# ATTORNEY GENERAL – CIVIL AFFAIRS

To the Court of Justice of the European Union

Oslo, 14 February 2018

## WRITTEN OBSERVATIONS

## BY

## THE KINGDOM OF NORWAY

represented by Marius EMBERLAND and Jørgen VANGSNES, advocates at the Office of the Attorney General (Civil Affairs), and Troels Bjerre LEMING, Higher Executive Officer at the Ministry of Foreign Affairs, acting as agents, submitted pursuant to the third paragraph of Article 23 of the Protocol on the Statute of the Court of Justice of the European Union, in the case of

**C-623/17 - Privacy International**

in which the Investigatory Powers Tribunal (UK) has requested a preliminary ruling pursuant to Article 267 of the Treaty on the Functioning on the European Union (TFEU) on the interpretation of Article 4 of the Treaty of the European Union (TEU) and Article 1(3) of Directive 2002/58/EC on privacy and electronic communications (the e-Privacy Directive).



POSTAL ADRESS:
P.O. BOX 8012 DEP
N-0030 OSLO, NORWAY

TELEPHONE: + [redacted] / + [redacted]
TELEFAX: + 47 22 99 02 50
E-MAIL: MEM@REGJERINGSADVOKATEN.NO

VISITING ADDRESS:
UNIVERSITETSGATA 8
OSLO

## 1 INTRODUCTION

(1) The referring court has posed two questions:

> *(1) Having regard to Article 4 TEU and Article 1(3) of Directive 2002/58/EC on privacy and electronic communications (the "e-Privacy Directive"), does a requirement in a direction by a Secretary of State to a provider of an electronic communications network that it must provide bulk communications data to the Security and Intelligence Agencies ('SIAs') of a Member State fall within the scope of Union law and of the e-Privacy Directive?*
>
> *(2) If the answer to Question (1) is 'yes', do any of the Watson Requirements, or any other requirements in addition to those imposed by the ECHR, apply to such a direction by a Secretary of State? And, if so, how and to what extent do those requirements apply, taking into account the essential necessity of the SIAs to use bulk acquisition and automated processing techniques to protect national security and the extent to which such capabilities, if otherwise compliant with the ECHR, may be critically impeded by the imposition of such requirements?*

(2) The Kingdom of Norway is not a party to the Treaty of the European Union (TEU) and its Article 4. There is no equivalent to Article 4 TEU in the Agreement on the European Economic Area (EEA Agreement), the scope of which is in any event less broad than that of the TEU and the Treaty of the Functioning of the European Union (TFEU), see in particular Articles 1 and 2 of the EEA Agreement.

(3) Directive 2002/58/EC on privacy and electronic communications (the e-Privacy Directive) is, however, incorporated into the EEA Agreement by the EEA Joint Committee's decision no. 80/2003 of 20 June 2003 (in force as from 1 August 2004).

(4) Norway is further a signatory to the European Convention on Human Rights, 4 November 1950, ETS 5; and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, ETS 108.

(5) Against this background, and without prejudice to the specific facts that have given rise to the referring court's request for a preliminary ruling, the Government of the Kingdom of Norway (the Norwegian Government) hereby respectfully submits its observations in the present case. The observations are confined to the first question asked by the referring court and are limited to the scope of the e-Privacy Directive. They do not consider which criteria are relevant in the event that the Directive applies.

## 2 AS TO QUESTION NO. 1 POSED BY THE REFERRING COURT

### 2.1 The wording of Article 1(3) and its immediate context

(6) Article 1(3) of the e-Privacy Directive is the third paragraph of a provision which, according to its title, sets out the scope (and aim) of the Directive:

> *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.*

(7) The wording in and by itself demonstrates that matters pertaining to state security does not per se lie within the ambit of the Directive: it states that it "shall not apply ... to activities concerning public security, defence, State security ...".

(8) The Court of Justice has consistently held that, in interpreting provisions of EU law, it is necessary to consider not only their wording but also the context in which they occur and the objectives pursued by the rules of which they are part, see, e.g., Grand Chamber judgment of 19 December 2013, *Koushkaki v. Germany*, C-84/12, ECLI:EU:C:2013:862, paragraph 34 with further references.

(9) The terms in question must consequently be read in conjunction with their immediate surrounding context, from which at least the following inferences may be drawn.

(10) First, in areas of public and state security (and defence), the wording of Article 1(3) states that the e-Privacy Directive does not apply to activities that "concern" or "relate to" public and state security. Conversely, in the area of criminal law the Directive shall not apply to activities to the extent that they concern "activities of the State". As a mere textual argument it may be inferred that the Directive does not apply to activities when they relate to public and state security, while the non-application of the e-Privacy Directive in the area of criminal law is not equally absolute.

(11) Second, by stating in the beginning of Article 1(3) that the Directive does not apply to activities which "fall outside the scope of the Treaty establishing the European Community", the text signals that the scope of the Directive merely intends to cover subject matters within the ambit of that treaty, notably the regulation of the movement of goods, services, persons and capital – and not the activities of security and intelligence agencies. This corresponds with the fact that the e-Privacy Directive from the outset has been considered to be EEA relevant, the subject matter of the EEA Agreement being chiefly similar to that of the EC Treaty. The proviso at the outset of Article 1(3) thus adds weight to an interpretation whereby state security and intelligence activities are not per se within the scope of the Directive.

### 2.2 The legislative history

(12) The 2002 e-Privacy Directive replaced Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (the 1997 Privacy Directive).

Article 1(3) of the 1997 Privacy Directive contained the exact same wording as does Article 1(3) of the e-Privacy Directive.

(13) The 2002 e-Privacy Directive was, when drafted, "not intended to create major changes to the substance of the existing Directive", see, e.g., para. 1 of Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the processing of privacy in the electronic communications sector, COM/2000/0385. It was emphasised that the proposed directive should "not apply ... to fields in the public sector where the activities of that sector fall outside the scope of Community law, e.g. the Intelligence service", cf. p. 21 of Commission Communication on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security, COM/90/314FINAL.

(14) This suggests a longstanding perception that the activities of security and intelligence services in the main are outside the realm of the aforementioned EU secondary legislation. The legislative background supports a literal reading of Article 1(3) of the e-Privacy Directive.

### 2.3 The Preamble and its premise of allocation of legal norms

(15) Further to the context of Article 1(3) of the e-Privacy Directive, the Government recalls recital 11 of the Preamble:

> *Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.*

(16) The Preamble, to put it briefly, states that the Directive "does not affect the ability of Member States to carry out lawful interception of electronic communications" if that is "necessary for", inter alia, "the protection of public security, defence, State security and the enforcement of criminal law". The recital thereby doubles the statement found in

Article 1(3) and adds weight to the discernment that the terms of the provision must be understood according to their plain textual composition.

(17) Recital 11 also makes reference to human rights obligations pertaining to the Member States being governed by the European Convention on Human Rights and that the balancing of national security interests and individual rights are to be solved by reference to that Convention ("in accordance with the European Convention on Human Rights and Fundamental Freedoms") and the case law of the European Court of Human Rights ("as interpreted by the rulings of the European Court of Human Rights").

(18) The Norwegian Government further refers to recitals 1, 2 and 3, as they, too, support the notion of allocation of norms as described above:

> *(1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data requires Member States to ensure the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community.*
>
> *(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.*

(19) It is further observed that recital 12 states:

> *Subscribers to a publicly available electronic communications service may be natural or legal persons. By supplementing Directive 95/46/EC, this Directive is aimed at protecting the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons. This Directive does not entail an obligation for Member States to extend the application of Directive 95/46/EC to the protection of the legitimate interests of legal persons, which is ensured within the framework of the applicable Community and national legislation.*

(20) It is a matter of interpretation what recital 12 suggests as to the proper scope of the Directive.

(21) The Member States of the European Union (and of the EEA Agreement) are – and must be – signatories to the European Convention on Human Rights, including its Article 8 on the right to respect for private life. They are also signatories to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of

Personal Data, ETS 108 (in force from 1 October 1981), which also does not exempt matters of state security. Further, as suggested by recital 3 of the Preamble of the e-Privacy Directive, privacy protection in the face of activities pursued by state security and intelligence services may be governed by the constitutional law of the Member States.

(22) The Norwegian Government submits that Article 1(3) of the Directive should be read in the context of a fundamental allocation of norms between legal systems in matters where public and state security meet the individual's right to protection of privacy, and which is expressed in the Preamble: for activities falling outside the scope of the Directive, other legal norms by which the Member States are bound cover these activities and cater for the balancing of opposing interests, including privacy concerns.

(23) A reading of the e-Privacy Directive which excludes the activities of security and intelligence agencies does not entail that individuals are left without legal safeguards in the face of such activities. Rather, such an interpretation is in conformity with the values of human rights as indicated by the Preamble. These considerations support an interpretation of Article 1(3) of the Directive whereby the activities of security and intelligence agencies lie outside the scope of the Directive.

### 2.4 Article 15(1) of the Directive and the case law of the Court

(24) Article 15 (Application of certain provisions of Directive 95/46/EC) states in para. 1:

> *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.*

(25) It should first be noted that Article 15(1) is not a general provision establishing requirements for permissible exceptions and restrictions of the rights and obligations set forth in the e-Privacy Directive: the title of Article 15 suggests that its only purpose be the governing of the relationship between the e-Privacy Directive and (certain provisions of) the Data Protection Directive. That in itself calls for a tempered approach when extracting meaning from Article 15 for the construction of Article 1(3).

(26) Further, a prerequisite for applying Article 15(1) is indisputably that the measure at hand is within the scope of the e-Privacy Directive, as limited by Article 1(3). The Norwegian Government submits that certain regulations may well be within the scope of the Directive, yet still be subject to restrictions on grounds of national security. On the other hand, Article 15(1) does not imply that every measure concerning national security is within the scope of the Directive. In the view of the Government, Articles 1(3) and 15(1) should be interpreted so as to give effect to both provisions.

(27) The key to harmonise the two is, in the opinion of the Norwegian Government, an examination of the Court's Grand Chamber judgment of 30 May 2006, *Parliament v. Council and Commissio*n, Joined Cases C-317/04 and C-318/04, ECLI:EU:C:2005:190, on the one hand; and the Grand Chamber judgment of 21 December 2016, *Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson and others*, Joined Cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, on the other.

(28) In *Parliament v. Council and Commission*, the Court found that Article 3(2) of Directive 95/46/EC of the Parliament and of the Council of 24 October 1995 on the protection on individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Directive) should be understood to mean that the Data Protection Directive did not apply. This the Court concluded notwithstanding the fact that the data were initially collected by the airline companies while acting within the scope of Community law (paragraph 57), and even though it was for the airline companies to arrange for the transfer of data to a third country (paragraph 58).

(29) Significantly, the Court in the last sentence of para. 58 observed that "[t]he transfer falls within a framework established by the public authorities that relates to public security" (emphasis added here). The Court thereby captured the wording of the provision that is relevant to matters of public security. The Government recalls paragraph 10 of its observations above regarding the textual difference in Article 1(3) of the e-Privacy Directive between matters of public security and matters of criminal law.

(30) Article 3(2) of the Data Protection Directive is terminologically identical to Article 1(3) of the e-Privacy Directive. Also, as the title of Article 15 of the e-Privacy Directive shows, Article 15(1) refers to and must be understood within the context of the Data Protection Directive. The approach taken by the Court in *Parliament v. Council and Commission* is therefore relevant for the interpretation of Article 1(3) of the e-Privacy Directive in the present case.

(31) On the other hand, the Court in *Tele2/Watson* did not opine on the possible significance of Article 1(3) for the purpose of interpreting Article 15(1). Although Article 1(3) was mentioned (in para. 69), the Court drew no explicit inferences from it in its interpreting of Article 15(1). However, the Court found that Article 1(3) could not be interpreted in a way that deprived Article 15(1) of any purpose (paragraph 73).

(32) Also, the purpose of the measure involving telecommunication providers in *Tele2/Watson* was the combating of crime, and not state security. The Government recalls, with reference to paragraph 10 above, the linguistic disparity in Article 1(3) between public and state security activities on the one hand and criminal law matters on the other. In the area of criminal law only the "activities of the State" exclude the application of the e-Privacy Directive. Conversely, the wording implies that every activity relating to public and state security is beyond the Directive's reach, regardless of the involvement of telecommunication providers.

(33) Further, it is to be noted that the consequence of the Court's reasoning in *Tele2/Watson* was the establishment of certain criteria to be satisfied for a measure to comply with the requirements in Article 15(1) of the e-Privacy Directive. The Norwegian Government observes that the criteria were developed with the combating of ordinary crimes in mind and that they do not necessarily transpose easily to the context of the activities of security and intelligence services.

(34) In the view of the Government these considerations may affect the import of *Tele2/Watson* for the purpose of the question posed by the referring court in the present case.

(35) In any event, in *Tele2/Watson* the Court considered a national measure chiefly ordering the telecommunication providers (or operators) to *retain* data for a certain period of time, for the purpose of combating crime. In the judgment, the Court stated that the e-Privacy Directive extends, "in particular", to measures "that requires ... providers to retain traffic and location data, since to do so necessarily involves the processing, by those providers, of personal data" (paragraph 75).

(36) The Court admittedly made remarks also with regard to the *accessing* of data (see, inter alia, paragraph 76). However, the essential feature of the national regulations in question was the imposition of an obligation on the providers to *retain* data.

(37) The Norwegian Government submits, with reference to *Tele2/Watson* and *Parliament v. Council and Commission*, that a distinction may be made between measures primarily constituting state activities as mentioned in Article 1(3) and measures that impose burdens on, and thereby involves the functioning of, the providers (such as a measure imposing an obligation to retain data). The Government recognises that such a distinction can hardly be drawn by applying a strictly logical approach, since many measures will have elements of both aspects. Rather, one must, when assessing activities in the areas of criminal law as in *Tele2/Watson*, consider the main characteristics of the measure in question. Despite the more absolute exemption from the scope of the Directive in the areas of public security, defence and State security, as explained above, the Government does not exclude that the same distinction may be drawn in these areas in order to fulfil the purpose of Article 1(3) of the e-Privacy Directive.

### 2.5 The relevance of the last sentence of Article 15(1)

(38) The Government further agrees with the referring court in that the last sentence of Article 15(1) should be understood as a mere reiteration of recital 11 and that the provision therefore only confirms the fundamental allocation of norms mentioned above, notably that European Convention on Human Rights does, and EU law does not, apply to the activities excluded from Article 1(3), see paragraph 38 of the referring court's request for a preliminary ruling.

## 3 CONCLUSION

(39) In the light of the observations above, the Norwegian Government respectfully proposes that the Court of Justice answer the first question posed by the referring court as follows:

> *Having regard to Article 1(3) of Directive 2002/58/EC on privacy and electronic communications (the "e-Privacy Directive"), and bearing in mind the fundamental allocation of norms between the Directive on the one hand and human rights norms on the other, activities of security and intelligence agencies do not per se fall within the scope of the e-Privacy Directive.*

****

Oslo, 14 February 2018

| | | |
|---|---|---|
| [redacted] | [redacted] | [redacted] |
| Marius Emberland | Jørgen Vatnsnes | Troels Bjerre Leming |
| agent | agent | agent |