Neutral Citation Number: [2015] EWCA Civ 1185

Case No: C1/2015/2612

IN THE COURT OF APPEAL (CIVIL DIVISION)
ON APPEAL FROM THE HIGH COURT OF JUSTICE, QUEEN'S BENCH DIVISION, DIVISIONAL COURT
LORD JUSTICE BEAN AND MR JUSTICE COLLINS
Cases No: CO/3655/2014; CO/3667/2014; CO3794/2014

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 20/11/2015

Before :

LORD JUSTICE PATTEN
LORD JUSTICE LLOYD JONES
and
LORD JUSTICE VOS

- -

Between :

SECRETARY OF STATE FOR THE HOME DEPARTMENT — **Appellant**

v.

(1) DAVID DAVIS MP
(2) TOM WATSON MP
(3) PETER BRICE
(4) GEOFFREY LEWIS

Respondents

(1) OPEN RIGHTS GROUP
(2) PRIVACY INTERNATIONAL
(3) THE LAW SOCIETY OF ENGLAND AND WALES

Interveners

- -
- -

James Eadie QC, Daniel Beard QC, Gerry Facenna and **Sarah Ford** (instructed by **Government Legal Department**) for the Appellant
Dinah Rose QC, Ben Jaffey and **Iain Steele** (instructed by **Liberty**) for the Respondents **Davis** and **Watson**
Richard Drabble QC, Ramby de Mello and **Azeem Suterwalla (**instructed by **Bhatia Best Solicitors)** for the Respondents **Brice** and **Lewis**

Jessica Simor QC and **Ravi Mehta** (instructed by **Deighton Pierce Glynn)** for **Open Rights Group** and **Privacy International,** intervening by way of written submissions
Tom Hickman (instructed by **Legal Services Department, the Law Society**) for **the Law Society of England and Wales**, intervening by way of written submissions

Hearing dates : 22nd & 23rd October 2015

- -

Approved Judgment

LORD JUSTICE LLOYD JONES:

1. This is the judgment of the court.

Introduction

2. This is an appeal against the order of the High Court of Justice, Queen's Bench Division, Divisional Court (Bean LJ, Collins J) dated 17 July 2015. The Divisional Court declared that section 1, Data Retention and Investigatory Powers Act 2014 ("DRIPA") is inconsistent with EU law insofar as:

   (1) it does not lay down clear and precise rules providing for access to and use of communications data retained pursuant to a retention notice to be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating to such offences; and

   (2) access to the data is not made dependent on a prior review by a court or an independent administrative body whose decision limits access to and use of the data to what is strictly necessary for the purpose of attaining the objective pursued.

   The Divisional Court also ordered that section 1, DRIPA be disapplied:

   (1) insofar as access to and use of communications data retained pursuant to a retention notice is permitted for purposes other than the prevention and detection of serious offences or the conduct of criminal prosecutions relating to such offences; and

   (2) insofar as access to the data is not made dependent on a prior review by a court or an independent administrative body whose decision limits access to the use of the data to what is strictly necessary for the purpose of attaining the objective pursued.

   The Divisional Court further ordered that the effect of the order disapplying section 1, DRIPA be suspended until after 31 March 2016.

3. The claimants before the Divisional Court, the respondents before this court, applied for judicial review of the data retention powers in section 1, DRIPA. Mr. Brice and Mr. Lewis are concerned about the width of the powers to retain and gain access to their data on a number of grounds including the confidentiality of communications with solicitors. Mr. Davis and Mr. Watson, who are both members of the House of Commons, share those concerns but also have particular concerns about the confidentiality of communications between Members of Parliament and their constituents. Their challenges are to the validity of section 1, DRIPA and the regulations made under it as being contrary to EU law, as expounded in the decision of the Grand Chamber of the Court of Justice of the European Union ("the CJEU") in

Joined Cases C/293/12 and C/594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources & Others* and *Seitlinger and Others* delivered on 8 April 2014 ("*Digital Rights Ireland*").

4. Both below and before this court the interveners, Open Rights Group, Privacy International and the Law Society of England and Wales have been permitted to intervene by way of written submissions. We are grateful to all counsel for the assistance they have given the court.

Preliminary Matters

5. DRIPA was enacted in consequence of the declaration of invalidity made by the CJEU in *Digital Rights Ireland* in relation to Directive 2006/24/EC ("the Data Retention Directive"). Both the Data Retention Directive and DRIPA are concerned with communications data. As the Divisional Court explained at paragraph 13 of its judgment, communications data does not include the content of a communication. Such data can be used to demonstrate who was communicating, when, from where, and with whom. They can include the time and duration of a communication, the number or e-mail address of the originator and recipient and sometimes the location of the device from which the communication was made. Communications data fall into three broad categories:

    (1) Subscriber data: information held or obtained by a communications service provider ("CST") in relation to a customer, for example their name, address and telephone number.

    (2) Service data: information relating to the use made by any person of a communications service and for how long, for example itemised telephone records showing the date, time and duration of calls and to what number each call was made.

    (3) Traffic data: data comprised in or attached to a communication by means of which it is being or may be transmitted, for example, who the user contacted, at what time the contact was made, the location of the person contacted and the location of the user.

6. Communications data are used by intelligence and law enforcement agencies in connection with operations relating to national security, anti-terrorism, serious crime and other operations concerning a threat to life or public safety. They can be used to identify members of a criminal network, place them in specific locations at specific times and to understand the criminal activities in which they are engaged. Communications data can be used as evidence in court.

7. Notwithstanding the fact that communications data do not include the content of communications, they can be highly revealing and informative and, as a result, highly intrusive into the privacy of users of communications services.

EU Law

EU Charter of Fundamental Rights

8. Article 6, Treaty on European Union ("TEU") provides

> "1. The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adopted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties.
>
> The provisions of the Charter shall not extend in any way the competences of the Union as defined in the Treaties.
>
> The rights, freedoms and principles in the Charter shall be interpreted in accordance with the general provisions in Title VII of the Charter governing its interpretation and application and with due regard to the explanations referred to in the Charter, that set out the sources of those provisions.
>
> 2. The Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms. Such accession shall not affect the Union's competences as defined in the Treaties.
>
> 3. Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law.

9. The Charter of Fundamental Rights of the European Union (2012/C326/02) provides:

> "Article 7
>
> Everyone has the right to respect for his or her private and family life, home and communications."
>
> Article 8
>
> 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(3)
>
> "In so far as this Charter contains rights which correspond to rights guaranteed by the [ECHR], the meaning and scope of those rights shall be the same as those laid down by the said Convention. This

provision shall not prevent Union law providing more extensive protection."

EU legislation on data retention

Directive 95/46/EC The Data Protection Directive

10. 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 ("the Data Protection Directive") provides:

"Article 1

Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data.

…

Article 3

Scope

…

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; …"

…

Article 13

Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others."

11. Chapter IV of the Directive sets out principles governing the transfer of personal data to third countries. By virtue of Article 25(1), such transfer could take place provided the third country in question ensured an "adequate level of protection" as defined in Article 25(2).

12. Article 28 of the Data Protection Directive required each Member State to provide for independent monitoring and oversight of the application within that Member State's territory of the provisions of the Directive.

Directive 2002/58/EC The e-Privacy Directive

13. Directive 97/66/EC, which was the first to address the retention and use of communications data at the EU level, was repealed and replaced by 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 ("the e-Privacy Directive").

14. Article 1(3) of the e-Privacy Directive contains the same stipulation as Article 3(2) of the Data Protection Directive.

15. Article 5 requires Member States to ensure the confidentiality of communications and related traffic data. In particular, it requires that they 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).

16. Article 6 requires that 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, subject to exceptions in paragraphs 2, 3 and 5 of Article 6 and subject to Article 15(1).

17. Article 15(1) permits Member States to adopt legislative measures to restrict the scope of the rights and obligations of the Directive in the following terms:

"Application of certain provisions of Directive 95/46/EC

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."

18. In *R (British Telecommunications plc) v Secretary of State for Culture, Olympics, Media and Sport* [2012] 2 CMLR 23 this court, following the decision of the CJEU in Case C-275/05 *Promusicae*, held that the grounds for derogation under Article 15(1) of the e-Privacy Directive include all the legitimate aims listed in Article 13(1) of the Data Protection Directive.

Directive 2006/24/EC The Data Retention Directive

19. Directive 2006/24/EC ("the Data Retention Directive") was adopted on the basis of Article 95 EC (now Article 114 TFEU), which provides that the Council shall adopt measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market.

Recital (6) states:

> "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."

Recital (25) provides that the Directive is without prejudice to the power of Member States to adopt legislative measures concerning the right of access to, and the use of, data by national authorities.

Article 1(1) provides:

> "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."

Article 3 provides:

> "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."

Article 4 provides with regard to 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 sets out in detail the categories of data to be retained. Article 6 requires that Member States shall ensure that the data are retained for periods of not less than six months and not more than two years from the date of the communication.

United Kingdom legislation

Data Protection Act 1998

20. The Data Protection Directive was implemented in the United Kingdom by the Data Protection Act 1998.

Regulation of Investigatory Powers Act 2000 ("RIPA")

21. Chapter II of Part I of RIPA set out the access regime pursuant to which certain public authorities might obtain and use communications data. Access to communications data required an authorisation by a designated person of an appropriate grade within a public authority with the requisite powers under RIPA. Section 22 provided:

> "Obtaining and disclosing communications data
>
> (1) This section applies where a person designated for the purposes of this Chapter believes that it is necessary on grounds falling within subsection (2) to obtain any communications data.
>
> (2) It is necessary on grounds falling within this subsection to obtain communications data if it is necessary—
>
> (a) in the interests of national security;
>
> (b) for the purpose of preventing or detecting crime or of preventing disorder;
>
> (c) in the interests of the economic well-being of the United Kingdom;
>
> (d) in the interests of public safety;

> (e) for the purpose of protecting public health;
>
> (f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
>
> (g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or
>
> (h) for any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State."

22. DRIPA amended s.22(2)(c) of RIPA by adding the proviso "so far as those interests are also relevant to the interests of national security". Some further purposes were specified by paragraph 2 of the Regulation of Investigatory Powers (Communications Data) Order 2010 which was itself amended in 2015.

Anti-terrorism, Crime and Security Act 2001

23. The Anti-terrorism, Crime and Security Act 2001 was enacted in response to the terrorist attacks of 11 September 2001. Part 11 addressed the retention of communication data. Section 102 allowed the Secretary of State to put in place a voluntary code of practice relating to the retention by communications providers of communications data obtained by or held by them.

Privacy and Electronic Communications (EC Directive) Regulations 2003

24. The e-Privacy Directive was implemented in the United Kingdom by the Privacy and Electronic Communications (EC Directive) Regulations 2003 (S.I. 2003/2426).

Data Retention (EC Directive) Regulations 2007 and 2009

25. The Data Retention Directive was implemented in the United Kingdom with respect to fixed network and mobile telephony by the Data Retention (EC Directive) Regulations 2007 (S.I. 2007/2199) ("the 2007 Regulations"). The 2007 Regulations were superseded by the Data Retention (EC Directive) Regulations 2009 (S.I. 2009/859) ("the 2009 Regulations"), which contain additional provisions relating to internet access, internet telephony and email.

Regulation of Investigatory Powers (Communication Data) Order 2010

26. The designated persons referred to in s.22(1) of RIPA are identified in the Regulation of Investigatory Powers (Communication Data) Order 2010. The same provisions are incorporated by reference into DRIPA.

Data Retention and Investigatory Powers Act 2014 (DRIPA)

27. In its judgment in *Digital Rights Ireland* delivered on 8 April 2014 the CJEU held that the Data Retention Directive was invalid. In the United Kingdom this put in doubt the

legal basis for requiring the continued retention of communications data under the 2009 Regulations. As a result, the Government introduced a Bill which was fast tracked through Parliament. It passed through all its stages in the House of Commons on 15 July 2014, was considered by the House of Lords on 16 and 17 July 2014 and received Royal Assent on 17 July 2014.

28. Section 1 of DRIPA provides:

> "Powers for retention of relevant communications data subject to safeguards
>
> (1) The Secretary of State may by notice (a "retention notice") require a public telecommunications operator to retain relevant communications data if the Secretary of State considers that the requirement is necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (h) of section 22(2) of the Regulation of Investigatory Powers Act 2000 (purposes for which communications data may be obtained).
>
> (2) A retention notice may-
>
> (a) relate to a particular operator or any description of operators,
>
> (b) require the retention of all data or any description of data,
>
> (c) specify the period or periods for which data is to be retained,
>
> (d) contain other requirements, or restrictions, in relation to the retention of data,
>
> (e) make different provision for different purposes,
>
> (f) relate to data whether or not in existence at the time of the giving, or coming into force, of the notice.
>
> (3) The Secretary of State may by regulations make further provision about the retention of relevant communications data.
>
> (4) Such provision may, in particular, include provision about-
>
> (a) requirements before giving a retention notice,
>
> (b) the maximum period for which data is to be retained under a retention notice,
>
> (c) the content, giving, coming into force, review, variation or revocation of a retention notice,

> (d) the integrity, security or protection of, access to, or the disclosure or destruction of, data retained by virtue of this section,
>
> (e) the enforcement of, or auditing compliance with, relevant requirements or restrictions,
>
> (f) a code of practice in relation to relevant requirements or restrictions or relevant powers,
>
> (g) the reimbursement by the Secretary of State (with or without conditions) of expenses incurred by public telecommunications operators in complying with relevant requirements or restrictions,
>
> (h) the 2009 Regulations ceasing to have effect and the transition to the retention of data by virtue of this section.
>
> (5) The maximum period provided for by virtue of subsection (4)(b) must not exceed 12 months beginning with such day as is specified in relation to the data concerned by regulations under subsection (3).
>
> (6) A public telecommunications operator who retains relevant communications data by virtue of this section must not disclose the data except-
>
> (a) in accordance with-
>
> (i) Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act 2000 (acquisition and disclosure of communications data), or
>
> (ii) a court order or other judicial authorisation or warrant, or
>
> (b) as provided by regulations under subsection (3).
>
> (7) The Secretary of State may by regulations make provision, which corresponds to any provision made (or capable of being made) by virtue of subsection (4)(d) to (g) or (6), in relation to communications data which is retained by telecommunications service providers by virtue of a code of practice under section 102 of the Anti-terrorism, Crime and Security Act 2001."

29. Section 2 defines a number of terms including "relevant communications data" which means communications data of the kind mentioned in the Schedule to the 2009 Regulations so far as such data is generated or processed in the United Kingdom by public telecommunications operators in the process of supplying the telecommunications services concerned.

30. The purposes for which a notice to retain relevant communications data may be given pursuant to section 1(1) of DRIPA are those set out in section 22(2)(a) – (h) of RIPA, with the amendment to section 22(2)(c) referred to above.

31. Section 7 requires the Secretary of State to appoint an independent reviewer of terrorism legislation to review the operation and regulation of investigatory powers. The review must consider the issues set out in s. 7(2), including the effectiveness and proportionality of existing legislation.

32. Section 8(3) is a "sunset clause" automatically repealing the Act on 31 December 2016. As a result, Parliament will have to enact new legislation if the retention regime is to continue beyond that date.

33. Section 21 of the Counter-Terrorism and Security Act 2015 amended the definition of "relevant communications data" to include data showing which internet protocol address, or other identifier, belongs to the sender or recipient of a communication. That section came into force on 13 April 2015.

The Data Retention Regulations 2014

34. The Secretary of State made Regulations on 30 July 2014, following affirmative resolutions of both Houses, in exercise of the powers contained in s.1 of DRIPA.

35. Regulation 4 makes provision in respect of retention notices as follows:

> "(1) A retention notice must specify—
>
> (a) the public telecommunications operator (or description of operators) to whom it relates,
>
> (b) the relevant communications data which is to be retained,
>
> (c) the period or periods for which the data is to be retained,
>
> (d) any other requirements, or any restrictions, in relation to the retention of the data.
>
> (2) A retention notice must not require any data to be retained for more than 12 months beginning with—
>
> (a) in the case of traffic data or service use data, the day of the communication concerned, and
>
> (b) in the case of subscriber data, the day on which the person concerned leaves the telecommunications service concerned or (if earlier) the day on which the data is changed.
>
> (3) A retention notice which relates to data already in existence when the notice comes into force imposes a requirement to retain the data for only so much of a period of retention as occurs on or after the coming into force of the notice.

> (4) A retention notice comes into force when the notice is given to the operator (or description of operators) concerned or (if later) at the time or times specified for this purpose in the notice.
>
> (5) A retention notice is given to an operator (or description of operators) by giving or publishing it in such manner as the Secretary of State considers appropriate for bringing it to the attention of the operator (or description of operators) to whom it relates."

36. Regulation 5 sets out the matters to be taken into account before giving retention notices:

> "(1) Before giving a retention notice, the Secretary of State must, among other matters, take into account—
>
> (a) the likely benefits of the notice,
>
> (b) the likely number of users (if known) of any telecommunications service to which the notice relates
>
> (c) the technical feasibility of complying with the notice,
>
> (d) the likely cost of complying with the notice, and
>
> (e) any other impact of the notice on the public telecommunications operator (or description of operators) to whom it relates.
>
> (2) Before giving such a notice, the Secretary of State must take reasonable steps to consult any operator to whom it relates."

37. Regulation 6 provides that the Secretary of State must keep a retention notice under review.

38. Regulations 7 and 8 impose obligations on public telecommunications operators who retain communications data, including: to secure its integrity and security; to protect it from accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful retention, processing, access or disclosure; to destroy the data so as to make it impossible to access if the retention of the data ceases to be authorised; and to put in place adequate security systems. Regulation 9 imposes a duty on the Information Commissioner to audit compliance with these requirements.

39. Regulation 9 requires the Information Commissioner to audit compliance with the requirements or restrictions imposed by Regulations 7 and 8.

40. Regulation 10 makes provision for the issue of codes of practice.

41. Schedule 1 specifies the types of communications data that may be retained under the Act, replicating the Schedule to the 2009 Regulations.

Retention of Communications Data Code of Practice

42. The Retention of Communications Data Code of Practice came into force on 25 March 2015. It provides guidance on the procedures to be followed when communications data is retained under Part 1 of DRIPA and the Data Retention Regulations 2014.

Acquisition and Disclosure Code of Practice

43. The Acquisition and Disclosure of Communications Data Code of Practice issued in 2007 was revised with effect from 25 March 2015. It provides guidance on the procedures to be followed when acquisition of communications data takes place under Chapter II of Part I of RIPA.

44. Paragraph 3.12 of the revised Code provides that designated persons must be independent from operations and investigations when granting authorisations or giving notices related to those operations.

45. Paragraphs 3.72 and following provide:

> "Communications data involving certain professions
>
> 3.72. Communications data is not subject to any form of professional privilege – the fact a communication took place does not disclose what was discussed, considered or advised.
>
> 3.73. However the degree of interference with an individual's rights and freedoms may be higher where the communications data being sought relates to a person who is a member of a profession that handles privileged or otherwise confidential information (including medical doctors, lawyers, journalists, Members of Parliament, or ministers of religion). It may also be possible to infer an issue of sensitivity from the fact someone has regular contact with, for example, a lawyer or journalist.
>
> 3.74. Such situations do not preclude an application being made. However applicants, giving special consideration to necessity and proportionality, must draw attention to any such circumstances that might lead to an unusual degree of intrusion or infringement of rights and freedoms, particularly regarding privacy and, where it might be engaged, freedom of expression. Particular care must be taken by designated persons when considering such applications, including additional consideration of whether there might be unintended consequences of such applications and whether the public interest is best served by the application."

46. Paragraph 3.78 provides that in the specific case of an application for communications data, which is made in order to identify a journalist's source, those law enforcement agencies with powers under the Police and Criminal Evidence Act 1984 must use the procedures of that Act to apply to a court for a production order to obtain this data.

The Decision of the Divisional Court

47. While the Divisional Court accepted that the CJEU in *Digital Rights Ireland* had only ruled on the validity of the Directive, it considered that the submission that it did not concern domestic legislation was an argument which elevated form over substance. The issue was not, as it had been in Case C-301/06 *Ireland v European Parliament*

and Council, a technical one about the jurisdictional basis of the Data Retention Directive. Rather, it was whether the EU legislature had failed to comply with the principle of proportionality in the light of the EU Charter. The CJEU had concluded that it had. Accordingly it must follow that an identically worded domestic statute would have been found to have exceeded the same limits. Similarly, it must follow from the CJEU's conclusion that the Directive did not provide sufficient safeguards to ensure effective protection of the data retained against the risk of abuse and against any unlawful access to and use of that data that in the view of the CJEU a domestic statute in identical terms would have had the same failings. (Judgment of Divisional Court at [83])

48. The Divisional Court referred to the submission by the appellant that in *Ireland v European Parliament and Council*, the CJEU had held that the provisions of the Directive were essentially limited to the activities of service providers and did not govern or seek to harmonise provisions on access to data. The Divisional Court considered it extraordinary that in *Digital Rights Ireland* the CJEU had said nothing about its reasoning in the earlier case. However it was clear that in *Digital Rights Ireland* the CJEU had held that the Directive was invalid, that it infringed the principle of proportionality in the light of Articles 7, 8 and 52(1) of the EU Charter and that it failed to provide sufficient safeguards against unlawful access to and use of retained data by public authorities. Whereas paragraphs [57]-[59] of the judgment concerned retention, paragraphs [60]-[67] concerned access. In the Divisional Court's view (at [84]-[89]), the solution to the conundrum, and the ratio of *Digital Rights Ireland*, was that the legislation establishing a general retention regime for communications data infringes rights under Articles 7 and 8 of the EU Charter unless it is accompanied by an access regime, laid down at national level, which provides adequate safeguards for those rights.

49. The Divisional Court (at [80]-[82]) rejected a submission that Article 8 of the EU Charter should be limited in its meaning and scope to that of Article 8 ECHR. Article 8 of the Charter clearly went further, was more specific and had no counterpart in the ECHR. On this basis the Divisional Court rejected the appellant's argument that EU law required the court to interpret *Digital Rights Ireland* so as to accord with the decisions of the ECtHR culminating in *Kennedy v United Kingdom.*

50. The Divisional Court (at [90]) did not interpret the judgment in *Digital Rights Ireland* as meaning that each criticism or concern expressed by the CJEU involved a fatal flaw in the legislation. However, some points were made with such emphasis that the Divisional Court considered that the CJEU had laid them down as mandatory requirements of EU law. It continued:

> "91 We put the following observations by the Court in this category:
>
> (a) The protection of the fundamental right to respect for private life requires that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary. Consequently the legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards sufficient to give effective protection against the risk of abuse and against any unlawful access to and use of that data (paragraphs 52 and 54);

> (b) Any legislation establishing or permitting a general retention regime for personal data *must* expressly provide for access to and use of the data to be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating to such offences (paragraph 61);
>
> (c) "*Above all*", access by the competent national authority to the data retained *must* be made dependent on a prior review by a court or an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued, and which intervenes following a reasoned request of those authorities (paragraph 62). [emphasis added]"

51. The Divisional Court referred (at [100]) to paragraph [68] of *Digital Rights Ireland* where the CJEU had referred to the lack of proper control in that the Directive did not require that data be retained within the EU. However, the Divisional Court did not consider that on a proper interpretation of *Digital Rights Ireland* it was necessary for restrictions on passing on information about communications data outside the EU to be embodied in statute.

52. The Divisional Court stated its conclusion (at [114]) as follows:

> "The application for judicial review succeeds. The Claimants are entitled to a declaration that section 1 of the Data Retention and Investigatory Powers Act 2014 is inconsistent with European Union law in so far as:
>
> (a) it does not lay down clear and precise rules providing for access to and use of communications data retained pursuant to a retention notice to be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating to such offences; and
>
> (b) access to the data is not made dependent on a prior review by a court or an independent administrative body whose decision limits access to and use of the data to what is strictly necessary for the purpose of attaining the objective pursued."

The appeal

53. The central issue in this appeal is the effect of the decision of the CJEU in *Digital Rights Ireland*. Subject to one matter, the respondents seek to uphold the Divisional Court's decision that the Court of Justice laid down mandatory requirements with which national legislation must comply. Furthermore, by a respondent's notice the respondents contend that the Divisional Court should have held that the observations of the Court of Justice on safeguards against removal of communications data from the EU should have been held by the Divisional Court to constitute further mandatory requirements of EU law with which DRIPA does not comply and that, for this additional reason, section 1, DRIPA should be held to be inconsistent with EU law and invalid.

54. At the hearing before us the appellant advanced three principal submissions:

(1) The CJEU in *Digital Rights Ireland* did not impose mandatory requirements which must to be applied to national legislation. It simply held that the harmonised EU scheme for data retention failed to incorporate any safeguards and therefore was not compliant with EU fundamental rights. (See paragraphs 72 – 90, below.)
(2) The EU Charter does not apply to national rules concerning access by law enforcement bodies to communications data. The judgment in *Digital Rights Ireland* cannot, therefore, be read as imposing substantive requirements on national law based on the EU Charter in areas where the Charter does not apply. (See paragraphs 91 – 106, below.)
(3) Even if EU law can impose such requirements on national data access laws, nothing in *Digital Rights Ireland* suggests that the CJEU intended to expand the content of Articles 7 and 8 of the EU Charter beyond the content of Article 8(2) ECHR. At most therefore EU law simply requires Member States to comply with Article 8(2) ECHR. (See paragraphs 107 – 115, below.)

The Data Retention Directive, Directive 2006/24/EC

55. The Data Retention Directive was adopted on the basis of Article 95 EC (now Article 114 TFEU) which gives the EU legislative competence to adopt harmonisation measures that have as their object the establishment and functioning of the internal market. Article 1(1) emphasises the harmonising objective.

Case C-301/06 *Ireland v. European Parliament and Council of the European Union*

56. In Case C-301/06 *Ireland v. European Parliament and Council of the European Union* [2009] ECR-I 593 the CJEU considered a request by Ireland to annul the Data Retention Directive on the ground that it was not adopted on an appropriate legal basis. Ireland submitted that the choice of Article 95 EC as the legal basis for the Directive was a fundamental error as neither Article 95 EC nor any other provision of the EC Treaty was capable of providing an appropriate legal basis. The sole, or at least predominant, objective of the Directive was to facilitate the investigation, detection and prosecution of crime, including terrorism. Therefore the only legal basis on which the measures it contained might be validly based was Title VI of the EU Treaty.

57. In rejecting the challenge, the Grand Chamber of the Court of Justice referred to the substantive content of the provisions.

> "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."

The Court considered (at [82]) that the measures provided for by the Directive did not in themselves involve intervention by the police or law-enforcement authorities of the Member States. It continued:

> "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."

It concluded:

> "91. … Directive 2006/24 covers the activities of service providers in the internal market and does not contain any rules governing the activities of public authorities for law-enforcement purposes."

58. It is a striking feature of the judgment of the Court of Justice in *Digital Rights Ireland* that it does not refer to its earlier decision in *Ireland v. European Parliament and Council*.

Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* and *Seitlinger and others*

59. *Digital Rights Ireland* was a request by the High Court in Ireland for a preliminary ruling. *Seitlinger* was a request by the Verfassungsgerichtshof for a preliminary ruling. The questions raised included the compatibility of the Data Retention Directive with Articles 7 and 8 of the EU Charter. At paragraphs 23 to 71 of its judgment the CJEU examined the validity of the Data Retention Directive in the light of Articles 7 and 8 of the Charter and concluded that in adopting the Directive the EU legislature had exceeded the limits imposed by compliance with the principle of proportionality. The Irish court had also asked to what extent the Treaties require a national court to inquire into and assess the compatibility of the national measures implementing the Data Retention Directive with the protections afforded by the EU Charter. However, in the light of its decision that the Data Retention Directive was invalid, the CJEU considered (at [72]) that there was no need to answer this further question.

60. The CJEU identified the main objective of the Data Retention Directive as to ensure that the data are available for the purpose of the prevention, investigation, destruction and prosecution of serious crime (the serious crime objective). It considered (at [23]–[30]) that the retention of data for the purpose of possible access by national authorities directly and specifically affected private life and fell within both Articles 7 and 8 of the Charter. It therefore proceeded to examine the validity of the Data Retention Directive in the light of those Articles of the Charter.

61. The CJEU considered (at [34]) that the obligations imposed by the Data Retention Directive to retain data constituted an interference with the rights guaranteed under Article 7 of the Charter. It then went on to state that access by national authorities to the data constituted a further interference with that fundamental right. It further considered that the Directive interfered with the rights guaranteed by Article 8 of the Charter because it provided for the processing of personal data. Although the interference with Charter rights was particularly serious, it considered that neither the retention provisions nor the access provisions of the Directive adversely affected the essence of those rights. Having regard to the objective of the Directive as stated in

Article 1(1), it concluded (at [41]-[44]) that the retention of data for the purpose of allowing the competent national authorities to have possible access to those data genuinely satisfied an objective of general interest.

62. The CJEU then turned to the issue of proportionality of the interference. Having regard to the importance of the protection of personal data and the seriousness of the interference with that right caused by the Directive, it considered (at [48]) that the discretion of the EU legislature was reduced with the result that review of that discretion should be strict. It considered that the retention of data may be considered to be appropriate for attaining the objective pursued by that Directive. However, such an objective of general interest, however fundamental it may be, did not, in itself, justify a retention measure such as that established by the Data Retention Directive being considered to be necessary for that purpose. It then stated:

> 54 Consequently, the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data: see, by analogy, as regards article 8 of the Human Rights Convention , *Liberty v United Kingdom (2008) 48 EHRR 1* ; *Rotaru's case 8 BHRC 449* , paras 57–59, and *S v United Kingdom* (2008) 48 EHRR 1169, para 99.

63. It considered that the need for such safeguards is all the greater where, as under the Data Retention Directive, personal data is subjected to automatic processing and where there is a significant risk of unlawful access to those data. The Court then drew attention to the breadth of application of the Data Retention Directive which applied to all means of electronic communication. The Court considered that it therefore entailed an interference with the fundamental rights of practically the entire European population. It then set out its criticisms of the retention provisions of the Directive.

> 57 In this respect, it must be noted, first, that Directive 2006/24 covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.
>
> 58 Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.
>
> 59 Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period

> and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.

64. The CJEU then turned to the access provisions:

> 60 Secondly, not only is there a general absence of limits in Directive 2006/24 but Directive 2006/24 also fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in article 1(1) , in a general manner to serious crime, as defined by each member state in its national law.
>
> 61 Furthermore, Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4 of the Directive, which governs the access of those authorities to the data retained, does not expressly provide that that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it merely provides that each member state is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements.

65. In the present proceedings the Divisional Court considered that paragraph 61 of *Digital Rights Ireland* gave rise to a mandatory requirement of EU law that any legislation establishing or permitting a general retention regime for personal data must expressly provide for access to and use of the data to be "strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating to such offences" (Divisional Court (at [91])).

66. The CJEU then turned to the issue of authorisation.

> 62 In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection

> or criminal prosecutions. Nor does it lay down a specific obligation on member states designed to establish such limits.

It was on the basis of this passage that the Divisional Court identified a second mandatory requirement with which the DRIPA regime did not comply: prior review by a court or by an independent administrative body. (Divisional Court at [91])

67. The CJEU criticised the provisions of the Data Retention Directive relating to the duration of retention before expressing the following conclusion:

> 65 It follows from the above that Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.

68. The CJEU then turned to consider whether the Directive provided sufficient safeguards in relation to the security and protection of retained data and concluded that it did not. In this regard it observed:

> 68 In the second place, it should be added that that Directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paras, is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data: see *European Commission v Republic of Austria (Case C-614/10) [2013] All ER (EC) 237* , para 37.

69. The Divisional Court (at [100]) referred to this passage. However, it did not consider that on a proper interpretation of *Digital Rights Ireland* it was necessary for restrictions on passing on information about communications data outside the EU to be embodied in statute. This has given rise to a respondents' notice in which the respondents invite this court to hold that section 1 of DRIPA is incompatible with EU law on the additional ground that it contains insufficient safeguards to prevent communications data from leaving the EU.

70. Finally, the Court of Justice concluded, having regard to all the foregoing considerations, that the Data Retention Directive had exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the EU Charter.

Case C-362/14 *Schrems v. Data Protection Commissioner*

71. In Case C-362/14 *Schrems v. Data Protection Commissioner* the CJEU considered a request for a preliminary ruling on the adequacy of the safe harbour privacy principles

(OJ 2000 L 215). In its judgment the Grand Chamber made the following observations concerning *Digital Rights Ireland*:

> "91 As regards the level of protection of fundamental rights and freedoms that is guaranteed within the European Union, EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must, according to the Court's settled case-law, lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data. The need for such safeguards is all the greater where personal data is subjected to automatic processing and where there is a significant risk of unlawful access to that data (judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, … paragraphs 54 and 55 and the case-law cited).
>
> 92 Furthermore and above all, protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary (judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, … paragraph 52 and the case-law cited).
>
> 93 Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail (see, to this effect, …, judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 57 to 61).
>
> 94 In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter (see, to this effect, judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 39)."

The effect of *Digital Rights Ireland*

72. The Divisional Court took the view that some, but not all, of the criticisms made by the CJEU in *Digital Rights Ireland* constitute the imposition by that court of mandatory requirements for legislation in this field which apply equally to EU legislation and to legislation by the Member States.

73. The appellant submits that the CJEU in *Digital Rights Ireland* was addressing the Data Retention Directive and whether the EU legislature in adopting that Directive had complied with the EU Charter and EU law. In the appellant's submission the CJEU found that in circumstances where the harmonised EU scheme for data retention incorporated no safeguards in relation to the access and use of retained data, that scheme was not compliant with EU fundamental rights. The approach adopted by the Court of Justice was to ask whether the EU regime included clear and precise rules governing the scope and application of the EU measure in question and imposing minimum safeguards to provide sufficient guarantees against the risk of abuse and unlawful access and use of the retained data. In identifying the type of safeguards that were absent from the EU regime, the Court of Justice was not deciding that those specific protections must, as a matter of EU law, be included in any national data retention regime.

74. We see the force of the submission that if the CJEU is laying down mandatory requirements for European legislation those requirements should apply equally to national legislation. However, the Court's observations were made in the context of a reference relating to the validity of the Data Retention Directive. The reasoning throughout is closely linked to the objective, provisions and scheme of the Data Retention Regulation. National legislation, by contrast, may not be limited to the single objective identified in that Directive. Accordingly, we consider that transposition of the observations of the Court of Justice in *Digital Rights Ireland* so as to apply them to national legislation certainly cannot be an automatic process.

75. In any event, we consider that the passages relied on by the respondents are descriptive not prescriptive. Thus at paragraphs [57]-[59] of its judgment the Court described in general terms the breadth of the provisions of the Data Retention Directive and what limitations and safeguards the Directive scheme on retention lacked. Similarly at paragraphs [60]-[62] it described the absence of limitations and safeguards in the Directive scheme on access. It is a catalogue of failings and omissions. In this regard we consider it significant that the Data Retention Directive appears to have contained no safeguards at all as to access and use of communications data and we do not, therefore, think it is obvious that the CJEU was laying down general requirements which are capable of automatic transposition and application to unspecified national legislation.

76. It is not surprising, in our view, that there was no consideration in the *Digital Rights Ireland* judgment of safeguards which may actually exist in the national legislation of Member States. The Court was concerned with the validity of the Directive and not the validity of any provision of national law. However, it seems to us that precisely what safeguards may be required must be assessed in the context of the measure concerned and, in particular, must have regard to its objectives, its breadth and such safeguards as have been included. That was the process undertaken by the CJEU in relation to the validity of the Data Retention Directive. It would be surprising, therefore, if the Court had intended to take this opportunity to lay down general requirements which were capable of automatic transposition and application to unspecified national legislation.

77. We find further support for the view that the Court of Justice was not intending in *Digital Rights Ireland* to lay down mandatory principles applicable to national legislation in the Opinion of Advocate General P Cruz Villalon in that case. He

described the issue which arose for decision (at [121]) as whether the EU may lay down such a measure "without at the same time regulating it with guarantees on the conditions to which access and use of those data are to be subject, at least in the form of principles" (emphasis added). In his view (at [123]) "the general referral to the member states [was] insufficient". Similarly, he observed:

> 124 Even accepting the division suggested by Advocate General Bot in his opinion in *Ireland v European Parliament* , and while sharing his view that it was, at that time at least, difficult to incorporate guarantees regarding access to the data retained, there was nothing to prevent the European Union legislature, in defining the obligation to collect and retain data, from accompanying that obligation with a series of guarantees at least in the form of principles, to be developed by the member states, that were intended to regulate use of the data and, thereby, to define the exact extent and complete profile of the interference which that obligation entails. (emphasis added)

This suggests that the Advocate General, at least, was not looking for the Directive to provide detailed regulation. It lends some weight to the view that the Court was addressing the general failure of the Directive to lay down such principles and accords with our view that it was the lack of principled guidance in the Directive which led to its invalidity.

78. We also note in this regard that the High Court in Ireland in its reference had asked a separate question concerning the extent to which the Treaties require a national court to inquire into and assess the compatibility of the national measures implementing the Data Retention Directive with Article 7 of the Charter and that the Court (at [72]) considered that, in view of its conclusion that the Directive was invalid, there was no need to answer this further question.

79. One difficulty faced by the respondents is that it is not possible to convert all of the critical observations of the CJEU into mandatory requirements. Many are simply too general. This led the Divisional Court (at [90]) to distinguish between different observations of the CJEU and to conclude that some imposed mandatory obligations whereas others did not. While the greater degree of particularity with which some of the observations are expressed makes such an approach possible, we doubt that it is correct. The Divisional Court distinguished those observations imposing mandatory requirements from those which do not on the basis of the emphasis with which they were stated by the CJEU. We do not consider this a satisfactory basis of distinction. If the CJEU was intending to lay down mandatory requirements in some matters but not in others, we would expect that it would have made that intention clear by an express statement to that effect.

80. It is therefore our provisional view that the Court of Justice in *Digital Rights Ireland* was not laying down specific mandatory requirements of EU law but was simply identifying and describing protections that were entirely absent from the harmonised EU regime. The Court's conclusion that the Data Retention Directive was unlawful was compelled by the cumulative effect of what was not in the Data Retention Directive. As the Stockholm Administrative Court of Appeals put it in the reference which is now pending before the Court of Justice as Case C-203/15 *Tele2 Sverige AB*, it came to that conclusion "on an overall assessment".

(a) Serious crime

81. The Divisional Court considered that paragraph 61 of *Digital Rights Ireland* gave rise to a mandatory requirement of EU law that national legislation permitting access to retained communications data must be limited to the objective of the prevention, detection or prosecution of a serious crime. It explained (at [94]-[95]) that this requirement does not mean that access must be limited to the data of people suspected to have committed a serious criminal offence. It also considered (at [96]) that the definition of serious crime is a matter for national legislatures, provided that the relevant offences are precisely defined and can properly be regarded as serious. It therefore made a declaration that section 1, DRIPA is inconsistent with EU law in so far as it does not lay down clear and precise rules providing for access to and use of communications data retained pursuant to a retention notice to be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating to such offences.

82. On the hearing of this appeal, Ms. Rose on behalf of the first and second respondents did not seek to persuade us that that the Divisional Court's conclusion on this point was correct. Rather she accepted that the CJEU in paragraph [61] of its judgment was not restricting the purpose for which access may lawfully be given to this sole objective. We understand Mr. Drabble to have taken the same position. It is now accepted by the respondents, therefore, that this passage in the judgment of the CJEU relates to the objective of the Data Retention Directive and that it cannot give rise to a mandatory requirement which applies to national legislation which may have different objectives.

83. This concession was correct in our view. In *Digital Rights Ireland* the CJEU was concerned with a Directive which states in Article 1 that its objective is to harmonise Member States' provisions concerning the obligations of service providers and public communications networks with regard to the retention of data "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". The judgment in *Digital Rights Ireland* has to be read in this context. The CJEU was here addressing whether the provisions made necessary and proportionate provision to attain the stated objective of the Directive. It was not saying that this is the only permissible objective for national legislation concerning access to retained communications data. In particular, it was not saying that other objectives, such as those set out in section 22(2) of RIPA and adopted by section 1(1) of DRIPA, are impermissible or unlawful.

84. Limiting the power of Member States to legislate for access to retained data only where it is necessary and proportionate for purposes relating to serious crime, would conflict with the more extensive powers of derogation enjoyed by Member States in EU law, (for example as identified in Article 13(1) of the Data Protection Directive and Article 15 of the e-Privacy Directive). If applied to access to communications data generally, this approach would also trespass into territory which is outside the scope of EU law and to which, accordingly, the EU Charter has no application. (See Article 3(2) of the Data Protection Directive; Article 1(3) of the e-Privacy Directive; Article 52(1) of the EU Charter). Moreover, the jurisprudence of the ECtHR provides no support for the proposition that data retention or access must be restricted to the purpose of the investigation, detection and prosecution of serious crime. (See, for example, *Kennedy v. United Kingdom* (2011) 52 EHRR 4.) More generally, this

demonstrates a need for caution in transposing the observations of the Court of Justice in *Digital Rights Ireland* in relation to the Data Retention Directive and applying them to the legislation of Member States.

85. Ms Rose now submits instead that paragraph 60 of the CJEU's decision in *Digital Rights Ireland* gives rise to a mandatory requirement of compliance with a high threshold of seriousness for any justification for a provision granting access to retained data. She submits that whatever the purpose may be, it must meet a defined threshold of seriousness. While we would certainly accept that the more serious the interference with fundamental rights, the more serious the justification must be, we are unable to accept that the CJEU was here intending to lay down a mandatory requirement which could justify a national court in holding national legislation invalid without a detailed consideration of the legislative scheme under challenge. The principle contended for is insufficiently specific to lead to such a result.

(b) Prior judicial or independent administrative approval

86. The Divisional Court (at [98]-[99]) was satisfied on the basis of paragraph [62] of *Digital Rights Ireland* that EU law requires a court or an independent administrative body to give prior approval for access and it held DRIPA invalid on this ground.

87. Here, the respondents point to the specific wording used by the CJEU which lends support to the view that it was laying down a mandatory requirement automatically applicable to national legislation. Nevertheless, we doubt that this was the intention of the Court of Justice. We note that the observation was made in a context where there was no provision at all under the Directive for approval for access. Moreover, we consider that it would be surprising if the CJEU were here seeking to lay down a mandatory minimum standard of universal application without referring to any of the relevant case law and without any consideration of the competing considerations. The question whether the imposition of such a general requirement of prior independent authorisation goes beyond the previous ECHR case law and, if so, the relevance of that fact to the present issue, are considered in a later section of this judgment.

(c) Removal of retained communications data from the EU

88. In its judgment the CJEU referred (at [68]) to the lack of proper control in that the Directive did not require the data to be retained within the EU. In the present case the Divisional Court concluded that on a proper interpretation of Digital Rights Ireland it was not necessary for restrictions on passing on information about communications data outside the EU to be embodied in statute. The basis on which it came to that conclusion is unclear. However, for reasons stated above, it is our provisional view that the CJEU was not seeking to impose mandatory requirements on national legislation and was simply addressing the inadequacies of the Data Retention Directive.

89. Mr. Eadie QC, on behalf of the appellant, submitted that EU law on the transfer of personal data to third countries is governed by the Data Protection Directive which is implemented in the United Kingdom by the Data Protection Act 1998. That Act makes provision for independent regulatory oversight by the Information Commissioner and implements Articles 25 and 26 of the Data Protection Directive concerning the transfer of personal data to third countries. He submitted, therefore,

that the concern expressed by the Court of Justice in *Digital Rights Ireland* in relation to the Data Retention Directive may not arise in the national context because all communications data which may be required to be retained under DRIPA must be processed in accordance with the Data Protection Act 1998. However, this point was not fully argued before us and, as it is not necessary to decide the point, we express no concluded view on this matter.

90. For these reasons, it is our provisional view that the judgment of the CJEU in *Digital Rights Ireland* does not lay down mandatory requirements of EU law with which national legislation must comply.

The scope of the EU Charter

91. The appellant submits that the limited exercise in which the CJEU was engaged in *Digital Rights Ireland* is apparent from the fact that the EU Charter does not apply to national rules concerning access by law enforcement bodies to communications data. The judgment in *Digital Rights Ireland* was based expressly on an assessment of whether the Data Retention Directive was compatible with the EU Charter. However, the Charter only applies to Member States when they are "implementing" EU law. National laws governing access to retained communications data by the police or other law enforcement bodies are not implementing EU law because there is no provision of EU law that regulates those activities, except in the specific context of EU cross-border co-operation. The judgment of the CJEU cannot therefore be read as imposing substantial requirements on national law based on the EU Charter in areas where the Charter does not apply.

92. Article 51(1) of the EU Charter provides that the provisions of the Charter are addressed to the Member States "only when they are implementing EU law". These words are to be interpreted widely and, in effect, mean whenever a Member State is acting within the material scope of EU law. (Case C-617/10 *Åkerberg Fransson* [2013] ECR 105; [2013] STC 1905; *Rugby Football Union v Consolidated Information Ltd* [2012] UKSC 55; [2012] 1 WLR 3333 at [28]; *R (Zagorski) v Secretary of State for Business, Innovation & Skills* [2010] EWHC 3110 (Admin); [2011] HRLR 6, at [66]-[71]).

93. It is helpful to refer to certain propositions which were not in dispute between the parties. It is common ground that national rules requiring data retention by communications service providers are within the scope of EU law and are subject to the requirements of the EU Charter. Furthermore, it is common ground that such national rules are subject to Article 15(1) of the e-Privacy Directive which provides for derogation on grounds which include "national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences". Article 15(1) permits retention of data for a limited period but provides that all derogating measures must be in accordance with the general principles of EU law, including those referred to in Article 6(1), TEU which gives effect to the EU Charter. Thus, the appellant accepts that national data retention regimes must comply with Article 15.

94. It is also common ground that EU law has not harmonised the law on access to communications data by the police or intelligence services. Article 1(2) of the Data Protection Directive and Article 1(3) of the e-Privacy Directive both provide that they

shall not apply to activities outside the scope of Community law and shall not apply to activities concerning public security, defence, State security (including the economic well-being of the State when activities relate to State security matters) and the activities of the State in areas of criminal law.

95. The provisions of the Data Retention Directive were essentially limited to the activities of service providers and did not govern access to data or the use of data by the police or judicial authorities of the Member States. It was intended to harmonise the national rules by means of provisions which are essentially limited to the retention of data. (See Case C-301/06 *Ireland v European Parliament and Council of the European Union* at [80]; *Digital Rights Ireland* per Advocate General P. Cruz Villalón at [41].)

96. The appellant draws attention to the fact that the Treaties themselves contain a number of provisions emphasising the competence of the Member States to act in this area and their essential interests in doing so, which EU law must respect. In particular, Article 4(2) TEU requires the EU to respect the Member States' essential State functions, including ensuring territorial integrity, maintaining law and order and safeguarding national security. Article 72 TFEU makes clear that the provisions of Title V of the TFEU do not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security. The appellant draws attention to Article 3(2) of the Data Protection Directive and Article 1(3) of the e-Privacy Directive, referred to above. The appellant also draws attention to the conclusion of the CJEU in *Ireland v Parliament* that measures relating to access to data by law enforcement authorities fell outside the Article 95 EC legal base of the Data Retention Directive.

97. The appellant submits that there are no other provisions of EU law that regulate such matters except in the specific context of EU cross-border co-operation. The appellant draws our attention to a proposed Directive on the processing of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (COM/2012/010). However that proposal has not been adopted. It would not, in any event, apply to activities that fall outside the scope of EU law.

98. Against this background the appellant submits that it follows that when adopting domestic legislation relating to the access and use of communications data by the police or other law enforcement bodies, Member States are not implementing EU law. It is submitted that the EU Charter has no application and that it would be remarkable if the judgment in *Digital Rights Ireland* were to lay down mandatory requirements based on the Charter for national data access laws.

99. We consider that the retention of communications data pursuant to a direction by a Member State necessarily falls within the scope of EU law and, in particular, Article 5 of the e-Privacy Directive. The storage of such data would require to be legally authorised in accordance with Article 15 which, in turn, requires the authorising measures to be in accordance with general principles of EU law which now include the EU Charter. It is in that context that the CJEU in *Digital Rights Ireland* has considered it necessary to evaluate the provisions of the Data Retention Directive relating to access to retained data by reference to the standards in the EU Charter.

100. In *Digital Rights Ireland* both the Advocate General and the CJEU considered that rules on access do fall to be evaluated by reference to general principles of EU law, including the EU Charter, as a part of the process of assessing the lawfulness of retention provisions. Although the CJEU in *Digital Rights Ireland* did not expressly address the question of the scope of EU law, it stated:

> "32 By requiring the retention of the data listed in article 5(1) of Directive 2006/24 and by allowing the competent national authorities to access those data, Directive 2006/24 … derogates from the system of protection of the right to privacy established by Directives 95/46 and 2002/58 with regard to the processing of personal data in the electronic communications sector, Directives which provided for the confidentiality of communications and of traffic data as well as the obligation to erase or make those data anonymous where they are no longer needed for the purpose of the transmission of a communication, unless they are necessary for billing purposes and only for as long as so necessary. "

It then went on to hold (at [34] and [35]) that the provisions of the Data Retention Directive relating to retention (Articles 3 and 6) and access (Articles 4 and 8) constituted an interference with the rights guaranteed by Article 7 of the EU Charter.

101. An explanation for this result is, however, provided in the Opinion of the Advocate General at [121] – [123].

> "121 It has been stated and repeated that Directive 2006/24 , as indicated in article 4 thereof, regulates neither *access* to the data collected and retained nor their use, and indeed it could not in the light of the division of areas of competence between the member states and the European Union: see point 122 et seq of the opinion of Advocate General Bot in *Ireland v European Parliament [2009] ECR I-593* ; see also the first indent of article 3(2) of Directive 95/46 , and Framework Decision 2008/977 . However, the issue which now arises is precisely that of whether the European Union *may* lay down a measure such as the obligation to collect and retain, over the long term, the data at issue without at the same time regulating it with guarantees on the conditions to which access and use of those data are to be subject, at least in the form of principles. It is this very regulation of the conditions for access and use of the collected and stored data which makes it possible to assess the scope of what that interference entails in practical terms and which may, therefore, determine whether or not the interference is constitutionally acceptable.
>
> 122 There is, in fact, an intimate relationship between the specific configuration of the obligation to collect and retain data and the circumstances in which those data are, where appropriate, made available to the competent national authorities and used by them. It must even be considered that, without knowing how that access and use may take place, it is not really possible to reach an informed judgment on the interference resulting from the collection and retention at issue.
>
> 123 While taking into consideration the fact that the legal basis of Directive 2006/24 was that of ensuring the proper functioning of the internal market and that all the detailed rules for access to the data and their use could not be included in its provisions, the "creating" effect of the obligation that data be collected and retained which it contains meant that it should have been accompanied by a series

> of guarantees in the form of principles, as a necessary and essential addition. To that end, the general referral to the member states is insufficient and cannot be remedied by the system of protection laid down by Directive 95/46 (see the first indent of article 3(2) of Directive 95/46) or by Framework Decision 2008/977 (article 1(2) of Framework Decision 2008/977 and recitals (7) and (9) in the Preamble) since they are not applicable."

102. We consider, therefore, that *Digital Rights Ireland*, a decision of the Grand Chamber of the CJEU which is binding on this court, establishes that when evaluating the lawfulness of a retention regime for communications data it is necessary to evaluate the safeguards in respect of access to the retained data. To this extent, provisions in relation to access fall within the scope of EU law and require to be evaluated by general principles of EU law including the EU Charter.

103. Nevertheless, the CJEU was here concerned with a Directive which established a regime for retention. Having regard to this context it would, in our view, be surprising if the CJEU had intended to lay down definitive mandatory requirements for an access regime which lies outside the scope of EU law save to the extent that it is incidentally relevant to the retention regime. As the appellant submits, this would involve the CJEU in legislating in relation to national rules on access to data, where such rules are not implementing EU law and where there is no EU law basis for imposing such requirements. Moreover, it would be doing so in an area where the EU Treaties specifically recognise the Member States' essential interests and responsibilities. It seems to us more likely, therefore, that the CJEU was simply pointing to the failure of the Data Retention Directive to provide any safeguards in this regard.

104. We also note that the CJEU in *Digital Rights Ireland* did not expressly address the extent to which EU law and the EU Charter apply to national access regimes. It seems to us that there is force in the appellant's submission that the CJEU was not, in fact, considering the application of mandatory requirements to domestic access regimes and that, therefore, it did not need to consider this matter.

105. The appellant also identifies a practical difficulty in this regard. If the CJEU did intend to lay down mandatory requirements for access it would be doing so only in relation to data which is accessible as a result of obligations imposed on service providers to retain it. It would not be doing so in relation to other categories of personal data where access would remain outside the scope of EU law and a matter for the Member States. This would be likely to result in different requirements for access depending on the basis on which it was available. This may be dismissed as no more than an inevitable consequence of the fact that access is outside the scope of EU law save to the extent that it impinges on retention. However, this would result in an impracticable situation, given that domestic access regimes do not treat access to data retained by a commercial service provider differently from other sources of data. This may, therefore, make it less likely that the CJEU intended in *Digital Rights Ireland* to lay down mandatory requirements for access.

106. We consider, therefore, that the considerations set out above support our provisional view that the CJEU in *Digital Rights Ireland* was not laying down definitive mandatory requirements in relation to retained communications data.

Digital Rights Ireland **and the ECHR jurisprudence on surveillance**

107. The Divisional Court held (at [80]–[82]) that Article 8 of the EU Charter as applied by the Court of Justice in *Digital Rights Ireland* clearly went further and was more specific than the provisions of the ECHR and accordingly rejected the appellant's submission that it was required to interpret *Digital Rights Ireland* so as to accord with the decisions of the ECtHR on Article 8 ECHR. It considered that *Kennedy v. United Kingdom* (2011) 52 EHRR 4 was distinguishable on the ground that it was a case about the interception of material relating to one individual pursuant to a case-specific warrant signed personally by the Secretary of State, whereas *Digital Rights Ireland* concerned "a general retention regime on a potentially massive scale". The Divisional Court considered itself bound to apply the standards which it considered had been prescribed by the Court of Justice in *Digital Rights Ireland*.

108. On behalf of the appellant it is submitted that even if EU law is capable of imposing substantive requirements in respect of national laws governing the ability of police and other law enforcement authorities to access and use retained data, EU law simply requires Member States to comply with Article 8(2) ECHR. It is submitted that there is nothing in the judgment of the CJEU in *Digital Rights Ireland* to suggest that it intended to expand the content of Articles 7 and 8 of the EU Charter beyond the content of Article 8(2) ECHR. In particular, it is said that the CJEU cannot be taken to have intended to go beyond established ECHR jurisprudence either by limiting access to retained data to cases where it is justified for the purposes of the prevention, detection or prosecution of serious crime, or by requiring "a prior review carried out by a court or by an independent administrative body". This, it is said, lends further support to the view that the Court of Justice in *Digital Rights Ireland* was not intending to lay down mandatory requirements for national legislation.

109. Mr. Eadie, on behalf of the appellant, submits that the EU Charter is not a free-standing source of rights but a catalogue of rights that already existed as general principles of EU law. Furthermore, he submits that both Article 7 and Article 8 of the Charter correspond to Article 8(1) ECHR and, by virtue of Article 52(3) of the Charter, must be given the same meaning and scope as Article 8(1) ECHR as interpreted by the European Court of Human Rights.

110. Article 52(3) of the Charter provides that in so far as the Charter contains rights which correspond to rights guaranteed by the ECHR, the meaning and scope of those rights shall be the same as those laid down by the ECHR. It goes on to provide that that provision shall not prevent EU law from providing more extensive protection. The Explanations relating to the Charter of Fundamental Rights (2007/C 303/02) ("the Explanations") state that this paragraph is intended to ensure the necessary consistency between the ECHR and the Charter. Article 7 of the Charter obviously corresponds to Article 8 ECHR and must therefore be given the same meaning and scope. We are, however, unable to accept Mr. Eadie's submission that Article 8 of the Charter must also be read in a manner consistent with the meaning and scope of Article 8 ECHR. Article 8 of the Charter is clearly closely connected with Article 7 of the Charter but Article 8 is a provision developed to guarantee the safeguards necessary in its specific field. The Explanations state that Article 8 is based on Article 286 of the Treaty establishing the European Community (now Article 16 TFEU and Article 39 TEU) and the Data Protection Directive as well as on Article 8 of the ECHR and on the Council of Europe Convention of 28 January 1981 for the

Protection of Individuals with regard to Automatic Processing of Personal Data. While its underlying principles may be derived from the protection of the right to privacy in Article 7, it is not limited by that provision. We agree with the Divisional Court that Article 8 of the Charter is more specific than Article 8 ECHR and is not limited in its meaning and scope to that of Article 8 ECHR. In our view, it has no counterpart in the ECHR.

111. However, we doubt that the CJEU in *Digital Rights Ireland* did in fact intend to go beyond the case law of the Strasbourg court and lay down more stringent requirements for the protection of personal data than those established in the ECHR jurisprudence. We have set out earlier in this judgment the reasons for our provisional conclusion that the CJEU did not intend to lay down mandatory requirements with which national legislation must comply. Furthermore, we doubt that the CJEU was intending to impose stricter requirements than those under Article 8 ECHR in the two matters in respect of which the Divisional Court held that the DRIPA regime did not meet the standards required by EU law.

112. Had the CJEU held in *Digital Rights Ireland* that the effect of the EU Charter was to limit access to retained data to cases where it is justified for the purposes of the prevention, detection or prosecution of serious crime, this would have represented a dramatic departure from the ECHR jurisprudence which acknowledges a number of other grounds of justification. However, we consider that the Divisional Court's conclusion on this point is based on a misreading of the judgment. As we have seen, the respondents no longer seek to uphold the conclusion of the Divisional Court on this point.

113. So far as concerns a possible requirement of a prior review carried out by a court or by an independent administrative body, the respondents are able to point to paragraph 62 of the judgment in *Digital Rights Ireland* in which the CJEU expresses with a striking degree of particularity the failure of the Directive to make access by the national authorities to the data retained "dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions".

114. In this regard we have been taken to a number of authorities on the ECHR. In *Kennedy v. United Kingdom* (2011) 52 EHRR 4 the ECtHR accepted prior authorisation of individual warrants by the Secretary of State even where the interception of content was concerned. However, as we have seen, the Divisional Court considered that this was distinguishable on the ground that it was concerned with an individual warrant and not mass surveillance. It is certainly correct that the ECtHR has consistently maintained that

> "… in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge." (*Klass and others v. Federal Republic of Germany* (1978) 2 EHRR 214 at [56]. See also *Rotaru v. Romania* (App.No. 28431/95 at [59]; *Kennedy v. United Kingdom* (2011) 52 EHRR 4 at [167])

However, it has not gone so far as to impose a general requirement of prior judicial or independent administrative approval as a necessary safeguard. Rather, its approach seems to be to review all aspects of the authorisation and oversight regime and to assess whether it provides overall sufficient protections to democratic freedoms. (See, generally, David Anderson QC, A Question of Trust, Report of the Investigatory Powers Review, June 2015 at [5.40] – [5.43].) In both *Klass* and *Kennedy* the ECtHR was prepared to accept as adequate the independent supervision available. In *Telegraaf Media Nederland Landelijke Media BV v. The Netherlands* (2013) No. 39315/06 at [97] – [102], on the other hand, the ECtHR distinguished this general approach, considering that, in cases of the targeted surveillance of journalists in order to discover their sources, prior review by an independent body with the power to prevent or terminate it was necessary. Here it made the point that the confidentiality of journalistic sources cannot be restored once it is destroyed.

115. What is said in *Digital Rights Ireland* about prior independent authorisation does seem, therefore, on its face, to go further than the current ECHR case law. This, however, reinforces our doubt that the CJEU in *Digital Rights Ireland* was intending to lay down mandatory requirements. The judgment of the CJEU contains no reference to the ECHR case law in this area. If it did intend to expand the requirements for prior authorisation, it gave no reasons for doing so. Indeed, the judgment includes no principled statement of the justification for such a general extension, nor does it contain any assessment of the competing interests in play here. The Divisional Court, in accepting that the CJEU had gone further than the case law of the ECtHR, noted that it had not given any explanation of why it had done so but considered that it was its prerogative not to explain. For our part, given the fundamental importance of the law on data protection to the public at large and its significance, in particular to the fight against crime and the maintenance of national security, we consider it most improbable that the Grand Chamber should have intended to effect such a major change in the law in such a way.

Reference to CJEU

116. The Divisional Court considered an application on behalf of the appellant that it request a preliminary ruling from the CJEU as to the effect of its judgment in *Digital Rights Ireland*. It refused the application for the following reasons.

(1) It was not the domestic court of last resort. While it did not doubt that the questions raised were of general importance, it did not consider that to refer the case to Luxembourg was likely to promote the uniform application of the law throughout the EU. The CJEU had already given general guidance in *Digital Rights Ireland* and Member States have different regimes governing the retention of and access to communications data.

(2) The fact that the Stockholm Administrative Court of Appeals had referred the issue to the CJEU in Case C-203/15 *Tele2 Sverige AB* did not mean that it should do the same. Courts in four other Member States had held their domestic legislation to be in breach of EU law on the basis of *Digital Rights Ireland* without making a reference.

(3) The request was made too late. DRIPA was enacted on 17 July 2014. The present proceedings were issued on 13 August 2014 and permission to apply for judicial

review was granted on 8 December 2014. If a request was to be made on the ground that the judgment in *Digital Rights Ireland* was so difficult to comprehend that only the CJEU itself could say what it meant, the application should have been made at an early stage.

(4) DRIPA contains a sunset clause which means that it will expire on 31 December 2016. It was unlikely that an answer to a reference would be received before the Act expired and the answer would have become academic.

117. In the light of our provisional view as to the effect of *Digital Rights Ireland*, we have to reassess the question whether a reference should be made. In our view the following considerations carry considerable weight.

(1) Although the CJEU has pronounced in *Digital Rights Ireland*, there is, with respect, considerable doubt as to the effect of its decision. On this, we have the misfortune to have come to a provisional view which differs from that of the Divisional Court.

(2) This is an issue of general and wide-reaching importance. Notwithstanding the expiry of DRIPA on 31 December 2016 it will not become academic. On the contrary, the true effect of the judgment in *Digital Rights Ireland* will remain central to the validity of all future legislation enacted by the Member States in this field.

(3) A factor which carries particular weight in our minds and which dissuades us from proceeding to deliver judgment on the basis of our provisional view is the fact that courts in six other Member States, including five courts of final appeal, have apparently applied *Digital Rights Ireland* in holding national legislation invalid.

(a) Austrian Federal Constitutional Court, Decision G 47/2012 e.a. regarding data retention, 27 June 2014;

(b) Slovenian Constitutional Court, Decision U-I-65/13-19, 3 July 2014;

(c) Belgian Constitutional Court, Decision 84/2015, 11 June 2015;

(d) Romanian Constitutional Court, Decision No. 440, 8 July 2015;

(e) District Court of the Hague, Netherlands, Case No. C/09/480009/KG ZA 14/1575, Decision of 11 March 2015;

(f) Slovak Constitutional Court, Decision PL. US 10/2014, 29 April 2015.

(4) If we were to proceed to decide the case, it is highly likely that on an appeal to the Supreme Court (or an application to the Supreme Court for permission to appeal) that court, as the court of final appeal, would consider that it was bound to make a reference to the CJEU. The making of a reference now would, therefore, be likely to shorten the time before a definitive answer can be obtained from the CJEU.

(5) While we are mindful of the volume and importance of other matters pending before the CJEU, we hope that that court may look favourably on a request from this court for the expedition of a reference. We also hope that it might be possible

to join a request for a reference from this court to that made by the Stockholm Administrative Court of Appeals now pending as Case C-203/15 *Tele2 Sverige AB.*

118. In these circumstances we have come to the conclusion that we should refer the following questions to the CJEU:

(1) Did the CJEU in *Digital Rights Ireland* intend to lay down mandatory requirements of EU law with which the national legislation of Member States must comply?

(2) Did the CJEU in *Digital Rights Ireland* intend to expand the effect of Articles 7 and/or 8, EU Charter beyond the effect of Article 8 as established in the jurisprudence of the ECtHR?

We consider that the answers to these questions of EU law are not clear and are necessary in order for us to give judgment in these proceedings. For the reasons set out above, we exercise our discretion in favour of making a reference to the CJEU.

119. We will hear the parties as to the form of the order for reference and the precise terms of the questions to be referred. We will also hear the parties on any applications in respect of interim relief.