.2 The Respondent

The EEA Agreement does not extend to matters of defence or national security. The purpose of the Agreement is solely to promote a continuous and balanced strengthening of trade and economic relations between the contracting parties, under equal conditions of competition and the respect of the same rules, with a view to establishing a homogeneous European Economic Area, cf. Article 1(1).

In order to attain these objectives, the EEA cooperation shall include the free movement of goods, the free movement of persons, the free movement of services, the free movement of capital, the establishment of a system ensuring that competition is not distorted and that the rules thereon are equally respected, as well as closer cooperation in other areas such as research and development, environment, education and social policy, cf. Article 1(2).

Since the EEA Agreement does not cover defence or national security, it imposes no constraints on the States' organisation of their national defence, including their intelligence services. Neither the main part of the EEA Agreement nor acts incorporated into the Agreement, such as Directive 2002/58/EC, impose limitations on national legislation governing the activities of the intelligence services. In this regard, it is irrelevant that private parties are required to facilitate intelligence activities
.
It follows that neither the main part of the EEA Agreement nor Directive 2002/58/EC applies to rules such as Section 7-2 of the Intelligence Service Act on facilitated collection of cross-border communications.

The Treaty on European Union (TEU) Article 4(2), and the CJEU's interpretation of that provision, are irrelevant for determining the scope of application of the EEA Agreement, cf. Article 1.

Should the EFTA Court find that the EEA Agreement and Directive 2002/58/C apply, the State submits that the conditions articulated in Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, are not relevant for rules such as Section 7-2 of the Intelligence Service Act, which concern only the mirroring of metadata from cross-border communications – and only as part of foreign intelligence.

It is evident that the collection of data concerning only cross-border communications, and used exclusively for foreign intelligence purposes, is less intrusive than provisions permitting the general retention of all metadata from all domestic communications for use in domestic intelligence, as was the case in *La Quadrature du Net.*.

The risks associated with general retention of metadata from all domestic communications are described in the judgment in Joined Cases C-203/15 and C-698/15 Tele2 Sverige and Watson and Others, where the CJEU in paragraph 99 endorsed the Opinion of the Advocate General in points 257 and 259 of his opinion:

> 257 Let us suppose, first of all, that a person who has access to retained data wishes to identify all the individuals in the Member State who have a psychological disorder. Analysing the content of all communications effected within the national territory for that purpose would require considerable resources. On the other hand, by using databases of communications data, it would be possible instantly to identify all the individuals who have contacted a psychologist during the data retention period. The data retained include the identity of the sender and the recipient of every communication, and it would merely be necessary to cross-reference that data with a list of telephone numbers of psychologists practising in the country. I might add that that technique could be extended to any of the fields of specialist medicine registered in a Member State …
>
> 259 I would emphasise that the risks associated with access to communications data (or 'metadata') may be as great or even greater than those arising from access to the content of communications … In particular, as the examples I have given demonstrate, 'metadata' facilitate the almost instantaneous castaloguing of entire populations, something which the content of communications does not.

In the ECtHR's judgment of 25 May 2021 in Case 35252/08 *Centrum för Rättvisa*, concerning Swedish provisions similar in many respects to Section 7-2 of the Norwegian Intelligence Service Act, the limitation to cross-border communications was regarded as "a significant limitation on the authorities' discretion and asa safeguard against abuse" (paragraph 308).

In Joined Cases C-793/19 and C-794/19 *SpaceNet* and Telekom Deutschland, the CJEU stated that the ECtHR's case-law on such systems, including *Centrum för Rättvisa*, was not relevant to provisions concerning the general and indiscriminate retention of metadata from domestic communications (paragraph 125):

> Furthermore, the judgments of the European Court of Human Rights of 25 May 2021, Big Brother Watch and Others v. the United Kingdom (CE:ECHR:2021:0525JUD005817013), and of 25 May 2021, Centrum för Rättvisa v. Sweden(CE:ECHR:2021:0525JUD003525208) relied on by certain governments at the hearing to argue that the ECHR does not preclude national legislation providing, in essence, for a general and indiscriminate retention of traffic and location data, cannot call into question the interpretation of Article 15(1) of Directive 2002/58 resulting from the foregoing considerations. Those judgments concerned the bulk interception of data relating to international communications. Thus, as the Commission observed at the hearing, the European Court of Human Rights did not rule, in those judgments, on the compatibility with the ECHR of a general and indiscriminate retention of traffic and location data on national territory or even a large-scale interception of those data for the purposes of the prevention, detection and investigation of serious criminal offences.

It appears from the Advocate General's Opinion in the case, cf. point 40, that this view was shared by the majority of the parties at the hearing.

The Government is likewise unaware of any other EEA States that have based their legislation on the collection of cross-border metadata for foreign intelligence purposes on the assumption that the criteria in *La Quadrature du Net* are relevant.

If the EFTA Court concludes that the criteria in *La Quadrature du Net* are relevant for provisions such as Section 7-2 of the Intelligence Service Act on foreign intelligence collection, the State submits that the judgment cannot be interpreted as requiring the criteria in paragraph 137 to be expressly set out in the national legislation. There is no support in the wording of paragraph 137, or elsewhere in the judgment, for concluding that the CJEU intended to impose such a requirement.

The CJEU derived the criteria in paragraph 137 from Article 15(1) of the Directive, which provides that limitations on the right to communications privacy must be necessary, appropriate, and proportionate. In the Norwegian Intelligence Service Act, these requirements are reflected in the necessity requirement set out in Section 7-3.

7. The Need for an Advisory Opinion

7.1 The scope of the EEA Agreement and Directive 2002/58/EC

Notwithstanding Article 4(2) TEU, the CJEU has held that national legislation authorising bulk interception regimes for the purpose of protecting national security falls within the scope of Directive 2002/58/EC (see *La Quadrature du Net and Privacy International).* In reaching this conclusion, the CJEU relied, inter alia, on the rights to privacy and data protection enshrined in Articles 7 and 8 of the Charter of Fundamental Rights.

The Charter is not incorporated into the EEA Agreement.

In preparing revisions to The Norwegian Intelligence Service Act chapters 7 and 8, the Norwegian Government raised the question of whether Directive 2002/58/EC and, consequently, the CJEU's interpretative judgments in *La Quadrature du Net* and *Privacy International* apply to the Norwegian Intelligence Service Act.

On this basis, the parties disagree as to whether national legislation in the defence sector, whose sole purpose is the protection of national security, falls within the scope of the EEA Agreement and Directive 2002/58/EC.

In the view of the preparatory judge, existing case law from the EFTA Court does not sufficiently resolve the question of the scope of the EEA Agreement and Directive 2002/58/EC in this context. It is therefore appropriate to refer a question concerning the scope of the EEA Agreement and Directive 2002/58/EC in relation to national legislation in the defence sector authorising bulk interception regimes for the sole purpose of safeguarding national security interests.

7.2 The Relevance of the LQN- Criteria

In *La Quadrature du Net,* the question before the CJEU concerned national legislation imposing on providers of electronic communications services, for the purposes set out in Article 15(1), an obligation to retain traffic and location data of all users and subscribers in a general and indiscriminate manner (cf. paragraphs 81 and 82).

By contrast, the bulk interception regime authorised under Chapters 7 and 8 of the Norwegian Intelligence Act is limited to the collection of cross-border communications for the sole purpose of foreign intelligence gathering. However, it is a fact that the facilitated collection of cross-border communications will, to a significant extent, include purely domestic communications, as described above.

The parties disagree as to whether the legal differences between the bulk interception regime examined *in La Quadrature du Net* and the Norwegian rules on the facilitated collection of metadata from cross-border communications are relevant for determining the scope of the LQN-criteria.

In the view of the preparatory judge, this question is not resolved by existing CJEU case law. It is therefore appropriate to refer a question on whether legislation authorising bulk interception regimes limited to cross-border communications for the purpose of foreign intelligence gathering falls within the scope of the LQN-criteria. In assessing this question, it should be borne in mind that the collection of metadata from cross-border communications will, in practice, affect purely domestic communications.

7.3 National legislation on the facilitated collection of cross-border electronic communications

With regard to the general interpretation of the proportionality requirement in Article 15(1) of Directive 2002/58/EC, the parties disagree on the implications of the CJEU's interpretative ruling in *La Quadrature du Net*, particularly as regards the design of national legislation authorising bulk interception regimes..

The disagreement between the parties particularly concerns the implications of paragraph 132 and paragraph 137, read in conjunction with paragraphs 135 and 136 of the judgment..

On the assumption that Directive 15(1) and the LQN criteria apply, the parties agree that a condition for the facilitated collection of cross-border communications must be that "there are sufficiently solid grounds for considering that the Member State concerned is confronted with a serious threat, as referred to in paragraphs 135 and 136 of the present judgment, to national security which is shown to be genuine and present or foreseeable," cf. LQN paragraph 137.

The parties disagree on whether that condition must be formulated explicitly in the national legislation, or whether it may be deduced from the necessity requirement in Section 7-3 of the Intelligence Service Act.

Even if Article 15(1) of Directive 2002/58/EC has previously been interpreted by the CJEU, existing case law, does not resolve the question of whether, and if so in what manner, the LQN-criteria must be set out in national statutory legislation. It is therefore appropriate to ask whether Directive 2002/58/EC requires that the substantive conditions laid down in paragraph 137 of *La Quadrature du Net* in conjunction with paragraphs 135 and 136, be explicitly reflected in national legislation.

8. Questions

In light of the foregoing, Borgarting Court of Appeal has decided to refer the following questions to the EFTA Court:

1. Does the scope of application of the EEA Agreement and Directive 2002/58/EC encompass national legislation governing the defence sector and mandating the facilitated bulk collection of metadata from cross border electronic communications, where its sole objective is the protection of national security?

2. If question 1 is to be answered in the affirmative, do the criteria established by the Court of Justice of the European Union under Article 15(1) of Directive 2002/58/EC in its judgment of 6 October 2020 in Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, apply to national legislation mandating the facilitated bulk collection, storage and processing of metadata from cross-border communications solely for the purpose of foreign intelligence gathering?

3. If question 2 is to be answered in the affirmative, does Article 15(1) of Directive 2002/58/EC require that the conditions set out in paragraph 137 of the Court of Justice's judgment of 6 October 2020 in Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, read in conjunction with paragraphs 135 and 136, be expressly laid down in national legislation (statutory law) restricting rights under the Directive on grounds of national security?

Borgarting Court of Appeal

Kristel Heyerdahl
Court of Appeal Judge