Observations of Estonia

Case C-623/17 *

Document lodged by:

Republic of Estonia

Usual name of the case:

Privacy International

Date lodged:

14 February 2018

Välisministeerium (Foreign Ministry)

Court of Justice

Registry

Rue du Fort Niedergrünewald

L-2925 Luxembourg

By e-curia

14 February 2018

nr 15.3-2/970

IN CASE C-623/17, reference for a preliminary ruling,

referring court: Investigatory Powers Tribunal, London (United Kingdom)

OBSERVATIONS OF THE GOVERNMENT OF THE REPUBLIC OF ESTONIA

in Case C-623/17

submitted in accordance with Article 23 of the Protocol on the Statute of the Court of Justice of the European Union

* Language of the case: English.

Service of Court documents by e-Curia or to the address Välisministeerium, Islandi väljak 1, 15049 Tallinn, Republic of Estonia, fax +372 6377 098

I. INTRODUCTION

1 The United Kingdom court referred questions to the Court of Justice on 18 October 2017 concerning the applicability of EU law, more precisely Directive 2002/58/EC [1] ('the e-Privacy Directive'), and the judgment of the Court of Justice in *Tele2 Sverige and Watson and Others*, [2] to the forwarding of bulk communications data to the security and intelligence agencies of a Member State.

2 More precisely, the United Kingdom court referred the following questions to the Court of Justice:

In circumstances where:

a. the [security and intelligence agencies'] capabilities to use [bulk communications data] supplied to them are essential to the protection of the national security of the United Kingdom, including in the fields of counter-terrorism, counter-espionage and counter-nuclear proliferation;

b. a fundamental feature of the [security and intelligence agencies'] use of the [bulk communications data] is to discover previously unknown threats to national security by means of non-targeted bulk techniques which are reliant upon the aggregation of the [bulk communications data] in one place. Its principal utility lies in swift target identification and development, as well as providing a basis for action in the face of imminent threat;

c. the provider of an electronic communications network is not thereafter required to retain the [bulk communications data] (beyond the period of their ordinary business requirements), which is retained by the State (the [agencies]) alone;

d. the national court has found (subject to certain reserved issues) that the safeguards surrounding the use of [bulk communications data] by the [agencies] are consistent with the requirements of the ECHR; and

e. the national court has found that the imposition of the requirements specified in [paragraphs 119 to 125 of the judgment of the Court of Justice in [*Tele2 Sverige and Watson and Others*] ('the Watson Requirements'), if applicable, would

[1] 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 on privacy and electronic communications), OJ 2002 L 201, p. 37.

[2] Judgment of 21 December 2016, *Tele2 Sverige and Watson and Others*, Joined Cases C-203/15 and C-698/15, EU:C:2016:970.

frustrate the measures taken to safeguard national security by the [agencies], and thereby put the national security of the United Kingdom at risk;

1. Having regard to Article 4 TEU and Article 1(3) of [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 … 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 [agencies] 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?

II. RELEVANT PROVISIONS

Treaty on European Union

Article 4(2)

2. The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.

Article 5(1) and (2)

1. The limits of Union competences are governed by the principle of conferral. The use of Union competences is governed by the principles of subsidiarity and proportionality.

2. Under the principle of conferral, the Union shall act only within the limits of the competences conferred upon it by the Member States in the Treaties to attain the objectives set out therein. Competences not conferred upon the Union in the Treaties remain with the Member States.

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, OJ 1995 L 281, p. 31

Recital 13

Whereas the activities referred to in Titles V and VI of the Treaty on European Union regarding public safety, defence, State security or the activities of the State in the area of criminal laws fall outside the scope of Community law, without prejudice to the obligations incumbent upon Member States under Article 56(2), Article 57 or Article 100a of the Treaty establishing the European Community; whereas the processing of personal data that is necessary to safeguard the economic well-being of the State does not fall within the scope of this Directive where such processing relates to State security matters;

Article 3(2)

2. This Directive shall not apply to the processing of personal data:

— in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

— by a natural person in the course of a purely personal or household activity.

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 on privacy and electronic communications), OJ 2002 L 201, p. 37

Recital 11

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.

Article 1(3)

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 15(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.

III. CIRCUMSTANCES OF THE CASE

3 Estonia summarises the circumstances of the main proceedings as follows:

4 The applicant (Privacy International) claims that the acquisition and use of bulk communications data by the United Kingdom's security and intelligence agencies ('the SIAs') breaches the right to respect for private life laid down in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms ('the ECHR') and is contrary to EU law.

5 Under the United Kingdom's Telecommunications Act, the minister may give the operator of a public electronic communications network the general or specific directions he regards as necessary in the interests of national security. The SIAs have acquired bulk communications data from the network operators on the basis of such directions. The SIAs hold the bulk communications data obtained from the network operators securely. As regards some techniques which the SIAs use for searching in bulk communications data, a basic feature is that the technique in question (for example, filtering and finding suitable results) is non-specific (non-targeted), that is, they are not directed to specific known targets.

6 The referring court is convinced on the basis of the evidence submitted to it that bulk communications data is essential in the SIAs' fight against actual dangers to public security, that is, in the field of combating terrorism, counter-intelligence and preventing the spread of nuclear weapons. The SIAs' possibilities in connection with bulk communications data, that is, the possibilities of acquiring

and using it, are essential for the defence of the national security of the United Kingdom.

IV. LEGAL ANALYSIS

Introductory comment

7 Estonia wishes to stress that the circumstances of the present main proceedings differ essentially from the circumstances of previous cases concerning the processing and protection of personal data. The earlier cases [3] did not concern activity connected with national security, more specifically intelligence and counter-intelligence. The issue in the present case is primarily whether activities connected with the protection of national security are within the scope of EU law.

Question 1

8 Estonia's answer to Question 1 is that in the conditions set out in the order for reference the requirements laid down in national law for network operators to give bulk communications data to the SIAs of the Member State do not fall within the application of EU law and the e-Privacy Directive.

Articles 4(2) and 5(1) and (2) TEU

9 The first sentence of Article 5(1) TEU expressly provides that the limits of EU competences are governed by the principle of conferral. Article 5(2) TEU specifies that, under the principle of conferral, the EU is to act only within the limits of the competences conferred upon it by the Member States in the Treaties to attain the objectives set out therein. Competences not conferred on the EU in the Treaties remain with the Member States. The constitutional character and consequential mandatory nature of the principle of conferral have also repeatedly been confirmed by the Court of Justice. [4]

10 The Member States have not transferred basic State functions in connection with national security to the EU; on the contrary, the second and third sentences of Article 4(2) TEU expressly provide that the EU is to respect essential State functions, inter alia ensuring the territorial integrity of the State, maintaining law

[3] Judgments of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238; of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650; of 21 December 2016, *Tele2 Sverige and Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970; and Opinion 1/15 (Agreement between Canada and the EU on the transfer of passenger name record data) of 26 July 2017, EU:C:2017:592.

[4] Judgment of 27 November 2012, *Pringle*, C-370/12, EU:C:2012:756; Opinion 2/12 (Accession of the EU to the ECHR) of 18 December 2014, EU:C:2014:2454; judgments of 16 June 2016, *Gauweiler and Others*, C-62/14, EU:C:2015:400; and of 5 December 2017, *Germany* v *Council*, C-600/14, EU:C:2017:935.

and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.

11 The Court of Justice has held that certain acts of the State are outside the scope of application of EU law, that is, they are protected by Article 4(2) TEU. [5] Interpreting the first two sentences of Article 4(2) together, it must be concluded that EU law does not call in question the competence of the State to organise and regulate national security, since that is protected by Article 4(2) TEU, under which the EU is obliged to respect the essential functions of the State, including safeguarding national security. Article 4(2) TEU is a protective clause protecting the powers of a Member State and as it were a positive reservation of the sovereignty of the Member States in relation to all the activities mentioned in that provision.

12 Since the Treaties do not give the EU competence to regulate questions of national security, the Member States are entitled under Article 4(1) TEU and Article 5(2) TEU to act in that field. [6]

13 Estonia considers that it is clear that the collection and use of data in the field of intelligence and counter-intelligence by the SIAs forms an essential part of the system of protection of national security, ensuring the prevention of military and other risks and the protection of sensitive information. The functioning of the field of security is founded especially on the collection, treatment and analysis of information, the drawing of conclusions on the basis of that information, and the implementation of the necessary counter-measures.

14 The aim of the activity of the SIAs in performing one of the core functions of the State is after all to collect information for making national security policy decisions and to give advance warning of possible attacks on the State, including military and terrorist ones. Access to the necessary data and analysis of such data by the SIAs are therefore an inseparable part of the basic functions of the State.

15 Estonia stresses that, since the basic functions of the State in connection with national security have not been transferred to the EU and national security is the sole responsibility of each Member State, it must be possible for the Member States to decide independently what measures and means it is necessary to apply for ensuring the activity of the SIAs, in other words carrying out a basic function of the State. That self-evidently also includes a decision on whether and to what extent to require network operators to provide data for the purpose of ensuring security.

16 Estonia considers that the protective clause of Article 4(2) TEU is confirmed, for example, by the Declaration on Article 16 TFEU annexed to the Final Act of the

[5] Judgments of 21 December 2016, *Remondis*, C-51/15, EU:C:2016:985, paragraphs 40 and 41, and of 12 April 2014, *Digibet and Albers*, C-156/13, EU:C:2014:1756, paragraph 34.

[6] By analogy, judgment of 27 November 2012, *Pringle*, C-370/12, EU:C:2012:756, paragraph 105.

Intergovernmental Conference which adopted the Treaty of Lisbon, [7] which provides that, whenever rules on protection of personal data to be adopted on the basis of Article 16 could have direct implications for national security, due account will have to be taken of the specific characteristics of the matter. [8] Similarly, recital 13 and Article 3(2) of Directive 95/46/EC, under which an activity concerning State security is not within the scope of EU law, Article 1(3) of the e-Privacy Directive, and recital 14 of Directive (EU) 2016/680, [9] according to which inter alia an activity concerning national security should not be regarded as an activity falling within the scope of that directive.

17 Estonia notes that the European Council too has stated that Article 4(2) TEU does constitute a derogation from EU law and should not therefore be interpreted restrictively. [10]

18 Estonia therefore considers that, where the transmission and use of bulk communications data take place for the purpose and within the framework of safeguarding national security, it is protected under Article 4(2) TEU from the application of EU law and is outside the scope of the Treaties. If such activity were not covered by the protective clause in Article 4(2) TEU, that provision would be completely ineffective.

Article 1(3) of the e-Privacy Directive

19 Should the Court of Justice find that the protection of national security and the rules of law governing it do, however, fall within the scope of EU law, Estonia considers that, in the circumstances of the request for a preliminary ruling, the requirements imposed on network operators in national law to give the SIAs bulk communications data do not in any event fall within the scope of the e-Privacy Directive.

20 Article 1(3) of the e-Privacy Directive provides that the directive is not to apply inter alia to activities which fall outside the scope of the Treaty establishing the European Community, and in any case to activities concerning defence and State security. Estonia considers that the exception to the scope of the e-Privacy Directive for ensuring national security must be interpreted in the light of the

[7] Article 16 TFEU lays down the legal basis for the adoption of rules on the protection of personal data.

[8] OJ 2010 C 83, p. 345, Declaration No 20.

[9] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L 119, p. 89.

[10] European Council of 18-19 February 2016 — Conclusions (document No EUCO 1/16); Annex I, Section C, 'Sovereignty', point 5.

Treaties, since the principles laid down in primary law cannot be changed by secondary law.

21 Acts of secondary law must follow primary law, so that those acts may not be interpreted in such a way that they permit interfere with basic State functions, [11] inter alia the protection of national security of the Member States. In accordance with the principle of conferral laid down in Article 5(2) TEU, the EU must act within the limits of the competences conferred on it by primary law, and cannot validly adopt legal acts that go beyond the bounds defined by primary law for security policy. [12] The e-Privacy Directive cannot therefore regulate activity necessary for the protection of national security.

22 In accordance with Article 4(2) TEU and the principles mentioned in the preceding paragraph, the exceptions to the scope of the e-Privacy Directive are defined in Article 1(3) of the directive, and the scope of the directive may not be extended to any activity whatsoever of a Member State in the protection of national security.

23 The above extends also to a network operator's obligation to provide bulk communications data to the SIAs. The Court of Justice has previously held that the activity of a private operator transferring data is also not within the scope of the directive, if the aim of such activity is to support the basic State function of safeguarding national security within a framework established by the State. [13]

24 National legal acts regulating the supply of mass communications data with the aim of protecting national security (more precisely, ensuring intelligence and counter-intelligence activities), for example the minister's instruction at issue in the main proceedings, do not fall within the scope of the e-Privacy Directive.

25 Estonia recognises that in the *Tele2 Sverige and Watson and Others* case the Court found that the obligation of data operators both to retain mass communications data and also to give the State authorities access to that data falls within the scope of the e-Privacy Directive. [14] Estonia considers that the present case and the national rules at issue differ essentially from the *Tele2 Sverige and Watson and Others* case.

26 The *Tele2 Sverige and Watson and Others* case concerned the obligation of network operators to retain communications data **for the purpose of fighting**

[11] Opinion of the Advocate General, 30 June 2016, *Remondis*, C-51/15, EU:C:2016:504, point 41.

[12] By analogy, judgment of 16 June 2015, *Gauweiler and Others*, C-62/14, EU:C:2015:400, paragraph 41.

[13] Judgment of 30 June 2006, *Parliament* v *Council*, C-317/04 and C-318/04, EU:C:2006:346, paragraphs 56 to 59.

[14] Judgment of 21 December 2016, *Tele2 Sverige and Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 75 to 78.

crime and the conditions of access of the law enforcement authorities to that data. In that case the Court analysed **only one** of the exceptions to its scope laid down in Article 1(3) of the e-Privacy Directive, more precisely the exception for **public order**, part of which is the fight against crime. The *Tele2 Sverige and Watson and Others* case therefore allows a conclusion to be drawn only as to the kind of activity for the purpose of the fight against crime the e-Privacy Directive applies or does not apply.

27 The *Tele2 Sverige and Watson and Others* case did not concern the purposes of the other exceptions to the scope of the e-Privacy Directive laid down in Article 1(3) of the directive, or their possible difference. The judgment did not analyse measures taken to safeguard national security, more precisely acts regulating the field of intelligence and counter-intelligence, and it did not therefore make use of Article 4(2) TEU in interpreting and determining the scope of Article 1(3) of the directive.

28 The fight against crime belongs to a field of competence shared between the EU and the Member States (Article 4(2)(j) TFEU), being part of the area of freedom, security and justice (Title 5 of the TFEU). The Declaration annexed to the Final Act of the Inter-Governmental Conference which adopted the Treaty of Lisbon on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation [15] and the case-law [16] confirm that the fight against crime and measures taken for that purpose are within the scope of EU law.

29 Ensuring national security, however, is the sole responsibility of the State (last sentence of Article 4(2) TEU). The distribution of competence laid down on the basis of Article 4(1) and (2) TEU and Article 4 TFEU shows clearly the difference between activity of a Member State connected with national security and activity of the law enforcement authorities.

30 Estonia observes that the Declaration annexed to the Final Act of the Inter-Governmental Conference which adopted the Treaty of Lisbon on Article 16 TFEU [17] shows that, where rules concerning the protection of personal data adopted on the basis of Article 16 may directly affect national security, account must be taken of the specific characteristics of the matter. The conference recalls that the legislation currently applicable (cf. in particular Directive 95/46/EC) includes specific derogations in that regard. [18] When the Treaty of Lisbon was adopted, it was therefore intended to emphasise once again the exceptions

[15] OJ 2010 C 83, p. 345, Declaration No 21.

[16] Opinion 1/15 (Agreement between Canada and the EU on the tranfser of passenger name record data), 26 July 2017, EU:C:2017:592, paragraph 96.

[17].Article 16 TFEU lay down the legal basis for the adoption of rules on the protection of personal data.

[18] OJ 2010 C 83, p. 345, Declaration No 20.

concerning national security to the scope of the rules on the protection of personal data.

31 Similarly, the purpose of activity of the SIAs in the field of intelligence and counter-intelligence for the protection of national security differs essentially from criminal proceedings, even if the methods and instruments used in the activity do not necessarily always differ. For example, a basic feature of the treatment of bulk data consists in the fact that it is non-targeted and is not directed at specific known targets. The purpose of criminal proceedings is to ascertain whether a crime has been committed, collect evidence and bring a prosecution. The purpose of collecting data in the field of intelligence and counter-intelligence for protecting national security is, however, to **prevent and contain** various threats to security, which differ from one State to another and over time.

32 Taking account of the above differences between activity of a Member State connected with security and activity of the law enforcement authorities, and of the requirement to interpret the directive consistently with the Treaties, national measures regulating the forwarding of bulk communications data to the SIAs for the purpose of protecting security (such as the minister's instruction in the main proceedings to collect and supply that data) do not fall within the scope of the e-Privacy Directive. The contrary interpretation would leave Article 1(3) of the directive entirely without effectiveness.

33 In summary, Estonia considers that, in accordance with Article 1(3) of the e-Privacy Directive, interpreted in conjunction with Article 4(2) TEU and Article 5 TEU, requirements laid down in national law in the circumstances of the reference for a preliminary ruling for network operators to provide bulk communications data to the SIAs of the Member State are not within the scope of EU law and the e-Privacy Directive.

34 Estonia stresses that the State must in any event guarantee the fundamental rights of persons in accordance with its own national legal acts, the constitution and international law (especially the ECHR). State activity in the intelligence and counter-intelligence field is not therefore as it were outside the law, and the rights of persons, review before and after the event, and State liability are governed by international (especially the ECHR) and national law.

Question 2

35 Although Estonia has answered Question 1 in the negative, Estonia will also answer the first subquestion of Question 2 in case the Court of Justice should answer Question 1 in the affirmative. Estonia answers Question 2 to the effect that, if EU law and the e-Privacy Directive are applicable, then none of the *Watson* requirements [19] or other requirements beyond those imposed by the ECHR

[19] Jdgment of 21 December 2016, *Tele2 Sverige and Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 119 to 125.

apply to the national rules on the forwarding of bulk communications data to the SIAs and access to the data.

36 In the *Tele2 Sverige and Watson and Others* case the Court analysed only the proportionality of the rules on the retention and use of communications data for the **purpose of the fight against crime**, that is, their compatibility with the Charter of Fundamental Rights of the European Union ('the Charter'). The judgment did not address the proportionality of restrictions of the rights of persons for the other purposes set out in Article 15(1) of the e-Privacy Directive.

37 Estonia considers that in the present case the restriction of the fundamental rights expressed in Articles 7 and 8 of the Charter has a different purpose, so that the requirements deriving from the principle of proportionality are also different. In the *Tele2 Sverige and Watson and Others* case, there was no analysis of measures adopted for the purpose of protecting national security, more precisely acts regulating the field of intelligence and counter-intelligence, or of what is a necessary, appropriate and proportionate measure precisely in order to protect national security.

38 As explained above, the purpose of data processing carried out in the course of the SIAs' activity in the field of intelligence and counter-intelligence for the protection of national security differs essentially from the purpose of criminal proceedings. Similarly, the use of that data by the SIAs is very different from the way in which the data is used with the aim of fighting against crime and investigating crime.

39 Estonia wishes to stress the importance in the field of security of retaining communications data and using such data. Anti-State activity does not in any event take place in public, and is therefore often not easy to predict. Protection of national security is based on wide-ranging analyses, carried out by the SIAs, who act and whose acts are reviewed in accordance with specific legal acts and the constitutional order of the State.

40 In their activity the SIAs often have to react to very non-specific suggestions and ascertain activities potentially threatening to the order of the State. All the relevant activity takes place in secret, as otherwise the collection of information would no longer be effective. In assessing dangers to national security, it is not possible publicly to determine beforehand, for example, the criteria by which data of only certain categories of persons should or could be retained. That has also been recognised by the Court of Justice. [20]

41 Estonia agrees with the referring court that, if the *Watson* requirements were to be applied to the exploitation of measures taken to protect national security, including bulk communications data, that would frustrate those measures and

[20] Judgment of 21 December 2016, *Tele2 Sverige and Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 119.

critically affect the SIAs' capability of protecting national security, thereby creating a danger to the security of the Member State.

42 Estonia emphasises again that the State must in any event secure the fundamental rights of persons in accordance with its national legal acts, the constitution and international law (especially the ECHR). State activity in the intelligence and counter-intelligence field is not therefore as it were outside the law, and the rights of persons, review before and after the event, and State liability are governed by international (especially the ECHR) and national law.

43 Estonia therefore considers that, if EU law and the e-Privacy Directive are applicable, then none of the *Watson* requirements or other requirements beyond those imposed by the ECHR apply to the national rules on the forwarding of bulk communications data to the SIAs and access to the data. Since in the present case the purpose of the restriction of the fundamental rights expressed in Articles 7 and 8 of the Charter is different, the requirements deriving from the principle of proportionality are consequently also different.

V. CONCLUSION

44 Estonia proposes that the referring court's questions should be answered as follows:

1) The answer to Question 1 should be that requirements laid down in national law in the circumstances of the reference for a preliminary ruling (such as the minister's instruction) for network operators to provide bulk communications data to the security and intelligence agencies of the Member State are not within the scope of EU law and the e-Privacy Directive.

2) If, as a result of the answer to Question 1, it is necessary to answer Question 2, the answer should be that, if EU law and the e-Privacy Directive are applicable, then none of the *Watson* requirements or other requirements beyond those imposed by the ECHR apply to the national rules (such as the minister's instruction) on the forwarding of bulk communications data to the security and intelligence agencies and access to the data.

Respectfully

For the Government of the Republic of Estonia

[signature]

Amika Kalbus

Agent of the Republic of Estonia before the Court of Justice of the European Union