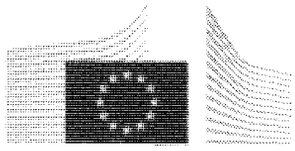

EUROPEAN COMMISSION

LEGAL SERVICE

Brussels, 20 September 2012
sj.g(2012)1276570

TO THE PRESIDENT AND THE MEMBERS OF THE COURT OF JUSTICE OF THE EUROPEAN UNION

WRITTEN OBSERVATIONS

submitted by

THE EUROPEAN COMMISSION

Represented by Dominique Maidani, Michael Wilderspin and Bernd Martenczuk, respectively Legal Advisers and Member of its Legal Service, acting as agents, with an address for service in Luxembourg at the office of Antonio Aresu, also a Member of its Legal Service, BECH Building, L-2721 Luxembourg

in Case C-293/12

Digital Rights Ireland Ltd

Plaintif

And

The Minister for Communications, Marine and Natural Resources, The Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and The Attorney General

Defendants

And

The Human Rights Commission

Notice Party

On the validity and interpretation of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ L 105, p.54)

TABLE OF CONTENTS

I. THE LEGAL BACKGROUND

I.1. The European Convention on Human Rights

1. *Article 8 – Right to respect for private and family life*

1 Everyone has the right to respect for his private and family life, his home and his correspondence.

2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

I.2. The Charter of Fundamental Rights

2. *Article 7 - Respect for private and family life*

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8 - Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

Article 52 – Scope of guaranteed rights

1. Any limitation of the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

I.3. Union Secondary law

3. Directive 95/46/EC

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 L 281, 23.11.1995, p. 31-50) sets out a number of rules of the protection of individuals with regard to the processing of personal data and on the free movement of such data.

In particular, Article 1 (1) requires Member States to protect the fundamental rights and freedoms of natural persons, and in particular their right of privacy with regard to the processing of personal data.

Article 6 sets out the principles relating to data quality.

Article 7 sets out the criteria for making data processing legitimate.

4. Directive 2002/58/EC

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 L 201, 31.7.2002, p. 37-47) provides, insofar as relevant, as follows:

Article 1

Scope and aim

1. *This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, 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.*

2. *The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.*

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 5

Confidentiality of the communications

1. *Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.*

2. *Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.*

3. *Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.*

Article 6

Traffic data

1. *Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).*

2. *Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.*

3. *For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent*

and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.

4. *The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3.*

5. *Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.*

6. *Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.*

5. Directive 2006/24/EC

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ L 105, 13.4.2006, p. 54-63) provides in pertinent part as follows:

(3) Articles 5, 6 and 9 of Directive 2002/58/EC lay down the rules applicable to the processing by network and service providers of traffic and location data generated by using electronic communications services. Such data must be erased or made anonymous when no longer needed for the purpose of the transmission of a communication, except for the data necessary for billing or interconnection payments. Subject to consent, certain data may also be processed for marketing purposes and the provision of value-added services.

(4) Article 15(1) of Directive 2002/58/EC sets out the conditions under which Member States may 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 that Directive. Any such restrictions must be necessary, appropriate and proportionate within a democratic society for specific public order purposes, i.e. to safeguard national security (i.e. State security), defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications systems.

(5) Several Member States have adopted legislation providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of criminal offences. Those national provisions vary considerably.

(6) The legal and technical differences between national provisions concerning the retention of data for the purpose of prevention, investigation, detection and prosecution of criminal offences present obstacles to the internal market for electronic communications, since service providers are faced with different requirements regarding the types of traffic and location data to be retained and the conditions and periods of retention.

(7) The Conclusions of the Justice and Home Affairs Council of 19 December 2002 underline that, because of the significant growth in the possibilities afforded by electronic communications, data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention, investigation, detection and prosecution of criminal offences, in particular organised crime.

(8) The Declaration on Combating Terrorism adopted by the European Council on 25 March 2004 instructed the Council to examine measures for establishing rules on the retention of communications traffic data by service providers.

(9) Under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), everyone has the right to respect for his private life and his correspondence. Public authorities may interfere with the exercise of that right only in accordance with the law and where necessary in a democratic society, inter alia, in the interests of national security or public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others. Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive. The adoption of an instrument on data retention that complies with the requirements of Article 8 of the ECHR is therefore a necessary measure.

(10) On 13 July 2005, the Council reaffirmed in its declaration condemning the terrorist attacks on London the need to adopt common measures on the retention of telecommunications data as soon as possible.

(11) Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive.

(12) Article 15(1) of Directive 2002/58/EC continues to apply to data, including data relating to unsuccessful call attempts, the retention of which is not specifically required under this Directive and which therefore fall outside the scope thereof, and to retention for purposes, including judicial purposes, other than those covered by this Directive.

(13) This Directive relates only to data generated or processed as a consequence of a communication or a communication service and does not relate to data that are the content of the information communicated. Data should be retained in such a way as to avoid their being retained more than once. Data generated or processed when supplying the communications services concerned refers to data which are accessible. In particular, as regards the retention of data relating to Internet e-mail and Internet telephony, the obligation to retain data may apply only in respect of data from the providers' or the network providers' own services.

(14) Technologies relating to electronic communications are changing rapidly and the legitimate requirements of the competent authorities may evolve. In order to obtain advice and encourage the sharing of experience of best practice in these matters, the Commission intends to establish a group composed of Member States' law enforcement authorities, associations of the electronic communications industry, representatives of the European Parliament and data protection authorities, including the European Data Protection Supervisor.

(15) Directive 95/46/EC and Directive 2002/58/EC are fully applicable to the data retained in accordance with this Directive. Article 30(1)(c) of Directive 95/46/EC requires the consultation of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established under Article 29 of that Directive.

(16) The obligations incumbent on service providers concerning measures to ensure data quality, which derive from Article 6 of Directive 95/46/EC, and their obligations concerning measures to ensure confidentiality and security of processing of data, which derive from Articles 16 and 17 of that Directive, apply in full to data being retained within the meaning of this Directive.

(17) It is essential that Member States adopt legislative measures to ensure that data retained under this Directive are provided to the competent national authorities only in accordance with national legislation in full respect of the fundamental rights of the persons concerned.

(...)

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Subject matter and scope

1. *This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.*

2. *This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.*

(...)

Article 3

Obligation to retain data

1. *By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.*

2. *The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the process of supplying the communication services concerned. This Directive shall not require data relating to unconnected calls to be retained.*

Article 4

Access to data

Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights.

Article 5

Categories of data to be retained

1. *Member States shall ensure that the following categories of data are retained under this Directive:*

(a) data necessary to trace and identify the source of a communication:

(1) concerning fixed network telephony and mobile telephony:

(i) the calling telephone number;

(ii) the name and address of the subscriber or registered user;

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the user ID(s) allocated;

(ii) the user ID and telephone number allocated to any communication entering the public telephone network;

(iii) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;

(b) data necessary to identify the destination of a communication:

(1) concerning fixed network telephony and mobile telephony:

(i) the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s);

(2) concerning Internet e-mail and Internet telephony:

(i) the user ID or telephone number of the intended recipient(s) of an Internet telephony call;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;

(c) data necessary to identify the date, time and duration of a communication:

(1) concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

(ii) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;

(d) data necessary to identify the type of communication:

(1) concerning fixed network telephony and mobile telephony: the telephone service used;

(2) concerning Internet e-mail and Internet telephony: the Internet service used;

(e) data necessary to identify users' communication equipment or what purports to be their equipment:

(1) concerning fixed network telephony, the calling and called telephone numbers;

(2) concerning mobile telephony:

(i) the calling and called telephone numbers;

(ii) the International Mobile Subscriber Identity (IMSI) of the calling party;

(iii) the International Mobile Equipment Identity (IMEI) of the calling party;

(iv) the IMSI of the called party;

(v) the IMEI of the called party;

(vi) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;

(3) concerning Internet access, Internet e-mail and Internet telephony:

(i) the calling telephone number for dial-up access;

(ii) the digital subscriber line (DSL) or other end point of the originator of the communication;

(f) data necessary to identify the location of mobile communication equipment:

(1) the location label (Cell ID) at the start of the communication;

(2) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.

2. No data revealing the content of the communication may be retained pursuant to this Directive.

Article 6

Periods of retention

Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

(...)

Article 9

Supervisory authority

1. *Each Member State shall designate one or more public authorities to be responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to Article 7 regarding the security of the stored data. Those authorities may be the same authorities as those referred to in Article 28 of Directive 95/46/EC.*

2. *The authorities referred to in paragraph 1 shall act with complete independence in carrying out the monitoring referred to in that paragraph.*

II. PROCEDURE BEFORE THE NATIONAL COURT

6. The Plaintiff, a limited liability company, limited by guarantee, claims it owns a mobile telephone, which was registered on the 3 June, 2006, and which it claims to have used from the date of its registration up to the present. On the 11 of August, 2006, the Plaintiff issued these proceedings against the Defendants. The Defendants comprise two different Ministers of the Government of Ireland, The Commissioner of *An Garda Síochána* (The Irish police force), the State itself and the State's Attorney General. The Irish Human Rights Commission was joined as a Notice Party to the proceedings and appears as an *Amicus Curiae.*

7. The Plaintiff seeks the following remedies:

   i) Declarations to the effect that the Minister for Communications and/or the Garda Commissioner have acted in breach of the Data Protection Acts 1998 and 2003 and in breach of EU law;

   ii) Declarations to the effect that s.63(1) of the Criminal Justice (Terrorist Offences) Act 2005 is null and void for breach of the Constitution and/or EU law; or is incompatible with Ireland's obligations under the ECHR;

   iii) A Declaration that the State has failed in its obligations to give effect to EU law;

   iv) A Declaration that Directive 2006/24/EC is null and void for breach of the TEC and/or on the grounds that it was adopted without any legal basis;

v) Reliefs including injunctive reliefs directed towards the lawfulness of a direction allegedly issued by the predecessor of the First Named Defendant under Section 110 of the Postal Telecommunications Services Act 1983 (as amended by the Interception of Postal Packets and Telecommunication Messages (Regulations) Act 1993;

vi) If necessary, a declaration that the said section, as amended, is repugnant to the Constitution of Ireland;

vii) Injunctions restraining the Defendants from acting under, or giving effect to, the impugned instruments including the EC Directive;

viii) An Order pursuant to Article 267 TFEU (ex Article 234 TEC) referring the following question to the Court of Justice for a preliminary ruling:

- Whether Directive 2006/24/EC is valid notwithstanding
  (a) Article 6(1) and (2) of the TEU
  (b) Article 3a TEU and 21 TFEU (ex Articles 10 and 18 TEC)
  (c) Articles 7, 8, 11 and 41 of the CFR, and
  (d) Article 5 TEU (ex Article 5 TEC) (the principle of proportionality).
- Whether Directive 2006/24/EC regulating data protection is invalid insofar as it lacks a correct legal basis in EU law.

ix) Damages; and

x) Such other consequential relief and costs as the Court may deem appropriate.

8. The Defendants have delivered a Defence in the proceedings in which they deny that the State has exercised control over mobile telephony data, whether wrongfully or at all. The Defendants further contend that insofar as the State has exercised control over mobile telephony data, it has done so in accordance with: (i) statute, (ii) EU law, and in particular the requirements of the TEU and the CFR, (iii) the Constitution of Ireland, and (iv) the ECHR.

9. The Plaintiff sought by notice of motion dated 6 February 2008 before the Irish High Court a preliminary reference under Article 267 TFEU (ex Article 234 TEC) of issues giving rise to the questions setting set forth in this schedule to the European Court of Justice. The Defendants brought a cross-application whereby they sought *inter alia* to challenge the standing of the Plaintiff to bring these proceedings.

10. In a judgment delivered on the 5 May 2010, the High Court held, in part in reliance upon the principle of effective judicial protection as a general principle of Community law, that the Plaintiff has *locus standi* to challenge the acts of which it complains. The High Court held that it may do so in reliance upon its right to privacy as a corporate body as recognized under Article 40.3.1 of the Constitution of Ireland Article 8 of the ECHR and Articles 7 and 8 of the Charter of Fundamental Rights and the right to communicate as an aspect of the rights of free speech and freedom of association under article 40.6.1 of the Constitution of Ireland, under Article 8 of the ECHR as regards respect for correspondence, and under Article 8 of the CFR as regards the protection of personal data. In contrast, the High Court concluded that the Plaintiff is not entitled to challenge the acts complained of in reliance of a right to family or marital privacy, or a right to travel since, obviously, these are rights which, as an artificial incorporeal legal entity, it does not have.

11. As regards the assertion of the rights to privacy and communications, the High Court went on to hold that the Plaintiff will be permitted to litigate those rights in these proceedings, not solely in is own capacity as an artificial legal person, but also on behalf of natural persons by way of an *actio popularis.*

12. The trial of the Plaintiff's action remains pending before the High Court.

13. In the Order for Reference, the national court explains that Article 29.4.6 of the Constitution of Ireland provides that no provision of the Constitution invalidates any laws enacted, acts done or measures adopted by the Irish State which are necessitated by the obligations of membership of the European Union or of the Communities, or prevents laws enacted, acts done or measures adopted by the European Union or by the Communities or by institutions thereof, or by bodies competent under the Treaties establishing the Communities, from having the force of law in the State. Accordingly, the

validity of Directive 2006/24/EC has a direct bearing on the constitutionality of the measures challenged.

14. Part 7 of the Criminal Justice (Terrorist Offences) Act 2005 is relied upon by the Defendant as a pre-existing implementation of Directive 2006/24/EC. Should the validity of the Directive be upheld, the provisions of Part 7, and any directions made under it, may be considered to have been "necessitated" by Ireland's membership of the European Union. In such circumstances, many of the measures complained of by the Plaintiff in the domestic legal proceedings would be incapable of challenge under the provisions of the Constitution of Ireland. Conversely, should Directive 2006/24/EC be invalid under European Union Law, the impugned domestic provisions are not protected by Article 29.4.10 of the Constitution of Ireland, and are amenable to challenge under other provisions of the Constitution. The questions that arise for resolution in this case under national law can therefore be resolved only when the validity of the impugned provisions of the Directive is determined in EU law.

15. The High Court of Ireland consequently stayed its proceedings and referred the following questions for a preliminary ruling:

1. Is the restriction upon the rights of the Plaintiff in respect of its use of mobile telephony constituted by the requirements of Articles 3, 4, and 6 of Directive 2006/24/EC incompatible with Article 5.4 TEU in that it is disproportionate and unnecessary or inappropriate to achieve the legitimate aims of:

(a) Ensuring that certain data are available for the purposes of investigation, detection and prosecution of serious crime? and/or

(b) Ensuring the proper functioning of the internal market of the European Union?

2. Specifically,

(i) Is Directive 2006/24/EC compatible with the right of citizens to move and reside freely within the territory of Member States laid down in Article 21 TFEU?

(ii) Is Directive 2006/24/EC compatible with the right to privacy laid down in Article 7 of the Charter and Article 8 ECHR?

(iii) Is Directive 2006/24/EC compatible with the right to the protection of personal data laid down in Article 8 of the Charter?

(iv) Is Directive 2006/24/EC compatible with the right to freedom of expression laid down in Article 11 of the Charter and Article 10 ECHR?

(v) Is Directive 2006/24/EC compatible with the right to Good Administration laid down in Article 41 of the Charter?

3. To what extent do the Treaties - and specifically the principle of loyal cooperation laid down in Article 4.3 of the Treaty on European Union - require a national court to inquire into, and assess, the compatibility of the national implementing measures for Directive 2006/24/EC with the protections afforded by the Charter of Fundamental Rights, including Article 7 thereof (as informed by Article 8 of the ECHR)?

III. LEGAL ANALYSIS

III.1. General remarks on the scheme of the Directive

16. Before analysing the questions of the national court in detail, the Commission considers it useful to explain the scheme of Directive 2006/24, in particular in the light of Directive 95/46/EC 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) and Directive 2002/58 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)[1].

17. Directive 95/46 lays down rules relating to the processing of personal data in order to protect the rights of individuals in that respect, while at the same time ensuring the free movement of those data in the European Union. However, it provides in Article 3(2) that it does 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 the processing operations concerning

[1] On this point see also the Report from the Commission to the Council and the European Parliament – Evaluation Report on the Data Retention Directive (Directive 2006/24/EC), COM(2011) 225 final, pp. 2-5.

public security, defence, State security...and the activities of the State in areas of criminal law".

18. Directive 2002/58 was adopted with a view to supplementing Directive 95/46 by provisions specific to the telecommunications sector. It is expressed to particularise and complement Directive 95/46 and, like that Directive, does not apply to activities falling outside the scope of the EC Treaty, in particular the activities of the State in areas of criminal law (Article 1).

19. Article 5(1) inter alia requires Member States to ensure the confidentiality of communications and related traffic data. In particular, it requires Member States to prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and related traffic data except when legally authorised to do so in accordance with Article 15(1).

20. Article 15(1) of Directive 2002/58 provides for a derogation in that it permits Member States to restrict certain rights and obligations in Articles 5, 6, 8 and 9 of the Directive inter alia when such a restriction is a necessary, appropriate and proportionate measure for the "prevention, investigation, detection and prosecution of criminal offences".

21. As is recorded in recitals 5 to 11 of the preamble to Directive 2006/24, several Member States had adopted legislation in reliance on Article 15 of Directive 2002/58, providing for the retention of data by service providers for the prevention, investigation, detection and prosecution of criminal offences; such provisions varied considerably, which in turn caused obstacles to the internal market for electronic communications, as the Court itself acknowledged in Case C-301/06, Ireland v European Parliament and Council[2]. At the same time, the Conclusions of the Justice and Home Affairs Council of 19 December 2002 underlined that data relating to the use of electronic communications were a valuable tool in the prevention, investigation, detection and prosecution of criminal offences, in particular organised crime[3].

---

[2] 2009 ECR I-593, in particular at paragraphs 63-72.

[3] On the background to Directive 2004/24, see generally the judgment in Ireland v European Parliament and Council, supra, in particular at paragraphs 7-11.

22. Article 1 of Directive 2006/24 specifies that its aim is to harmonise Member States' provisions concerning providers' obligations with regard to the retention of data for the purpose of the investigation, detection and prosecution of serious crime.

23. Article 3 provides a derogation from Articles 5, 6 and 9 of Directive 2002/58 by requiring Member States to ensure that certain categories of data (specified in Article 5 of Directive 2006/24) are retained by service providers.

24. Article 5 specifies the categories of fixed line and mobile telephony and internet-related data that are to be retained. Those categories were defined and included by the Commission in its proposal for a Directive. The Directive does not authorise retention of data revealing the content of the communication (Article 5(2)).

25. Article 6 requires Member States to ensure that the data are retained for not less than 6 months and not more than two years from the date of the communication.

26. Article 11 makes a consequential amendment to Article 15 of Directive 2002/58 in that it disapplies paragraph 1 thereof to data specifically required by Directive 2006/24 to be retained.

27. The question of access to data by the authorities of the Member States is not regulated by Directive 2006/24 except insofar as Article 4 thereof requires Member States to ensure that data retained pursuant to the Directive are provided to the competent authorities in specific cases and in accordance with national law (see also recital 25). Consistently with Article 3(2) of Directive 95/46 and Article 1 of Directive 2002/58, this question is not regulated by those Directives but by national law "subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights".

28. Like Directive 2002/58, Directive 2006/24 is based on Article 95 EC (now Article 114 TFEU) and is thus to be seen predominantly as an internal market measure. As the Court is well aware, a challenge to the choice of the legal basis was dismissed by the Court in Ireland v Parliament and Council, supra, in which the Court held as follows:

> *80. In that connection, the provisions of Directive 2006/24 are essentially limited to the activities of service providers and do not govern access to data or the use thereof by the police or judicial authorities of the Member States.*
>
> *81. More specifically, the provisions of Directive 2006/24 are designed to harmonise national laws on the obligation to retain data (Article 3), the categories of data to be retained (Article 5), the periods of retention of data (Article 6), data protection and data security (Article 7) and the conditions for data storage (Article 8).*
>
> *82. By contrast, the measures provided for by Directive 2006/24 do not, in themselves, involve intervention by the police or law-enforcement authorities of the Member States. Thus, as is clear in particular from Article 3 of the directive, it is provided that service providers are to retain only data that are generated or processed in the course of the provision of the relevant communication services. Those data are solely those which are closely linked to the exercise of the commercial activity of the service providers.*
>
> *83. Directive 2006/24 thus regulates operations which are independent of the implementation of any police and judicial cooperation in criminal matters. It harmonises neither the issue of access to data by the competent national law-enforcement authorities nor that relating to the use and exchange of those data between those authorities. Those matters, which fall, in principle, within the area covered by Title VI of the EU Treaty, have been excluded from the provisions of that directive, as is stated, in particular, in recital 25 in the preamble to, and Article 4 of, Directive 2006/24.*
>
> *84. It follows that the substantive content of Directive 2006/24 is directed essentially at the activities of service providers in the relevant sector of the internal market, to the exclusion of State activities coming under Title VI of the EU Treaty.*

29. Thus to summarise, Directive 2006/24 primarily provides for a solution to the internal market problem caused by divergent utilisation by the Member States of the derogation facility in Article 15 of Directive 2002/58 by providing for minimum harmonisation of the periods during which the data set out in Article 5 must be retained. At the same time, it aims to ensure, for the purposes of law enforcement in the Member States, that data are retained in all Member States and that they are made available to law enforcement authorities for a certain period[4].

---

[4] Recital 9 of the preamble.

30. Directive 2006/24 simply requires the Member States to adopt measures to ensure that the data specified in Article 5 thereof are retained for a minimum period of six months and a maximum of two years. By contrast, the Directive does not authorise retention of data revealing the content of the communication. Nor does it contain any provisions regarding access to those data, other than to stipulate they are "available for the purpose of the investigation, detection and prosecution of serious crime" (Article 1(1) and that the procedures and conditions relating to access are regulated by national law, including where relevant, other EU law provisions and international law (Article 4).

III.2. The dispute in the main proceedings and the provisions of national law in issue

31. At paragraph 13 of the judgment of the High Court of 5 May 2010, annexed to the Order for Reference, it is stated that the Plaintiff alleges that the Defendants have wrongfully exercised control over data, in that they have illegally processed and stored data relating to the Plaintiff. If the claim were limited to such allegations, the questions relating to the validity of Directive 2006/24 would not call for a reply, since, as explained above, the scope of that Directive is limited to the obligation on the part of the service provider to retain data and does not touch on the issue of access to and use of the data by law enforcement agencies.

32. Nevertheless, in the Order for Reference, (paragraph 1.3) it is explained that one of the remedies sought by the Plaintiff is a declaration that section 63(1) of the Criminal Justice Act (Terrorist Offences) Act 2005 is null and void. At paragraph 3.2, it is explained that that provision, now repealed, required service providers to retain traffic and location data inter alia for the purposes the prevention, detection, investigation or prosecution of crime. At paragraph 4, it is explained that that provision, which is relied upon by the Defendants as a pre-existing implementation of Directive 2006/24, cannot be impugned under the Constitution of Ireland if Directive 2006/24 is valid. That provision has now been repealed by the Communications (Retention of Data) Act 2011, the provision whereby Directive 2006/24 was transposed into national law. However, no remedy is sought in respect of the 2011 Act, which can no doubt be explained by the fact that the action was brought on 11 August 2006, shortly after the adoption of the Directive.

33. The Commission therefore has some doubts as to the relevance in principle and thus the admissibility of the questions referred.

34. Nevertheless, this question is specifically addressed in paragraph 4 of the Order for Reference and it appears to be common ground, as a matter of national procedural law, that the validity of Directive 2004/24 is relevant to the constitutionality of the 2005 Act.

35. Thus insofar as the Plaintiff's action is directed towards the legality of the retention, as opposed to the access to and use of, data falling within the scope of Directive 2006/24 and insofar as the validity of that directive has a bearing on the legality of national measures that are treated as transposing the Directive, the questions, or at least certain parts of them (infra, paragraph 38), would appear to be admissible.

III.3. Questions 1 and 2

i) Introductory remarks

36. By its first question, the national court has asked a general question relating to the principle of proportionality whereas, in its second question, it asks specific questions relating to the compatibility of Directive 2006/24 with rights of citizenship and various rights enshrined in the Charter of Fundamental Rights. In the Commission's view, analysis of the second question necessarily entails consideration of the principle of proportionality. Thus, in order to avoid duplication, the two questions will be addressed together.

37. A further problem with the second question is that it is subdivided in various parts. Points i), iv) and v) ask about the compatibility of the Directive with Article 21 TFEU, Article 11 of the Charter and Article 41 of the Charter respectively.

38. However, the Order for Reference contains no arguments of the Plaintiff or any other indication as to how those particular provisions could possibly have a bearing on the legality of a Directive dealing with data retention. In the Commission's view, those parts of the second question do not call for a reply.

39. In order best to assist the Court, the Commission will concentrate therefore, on points ii) and iii) of the second question which address the question of the compatibility of Directive 2006/24 with Articles 7 and 8 of the Charter and Article 8 of the European Convention on Human Rights (ECHR). They clearly represent the nub of the issue and need to be analysed in the light of the relevant case law of the Court of Justice and that of

the European Court of Human Rights. Since both Article 7 and Article 8 of the Charter are closely related and both correspond to Article 8 of the ECHR[5] the Commission will examine these provisions together.

40. Finally, since the questions of the national court refer only to the validity of Articles 3, 4 and 6 of the Directive, the Commission will confine itself to those Articles and will not, in particular, address questions of data protection and data security, which are regulated by Article 7 of the Directive, or storage requirements, regulated by Article 8.

ii) Does the retention of the data by a commercial company constitute a limitation on the rights recognised by Articles 7 and 8 of the Charter?

41. At the outset, it is necessary to recall the limited scope of Directive 2006/24. As stated above, it merely obliges Member States to require service providers to retain certain data for a period varying between 6 months and 2 years. It does not regulate access to or use of the retained data, which remain regulated by national law. Indeed, given the nature of the Directive as a first pillar instrument, it could not have regulated these questions at the time of its adoption. Nor does the Directive require the content of the communication to be retained.

42. Nevertheless, the Commission concedes that mere retention of such data does represent a prima facie interference with the rights recognised by the Charter. This flows inter alia from the judgment of the European Court of Human Rights (ECtHR) in S. and Marper v United Kingdom[6] where that Court rejected the argument of the respondent government that the mere storage, as opposed to the access to and use of, personal data did not constitute an interference with private life. The ECtHR, citing earlier case law, stated that "the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8". The EU data protection directive equally clearly recognises that the storage of personal data constitutes processing of personal data which affects the right to the protection of personal data.[7]

---

[5] According to the Explanations relating to the Charter of Fundamental Rights (2007 OJ C 303/17), Article 7 corresponds to Article 8 of the ECHR whereas Article 8 is merely based on that same provision.
[6] Applications nos. 30562/04 and 30566/04, judgment of 4 December 2008.
[7] Cf. Directive 95/46/EC, Article 2 (b).

iii) If the retention of the data constitutes an interference with privacy can it nevertheless be justified?

43. According to Article 52(1) of the Charter, any limitation on the rights and freedoms that it contains "must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others". However, by virtue of Article 52(3) of the Charter, where the Charter contains rights that correspond to rights guaranteed by the ECHR, the meaning and scope of those rights is the same as those laid down by the ECHR. The Commission notes that under Article 8 of the ECHR interference with the right of privacy may be justified if it is "in accordance with the law and is necessary in a democratic society" in the interests of a number of listed aims. However, the Commission does not consider that there is any difference of substance in the two formulations and will follow the methodology as set out in Article 52(1) of the Charter, as the Court itself did in its judgment in Schecke and Eifert[8], in particular at paragraphs 65-89.

a) Is the interference provided for by law?

44. The interference required by the Directive, namely the storage of personal data by telecommunications operators, is required in the Directive itself, as well as in the national laws transposing the Directive, and is therefore provided for by law. The fact that as regards the duration of the storage, the Directive leaves a margin to the national legislator, does not change anything in this respect, since the national legislator must define the duration in its national law.

[8] Joined Cases C-92/09 and C-93/09, 2010 ECR I-11063.

45. As regards any interference which results from the access of national law enforcement authorities to the personal data retained, it should be noted that, as explained above, this matter is not regulated in the Directive itself. Therefore, no question of justification of the Directive arises in this regard. This notwithstanding, it is to be noted that Article 4 of the Directive requires that the conditions of access by the competent authorities shall be defined by each Member State in its national law in accordance with in accordance with the requirements of the ECHR (see also Recitals 17 and 25 of the preamble to the Directive).

b) Does the legislation pursue an objective of general interest?

46. In order to address this question, it is important to bear in mind the background to adoption of the Directive[9]. Article 15(1) of Directive 2002/58 permits but does not require Member States to restrict the scope of the rights and obligations in Articles 5, 6 and 8 of that Directive. In reliance on that provision, several Member States adopted measures with a view to imposing obligations on service providers concerning the retention of such data[10]. National measures adopted differed considerably and, indeed, when Directive 2006/24 was adopted, not all Member States had enacted rules on data retention[11].

47. Directive 2006/24 thus sought to address two problems. On the one hand, a purely internal market problem existed in that the disparities between the national rules "were liable to have a direct impact on the functioning of the internal market and that it was foreseeable that that impact would become more serious with the passage of time"[12]. On the other hand, precisely because data retention had proved to be a necessary and investigative tool for law enforcement, it had become necessary to ensure that minimum rules requiring such retention in all Member States be adopted in order to ensure that such data could be made available to law enforcement authorities for a certain period[13].

---

[9] See generally recitals 4-11 of the preamble.
[10] Recitals 5 and 6, Ireland v Parliament and Council, para 66.
[11] Ibid, paras 69-70.
[12] Ireland, para 71.
[13] Recital 9 of the preamble.

48. It can scarcely be disputed that the legislation genuinely pursues both aims and that, moreover, both are legitimate.

49. As regards the internal market aim, the Court itself has acknowledged that "the differences between the various national rules... were liable to have a direct impact on the functioning of the internal market" and that this "situation justified the Community legislature in pursuing the objective of safeguarding the proper functioning of the internal market through harmonised rules[14]".

50. As regards the law enforcement aim, Recitals 7 to 11 of the preamble to the Directive clearly refer to the importance of data retention as a tool for law enforcement, and make reference to the conclusions of the Justice and Home Affairs Council of 19 December 2002, which underline this point, and to the Declaration on Combating Terrorism adopted by the European Council on 25 March 2004 which instructed the Council to examine measures for establishing rules on the retention of communications traffic data by service providers.

51. The Commission considers it axiomatic that the facilitation of the investigation, detection and prosecution of serious crime is a legitimate purpose. This point was accepted without more by the ECtHR in S. v Marper[15] and was also accepted by the Court of Justice in Case C-305/05, Ordre des barreaux francophones et germanophone[16]. Furthermore, the fact that the Directive relates predominantly to the functioning of the internal market[17] is relevant only to the choice of legal basis. It is unconnected with the question whether any interference with privacy that the Directive may entail may be justified by reference to the fight against serious crime[18]. In fact, it is entirely common that measures of harmonisation in the internal market also need to take into account secondary policy objectives from other policy areas. Where such harmonisation measures involve a limitation of fundamental rights, such secondary policy objectives can also be taken into account in the assessment of the justification of the limitation.

---

[14] Ireland, paragraphs 71 and 72.
[15] At paragraph 100.
[16] 2007 ECR I-5305.
[17] Ireland, paragraph 85.
[18] See the argument of the European Parliament to this effect in Ireland v Parliament and Council, summarised at paragraph 39, to which the Court did not demur.

c) Is the limitation on the rights conferred by Articles 7 and 8 of the Charter proportionate to the legitimate aim pursued?

52. It is settled case law that the principle of proportionality requires that measures implemented by acts of the European Union be appropriate for attaining the objective pursued and do not go beyond what is necessary to achieve it[19].

53. Before tackling each of these points, the Commission wishes to point out that the Directive did not paint a regulatory framework onto a blank canvas. On the contrary, the question of data retention was governed by Directive 2002/58, in particular by the open-ended derogation contained in Article 15(1). At the time that the Commission produced its impact assessment for the proposal for a Data Retention Directive 10 Member States had already provided in their national law some form of data retention measures[20] and these regimes presented considerable divergences, for example in relation to the categories of data that were to be retained and to the data retention periods that they established[21]. The Directive, therefore, cannot simply be seen as a piece of legislation that establishes an interference with privacy. On the contrary, taken overall, it merely regulates, by partially harmonising, existing national regimes and therefore introduces an element of predictability where none existed before. Indeed, in the Member States that had adopted data retention measures that were more far reaching than those permitted by Directive 2006/24 that Directive actually has the effect of decreasing existing interference with privacy, albeit it might be thought to have created or increased interference in other Member States. The Commission submits that in such a situation the leeway granted to the EU legislature in determining whether the interference is proportionate to the aim pursued should be relatively broad.

---

[19] Schecke and Eifert, supra, at paragraph 74.

[20] See the Impact Assessment for the Commission's proposal for the Data Retention Directive, SEC(2005) 1131, at page 6. Member States in which data retention was already provided for in national law by 2005 were Belgium, Czech Republic, Denmark, France, Ireland, Italy, Latvia, Lithuania, the Netherlands, Poland and the United Kingdom.

[21] See for example paragraph 50 of Ireland v EP and Council, supra: in Member States that had data retention regimes, data retention periods varied from three months in the Netherlands to four years in Ireland.

The general effectiveness of data retention in the fight against serious crime

54. Considerable empirical evidence[22] attests that data retention is valuable, and in some cases indispensable, for investigating and prosecuting crime. Retained data have been instrumental in providing evidence of complicity in crimes, linking witnesses to incidents and to clearing suspects without having to resort to other methods of surveillance that might be more intrusive.

55. More specifically, those data may enable the construction of a trail of evidence leading up to an offence, particularly in the context of complex organised crime structures. In the absence of forensic or eye witness evidence retained data may represent the only way to start a criminal investigation, which is often the case where internet or telecommunication services are used to commit a crime.

Are less intrusive means available and, if so, are they as effective in the fight against serious crime?

56. One alternative to data retention that has been advocated is data preservation. Data preservation is distinct from data retention in that, under the former, operators may be ordered to retain data, as from the date of the order, relating to specific individuals where there is a suspicion of criminal activity (known as "quick freeze"). It may also take a different form (known as "quick freeze plus"), whereby access may be granted to existing data that have not yet been deleted by the commercial operators. Data preservation is envisaged and used by participating States under the Council of Europe Convention on Cybercrime.

57. As yet, there has not been any publicly available evaluation of the effectiveness of data preservation as a tool for law enforcement. However, in the Commission's view, it is only logical that any form of data preservation outlined in the previous paragraph will be less effective than data retention in combating crime. Rules requiring data retention guarantee that potentially valuable data will be available for a given amount of time. Without such a guarantee, law enforcement must rely on data preservation rules. The basic "quick freeze" model does not allow access to data which were generated prior to the order to preserve data and the "quick freeze plus" model is dependent on the chance that data have not been

[22] See generally the Evaluation Report, section 5, pp. 21-25, and sources cited therein.

deleted at the moment that the order is made. Thus, the effectiveness of data preservation without data retention is wholly dependent on the commercial convenience of the operators rather than on objective criteria relating to the necessity to retain the data for the purposes of investigating and prosecuting serious crime. However, certain types of data[23] that have minimal business value and are unlikely to be retained by the commercial operators in the absence of an obligation to do so, are important and often crucial in providing the first investigative lead in serious cases.

58. In the Commission's view, this factor justifies the necessity of guaranteeing that these data will be available if needed. Directive 2006/24 strikes an appropriate balance between the requirements of law enforcement and the need to keep interference with privacy to a minimum by requiring only traffic and location data, as opposed to data revealing the content of the communication, to be retained, and subject to the implementation of data protection and data security principles. These data may be accessed only by law enforcement authorities on a case-by-case basis, in accordance with procedures laid down by national law.

Justification for the categories of data to be retained

59. The categories of telephony and internet-related data which are to be retained enable the competent authorities to identify who has been involved in a particular case of serious crime (unique identifiers, such as the calling and dialled telephone number, name and address of the user or subscriber, the internet protocol address enabling access to and use of the internet access), where the incident has taken place (the location label or cell ID at the start of mobile telephone communication), when it has taken place (the time and data of the start and end of a telephone communication and the log-in and log-off for internet access) and the means of communication (the International Mobile Equipment Identity). These technical categories were defined on the basis of the needs outlined by experts from Member States' police and judicial authorities and following consultation with service providers and discussions in Council working groups.

[23] In particular, fixed/mobile traffic data for flat-rate unlimited use contracts and pre-paid services, telephone number for incoming calls and IP addresses.

Justification for the period for retention of data provided for by the Directive

60. By virtue of Article 6, Member States are to ensure that the data specified in Article 5 are retained for a period of not less than six months and not more than two years from the date of the communication. This period differs from what was proposed by the Commission in its proposal for a Directive[24], Article 7 of which provided for a fully harmonised period of one year from the date of the communication, with the exception of data relating to electronic communications taking place using wholly or mainly the Internet Protocol which were to be retained for six months.

61. Use of the facility for Member States to provide for a period of retention going beyond 6 months in their implementing legislation has varied widely[25]. Of the 25 Member States that have successfully transposed Directive 2006/24, 8 have specified the minimum period for all or some data, 10 have a retention period of 1 year for all data and 3 have provided for a retention period of the maximum 2 year period, 2 of which in any event apply a 1 year period for internet data. Among the remaining Member States, Slovenia applies a period of 8 months (internet) and 14 months and Latvia 18 months (all data).

62. Evidence suggests that older data are particularly relied on in cases of serious crime such as terrorism, murder and child-grooming and offences that are characterised by repetition or a long period of preparation, cases of serious sexual offences, where the victim may not report the crime for months after the event and for large cross-border cases which may involve mutual legal assistance procedures. This factor led to the choice of granting the facility to retain data for a maximum period of two years, also taking into account the wide divergencies that existed before the adoption of the Directive.

---

[24] Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, COM(2005)0438 final.

[25] See the Evaluation Report, at p. 14.

III.4. Analysis of Question 3

63. The third question is clearly to be answered to the effect that such an obligation is incumbent on national courts. Such an obligation flows first and foremost directly from the Charter itself. Article 51(1) specifies that the provisions of the Charter are addressed to the Member States "when they are implementing Union law". This is confirmed by case-law of the Court, for example the judgment in Case C-275/06, Productores de Musica de España, in which the Court, stated at paragraph 68 that "Member States must, when transposing the directives [...], take care to rely on an interpretation of the directives which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order. Further, when implementing the measures transposing those directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality (see, to that effect, Lindqvist, paragraph 87, and Case C-305/05 Ordre des barreaux francophones et germanophone and Others [2007] ECR I-0000, paragraph 28)".

64. Furthermore, in Case C-115/08, Land Oberösterreich v CEZ, the Court stated at paragraph 138 that " In that regard, it must be borne in mind that, according to settled case-law which has developed in relation to Article 10 EC [Article 4(3) of the Treaty on the European Union], which is also applicable in respect of Article 192 EA, the duty imposed on Member States by those provisions to take all appropriate measures, whether general or particular, to ensure fulfilment of the obligations arising out of Community law is incumbent on all the authorities in the Member States, including, for matters within their jurisdiction, the courts. When applying domestic law the national court must, as far as is at all possible, interpret it in a way which accords with the requirements of Community law. Where application in accordance with those requirements is not possible, the national court must fully apply Community law and protect the rights conferred thereby on individuals, if necessary disapplying any provision if its application would, in the circumstances of the case, lead to a result contrary to Community law (see, inter alia, Case 157/86 Murphy and Others [1988] ECR 673, paragraph 11, and Case C-262/97 Engelbrecht [2000] ECR 1- 7321, paragraphs 38 to 40)."

65. Thus to summarise, a national court is required to interpret the national measures implementing a Directive in a manner consistent both with the Directive and with the provisions of the Charter of Fundamental Rights.

IV. CONCLUSION

66. In the light of the above, the Commission respectfully suggests that the Court should answer the questions referred for a preliminary ruling by the High Court of Ireland as follows:

Questions 1 and 2

Consideration of the questions referred has not disclosed any factors that would affect the validity of Directive 2006/24.

Question 3

A national court is required to interpret the national measures implementing a Directive in a manner consistent both with the Directive and with the provisions of the Charter of Fundamental Rights.

DOMINIQUE MAIDANI MICHAEL WILDERSPIN BERND MARTENCZUK

Agents for the Commission