Neutral Citation Number: [2015] EWHC 2092 (Admin)

Case No: CO/3665/2014, CO/3667/2014, CO/3794/2014

IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
DIVISIONAL COURT

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 17/07/2015

Before :

LORD JUSTICE BEAN
and
MR JUSTICE COLLINS

- -

Between :

THE QUEEN **on the application of** **(1) DAVID DAVIS MP** **(2) TOM WATSON MP** **(3) PETER BRICE** **(4) GEOFFREY LEWIS**	**Claimants**
- v -	
THE SECRETARY OF STATE FOR THE HOME DEPARTMENT	**Defendant**
-and -	
OPEN RIGHTS GROUP **PRIVACY INTERNATIONAL** **THE LAW SOCIETY OF ENGLAND AND WALES**	**Interveners**

Dinah Rose QC, Ben Jaffey and **Iain Steele** (instructed by **Liberty**) for the Claimants **Mr Davis** and **Mr Watson**
Richard Drabble QC, Ramby de Mello, Azeem Suterwalla and **James Dixon (**instructed by **Bhatia Best)** for the Claimants **Mr Brice** and **Mr Lewis**
James Eadie QC, Daniel Beard QC and **Sarah Ford** (instructed by **Government Legal Department**) for the **Defendant**
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 : 4-5 June and 9 July 2015

- - - - - - - - - - - - - - - - - - - -

Approved Judgment

Lord Justice Bean :

This is the judgment of the court to which we have both contributed.

1. The claimants in three separately issued claims, which we heard together, apply for judicial review of the data retention powers in section 1 of the Data Retention and Investigatory Powers Act 2014 ("DRIPA"). Mr Brice and Mr Lewis, the claimants for whom Mr Drabble QC appeared, are concerned about the width of the powers to retain and gain access to their data on a number of grounds, including (but not limited to) the confidentiality of communications with solicitors. Mr Davis and Mr Watson, who are joint claimants in case CO/3794/2014, do so as members of the House of Commons who share those general concerns but also in addition have particular concerns about the confidentiality of communications to and from constituents. Mr Davis is Conservative MP for Haltemprice and Howden; Mr Watson is Labour MP for West Bromwich East.

2. Permission to seek judicial review was initially refused on the papers by Blake J but was granted at an oral hearing by Lewis J on 8th December 2014. Lewis J also permitted Open Rights Group and Privacy International to submit an intervention by way of written submissions (on terms that the interveners would bear their own costs). We granted an application by the Law Society made shortly before the hearing to intervene by way of written submissions on the same basis.

3. The challenge is to the validity of s 1 of DRIPA and the Regulations made under it as being contrary to European Union law, as expounded in the decision of the Grand Chamber of the Court of Justice of the European Union ("the CJEU") in *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others* and the conjoined case of *Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others* delivered on 8th April 2014 and reported at [2015] QB 127. We shall refer to this decision as "*Digital Rights Ireland*".

4. At common law, Acts of the United Kingdom Parliament are not open to challenge in the courts. But the position under EU law is different. Decisions of the CJEU as to what EU law is are binding on the legislatures and courts of all Member States. The subtleties of the relationship between UK domestic courts and the European Court of Human Rights at Strasbourg arising, since 2000, from the duty under s 2(1) of the Human Rights Act 1998 to "take account" of the jurisprudence of that court, do not arise. The claimants (as a fallback to their EU law arguments) have pleaded an alternative claim for a declaration under s 4 of the HRA 1998 that s 1 of DRIPA is incompatible with their Convention rights; but this was scarcely mentioned in oral argument. Indeed, as will be seen later in this judgment, it was mainly counsel for the Home Secretary, not counsel for the claimants, who asked us to take account of the jurisprudence of the Strasbourg court in support of his arguments.

5. The present claims involve, as did *Digital Rights Ireland*, the CJEU's interpretation of Articles 7 and 8 of the Charter of Fundamental Rights of the EU. Article 7 provides:

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

Article 8 provides:

> "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."

The first of these Articles is in identical terms to Article 8(1) of the ECHR, except that the word "correspondence" is replaced by "communications". The second has no counterpart in the ECHR.

6. In *Rugby Football Union v Consolidated Information Services Ltd (formerly Viagogo Ltd)* [2012] 1 WLR 3333 Lord Kerr of Tonaghmore JSC, with whom the other Justices of the Supreme Court agreed, said at paragraphs 27-28:-

> "The Charter was given direct effect by the adoption of the Lisbon Treaty in December 2009 and the consequential changes to the founding treaties of the EU which then occurred. Article 6(1) of the Treaty on European Union (TEU) now provides:
>
> > "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 adapted 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."
>
> Although the Charter thus has direct effect in national law, it only binds member states when they are implementing EU law - article 51(1). But the rubric, "implementing EU law" is to be interpreted broadly and, in effect, means whenever a member state is acting "within the material scope of EU law".…….Moreover, article 6(1) of TEU requires that the Charter must be interpreted with "due regard" to the explanations that it contains."

7. The Secretary of State's Detailed Grounds of Defence are thus correct in stating at paragraph 38 that "the test of validity of the Act [DRIPA] and the 2014 Regulations is whether they are compliant with Articles 7 and 8 of the EU Charter and/or Article 8 ECHR." Data protection law has been within the scope of EU law for 20 years. The Data Protection Act 1998 was enacted to implement the Data Protection Directive (95/46/EC). The Explanations referred to in the Charter and printed in the Official Journal of the EU make it clear that Article 8 of the Charter was based on Article 286 of the Treaty establishing the European Community (as amended) and on the Data Retention Directive, among other sources. This is not a case in which any party has argued that Article 8 of the Charter lies outside the proper scope of EU law, although it will be seen that there is a dispute as to whether it covers access to data as well as retention.

8. Article 52(3) of the Charter provides:-

> "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."

9. The Secretary of State prays in aid the first sentence; the Claimants the second. As to the second, Mr Eadie submitted that it does not entitle the CJEU (or this court) to hold that the scope of anyone's rights has been extended by virtue of the Charter, since it was not intended to give fresh rights but to consolidate existing rights. This approach, he submitted, is confirmed by Protocol 30 to the EU Treaties, negotiated by the UK and Poland, which provides:-

> "The Charter does not extend the ability of the Court of Justice, or any court or tribunal of Poland or of the UK, to find that the laws, regulations or administrative provisions or action of Poland or of the UK are inconsistent with the fundamental rights, freedoms and principles that it reaffirms.
>
> In particular, and for the avoidance of doubt, nothing in Title IV of the Charter creates justiciable rights applicable for Poland or the UK except in so far as Poland or the UK has provided for such rights in the national law." [Title IV is not relevant in this case]

10. The precise scope of Protocol 30 is far from clear, since it only precludes the *extension* by the CJEU or domestic courts of their existing powers to find that UK laws are not in accordance with the Charter. It cannot be used to prevent the court from defining the extent of rights contained in the Charter which set out provisions within the material scope of EU law.

11. The extent of the State's powers to require the retention of communications data and to gain access to such retained data are matters of legitimate political controversy both in the UK and elsewhere. The Queen's Speech opening the new Parliament on 27 May 2015 indicated that "new legislation will modernise the law on communications data". To take one example from abroad, on 2 June 2015 the US Congress passed one

statute (the USA FREEDOM Act) restricting the data retention powers previously conferred by another statute passed in 2001 (the USA PATRIOT Act). It is not our function to take sides in this continuing debate, nor to say whether in our opinion the powers conferred by DRIPA are excessive or not. We have to decide the comparatively dry question of whether or not they are compatible with EU law as expounded by the CJEU in *Digital Rights Ireland*.

12. On 11 June 2015, a few days after the main hearing before us had concluded, the Government published "A Question of Trust", a 373-page report on the operation and regulation of investigatory powers by David Anderson QC, Independent Reviewer of Terrorism and Security Legislation. His report was rightly described by the Prime Minister in a statement to Parliament as thorough and comprehensive. We allowed the parties to make short written submissions to us about it.

Communications data

13. The phrase "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 email address of the originator and recipient, and sometimes the location of the device from which the communication was made. They do not include the content of any communication: for example the text of an email or a conversation on a telephone. Communications data comprise three broad categories:

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

    (b) 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; and

    (c) 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.

14. Communications data are used by the intelligence and law enforcement agencies during investigations regarding national security and organised and serious crime. They enable investigators to identify members of a criminal network, place them in specific locations at given times and in certain cases to understand the criminality in which they are engaged. They can be used as evidence in court.

15. As the Home Secretary said in a statement to the House of Commons on 10 July 2014:

> "Communications data has played a significant role in every Security Service counter-terrorism operation over the last decade. It has been used as evidence in 95 per cent of all serious organised crime cases handled by the Crown Prosecution Service. And it has played a significant role in the investigation of many of the most serious crimes in recent time, including the Oxford and Rochdale child grooming cases, the murder of Holly Wells and Jessica Chapman and the murder of Rhys Jones. It can prove or disprove alibis, it can identify associations between potential criminals, and it can tie suspects and victims to a crime scene."

16. Similarly, in his March 2015 Report, the Interception of Communications Commissioner, Sir Anthony May, explained:

> "My inspectors identified that communications data was frequently relied on to provide both inculpatory and exculpatory evidence. The communications data acquired revealed suspects movements and tied them to crime scenes. It often led to other key evidence being identified or retrieved. Links to previously unidentified offenders and offences were revealed. Dangerous offenders were located and offences were disrupted with the assistance of communications data. Patterns of communication provided evidence of conspiracy between suspects. The data highlighted inconsistencies in accounts given by suspects and corroborated the testimony of victims. The data determined the last known whereabouts of victims and persons they had been in contact with. Similarly, communications data assisted to eliminate key suspects or highlighted inconsistencies in accounts given by victims."

EU legislation on data retention

The Data Protection Directive

17. 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") contained provisions designed to ensure the free movement of personal data between Member States and to protect individuals' fundamental rights and freedoms, in particular their right to privacy.

18. Article 3(2) provided that the Directive did not apply to the processing of personal data which fell outside the scope of Community law, and in any case to processing operations concerning public security, defence, State security (including the economic wellbeing of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.

19. Article 13(1) preserved the right of Member States to enact domestic provisions to restrict the scope of the obligations and rights set out in the Directive where necessary

to safeguard inter alia national security; defence; public security; and/or the prevention, investigation, detection and prosecution of criminal offences.

20. Chapter IV of the Directive set 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).

21. 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 97/66/EC

22. The retention and use of communications data was first addressed at EU level by Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector ("Directive 97/66/EC").

23. Article 1(3) of Directive 97/66/EC contained the same stipulation as Article 3(2) of the Data Protection Directive to the effect that it did not apply to activities which fell outside the scope of Community law, such as those provided for by Titles V and VI of the EU Treaty, or in any case to activities concerning public security, defence, State security or the activities of the State in areas of criminal law.

24. Article 14 of Directive 97/66/EC reiterated Article 13(1) of the Data Protection Directive in providing that Member States may adopt domestic legislative measures to restrict the rights laid down in the Directive where necessary inter alia to safeguard national security, defence, public security or the prevention, investigation, detection and prosecution of criminal offences.

The e-Privacy Directive

25. Directive 97/66/EC 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").

26. Again, Article 1(3) of the e-Privacy Directive provided that it did not apply to activities which fell outside the scope of Community law, or in any case to activities concerning public security etc. Following the pattern of the Data Protection Directive and Directive 97/66/EC, Article 15(1) authorised Member States to adopt domestic legislation to restrict the rights and obligations contained in 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 or the electronic communications 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."

27. Article 5 of the e-Privacy Directive requires that the confidentiality of communications be ensured *except* when access is legally authorised in accordance with Article 15(1). This permits legislation to restrict the scope of the rights otherwise protected by the 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 electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC [the Data Retention Directive]. 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 the paragraph."

The Data Retention Directive

28. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC ("the Data Retention Directive") sought to harmonise the communications data retention arrangements across the EU.

29. The need for an EU-wide approach arose from an increasing recognition by the Member States of the importance of communications data for the investigation, detection and prosecution of crime, coupled with the differences between national data retention regimes which were creating barriers to free movement of services in the internal market. These matters are recorded in the recitals to the Data Retention Directive:

> "(5) Several Member States have adopted legislation providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of criminal offences. Those national provisions vary considerably.
>
> (6) The legal and technical differences between national provisions concerning the retention of data for the purpose of prevention, investigation, detection and prosecution of criminal offences present obstacles to the internal market for electronic communications, since service providers are faced with different requirements regarding the types of traffic and

> location data to be retained and the conditions and periods of retention.
>
> (7) The Conclusions of the Justice and Home Affairs Council of 19 December 2002 underline that, because of the significant growth in the possibilities afforded by electronic communications, data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention, investigation, detection and prosecution of criminal offences, in particular organised crime…
>
> (9)…Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive. The adoption of an instrument on data retention that complies with the requirements of Article 8 of the ECHR is therefore a necessary measure…
>
> (11) Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive…
>
> (21) Since the objectives of this Directive, namely to harmonise the obligations on providers to retain certain data and to ensure that those 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, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of this Directive, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty…"

30. 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.

31. Article 1 of the Data Retention Directive emphasised this harmonising objective:

> "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."

32. The Data Retention Directive specified the categories of data to be retained and imposed certain requirements relating to the security and storage of retained data. Article 6 imposed an obligation on each Member State to ensure that the specified communications data were retained by telecommunications providers for periods of not less than six months and not more than two years.

33. Article 4 of the Data Retention Directive provided that:

> "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."

Ireland v European Parliament and Council

34. In Case C-301/06 *Ireland v. European Parliament & Council* (ECLI:EU:C:2009:68; [2009] 2 CMLR 37) Ireland sought to argue before the CJEU that the Data Retention Directive was invalid and that it could not properly have been based on former Article 95 EC, because its principal focus was not the functioning of the internal market but the investigation, detection and prosecution of crime. That argument was rejected by the Grand Chamber of the Court of Justice. The Court observed that:

> "…the Community legislature may have recourse to Article 95 EC in particular where disparities exist between national rules which are such as to obstruct the fundamental freedoms or to create distortions of competition and thus have a direct effect on the functioning of the internal market".

35. It found that Article 95 EC was the correct legal basis for the Data Retention Directive, in particular because:

(a) "the differences between the various national rules adopted on the retention of data relating to electronic communications were liable to have a direct impact on the functioning of the internal market" and "such a situation justified the Community legislature in pursuing the objective of safeguarding the proper functioning of the internal market through the adoption of harmonised rules";

(b) the Directive amended the e-Privacy Directive, which was also based on Article 95 EC. In so far as amendment of that Directive was within the scope of Community (i.e. 'First Pillar') powers, the Data Retention Directive could not be based on (what was at the time) a 'Third Pillar' provision of the EU Treaty relating to police and judicial cooperation in criminal matters, without infringing the separation put in place by (what was at the time) Article 47 of the EU Treaty;

(c) the provisions of the Data Retention Directive were essentially limited to the commercial activities of communications service providers and did not govern access to, or use of, data by the police or judicial authorities of the Member States (paragraph 80 of the judgment). It regulated operations that were independent of the implementation of any police and judicial cooperation in criminal matters and harmonised "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……..have been excluded from the provisions of that Directive, as is stated in particular in recital 25 to the preamble to, and Article 4 of, the Directive."

36. At paragraph 57 of its judgment the CJEU said:-

> "It must also be stated that the action brought by Ireland relates solely to the choice of legal basis and not to any possible infringement of fundamental rights arising from interference with the exercise of the right to privacy contained in Directive 2006-24"

That challenge was to come in *Digital Rights Ireland.* Before coming to that case it is convenient to set out the relevant UK domestic legislation prior to 2014.

Domestic legislation

Data Protection Act 1998

37. As we have noted, the Data Protection Directive was implemented in the UK by the Data Protection Act 1998. Section 6 and Schedule 5 provide for independent oversight by the Information Commissioner. The eighth of the data protection principles listed in Schedule 1 to the Act, together with the derogations in Schedule 4 to the Act, implement Articles 25 and 26 of the Data Protection Directive concerning the transfer of personal data to third countries.

38. The safeguards in the Data Protection Act applied to access to communications data. However, there was no mandatory data retention regime. Security, intelligence and law enforcement agencies making use of communications data were obliged to rely solely on data routinely retained by communications companies for their own purposes.

Regulation of Investigatory Powers Act 2000 ("RIPA")

39. 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, headed "Obtaining and disclosing communications data", provided:-

> "(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) 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."

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 limited additional 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

40. Following the terrorist attacks in the United States on 11 September 2001, the Anti-terrorism, Crime and Security Act 2001 put in place arrangements for the retention of communications data by communications providers pursuant to a voluntary code of practice so that they could be accessed by the security, intelligence and law enforcement agencies.

Privacy and Electronic Communications (EC Directive) Regulations 2003

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

Data Retention (EC Directive) Regulations 2007 and 2009

42. 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 contained additional provisions relating to internet access, internet telephony and email.

Regulation of Investigatory Powers (Communications Data) Order 2010

43. This statutory instrument set out the office holders designated for the purposes of chapter II of RIPA and thus permitted to grant authorisations or give notices under that statute. The same provisions are incorporated by reference into DRIPA. An example is that a police superintendent may give a notice in relation to traffic data or service data but a police inspector may give a notice in relation to subscriber data.

Digital Rights Ireland

44. In *Digital Rights Ireland* the CJEU held that the Data Retention Directive was invalid. The reasoning of the CJEU in *Digital Rights Ireland* is so central to the present case that we set it out in full in Appendix 1.

45. The invalidation of the Data Retention Directive by the CJEU put in doubt the legal basis for requiring the continued retention of communications data under the 2009 Regulations. Although the 2009 Regulations remained in force, they had been made under s. 2(2) of the European Communities Act 1972 to implement the Data Retention Directive and were already subject to a legal challenge that had been stayed pending the outcome of the *Digital Rights Ireland* case. We were told that following the *Digital Rights Ireland* judgment, some CSPs expressed the view that there was no legal basis for them to continue to retain communications data, and indicated that they would start to delete data that had been retained under the 2009 Regulations.

46. The absence of a clear legal power to require communications data to be retained threatened the ability of UK law enforcement and intelligence agencies to use communications data to investigate criminal activity and protect the public. The fact that DRIPA was a response to *Digital Rights Ireland* is apparent from the opening words of the long title of the statute, describing it as: "An Act to make provision, in consequence of a declaration made by the Court of Justice of the European Union in relation to Directive 2006/24/EC, about the retention of certain communications data……". Mr Regan's evidence notes that the Bill 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, and received the Royal Assent on 17 July.

The 2014 Act (DRIPA)

47. Section 1 of DRIPA provides as follows:

"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."

48. Section 2 of the Act includes a number of definitions, 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".

49. The purposes for which a notice to retain relevant communications data may be given pursuant to s.1(1) of DRIPA are those enumerated in s.22(2)(a)-(h) of RIPA, as set out above, with the amendment to s 22(2)(c) which we have noted.

50. Section 8(3) of DRIPA is a "sunset clause": it provides that the Act "is repealed" on 31 December 2016, thus putting the onus on Parliament to enact new primary legislation by that time.

51. 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

52. 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.

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

> "4.— Retention notices
>
> (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."

54. Regulation 5 sets out the matters that the Secretary of State must take into account before giving retention notices:

> "5.— 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."

55. Regulation 6 requires the Secretary of State to keep a retention notice under review.

56. 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.

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

58. Regulation 10 of the Regulations makes provision for the issue of codes of practice.

Retention of Communications Data Code of Practice

59. The Retention of Communications Data Code of Practice came into force on 25 March 2015. It provides further guidance as to the procedures to be followed when communications data is retained pursuant to s.1 DRIPA and the Regulations.

Acquisition and Disclosure Code of Practice

60. The Acquisition and Disclosure of Communications Data Code of Practice issued in 2007 was revised with effect from 25 March 2015, inter alia to reinforce the independence of the authorising officer from the specific investigation for which the communications data is required. 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".

61. In the case of communications data involving certain professions, the revised Code provides as follows:

> "3.72 Communications data is not subject to any form of professional privilege – the fact that a communication took place does not disclose what was discussed, considered or advised.
>
> 3.73 However the degree of interference with privacy 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 (such as a medical doctor, lawyer, journalist, Member of Parliament, or minister 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 privacy, and clearly note when an application is made for the communications data of a medical doctor, lawyer, journalist, Member of Parliament, or minister of religion. Particular care must be taken by designated persons when considering such applications. That such an application has been made must be recorded (see section 6 on keeping of records for more details)."

The scope of Article 15(1) of the e-Privacy Directive

62. One issue raised in the skeleton arguments, particularly that submitted on behalf of the first and second interveners, was that s1 of DRIPA was in breach of EU law on the simple grounds that it allows retention of traffic data for purposes other than those expressly permitted by article 15 of the e-Privacy Directive, namely "to safeguard national security (i.e. state security), defence, public security and the prevention, investigation, detection and prosecution of criminal offences". Since the list of purposes permitted by s22(2) of RIPA, and therefore by s1 of DRIPA, goes beyond this list, it was submitted that the statute can be seen to be incompatible on its face without reference to the EU Charter or the judgment in *Digital Rights Ireland*. The argument was taken up by counsel for the claimants.

63. However, Mr Eadie drew our attention to the inclusion in article 15(1) of the e-Privacy Directive of a reference to article 13(1) of the Data Protection Directive; and to the fact that in *R (British Telecommunications PLC) v Secretary of State for Culture, Olympics, Media and Sport* [2012] Bus LR 1766 the Court of Appeal, following the decision of the CJEU in *Promusicae* (Case C-275/06), held that the grounds for derogation under article 15(1) of the e-Privacy Directive included the

purposes listed in article 13(1) of the Data Protection Directive. The claimants accept that this decision is binding on us but reserve the point should the present case go to the Supreme Court. We therefore need say no more about it.

Retention notices

64. The evidence before us does not include, even in a redacted form, the contents of any retention notice. In his evidence on behalf of the Secretary of State Paul Regan, Head of the Counter-Terrorism Legislation and Investigatory Powers Unit in the Home Office, states that the Home Office does not intend to publicise either the content of such notices or the identity of the CSPs to whom they are given. He explains:-

> "…This is because to do so would risk undermining national security and the prevention and detection of crime and for reasons of commercial confidentiality. To provide a confirmation or denial as to whether a notice has been given to a specific CSP or to disclose any details of such a notice would allow interested parties to determine the extent and scope of work in this area. This would provide an insight into what the limit or scope of operation capability might be. Information concerning operation capability in respect of law enforcement and national security is highly sensitive information. It would be of significant value to criminal or terrorist groups. If, for example, the Home Office were to confirm that no notice had been given to a particular company, criminals and terrorists may choose to use that company rather than companies they know or suspect could be subject to a notice."

65. Mr Eadie accepted that the consequence of this policy stance is that we should test the validity of DRIPA on the assumption that the retention notices issued under it may be as broad in scope as the statute permits, namely a direction to each CSP to retain all communications data for a period of 12 months. The case was argued on both sides on that basis. We shall refer in this judgment to a system under which the State may require CSPs to retain all communications data for a period as a "general retention regime".

66. It was also accepted on all sides that it is unnecessary for any of the Claimants to show that public authorities have in fact acquired their communications data. The ECHR said in *Weber and Saravia v Germany* (2008) 46 EHRR SE5 at [78]:

> "The Court further notes that the applicants, even though they were members of a group of persons who were likely to be affected by measures of interception, were unable to demonstrate that the impugned measures had actually been applied to them. It reiterates, however, its findings in comparable cases to the effect that the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an

> interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them."

The Investigatory Powers Tribunal has adopted the same approach in this jurisdiction: see *Liberty v GCHQ and others* [2015] 3 All ER 142 at paragraph 4(ii).

Privilege

67. The Code of Practice issued by the Secretary of State states that communication data will not be subject to legal professional privilege since there will be no access to the contents of retained communications. The Law Society made written submissions which challenge the correctness of this statement. Reliance is placed on a dictum of Cotton LJ in *Gardner v. Irvin* (1878) 4 Ex D 49 at 83 where he said:-

> "I think that the plaintiffs are not entitled to have the dates of the letters and such other particulars of the correspondence as may enable them to discover indirectly the contents of the letters, and thus to cause the defendants to furnish evidence against themselves in this action".

This approach was confirmed by Vinelott J in *Derby v. Weldon (No 7)* [1990] 1 WLR 1156.

68. No doubt such an example of privilege would rarely arise. However, communications with practising lawyers do need special consideration. The same in our view can properly be said to apply to communications with MPs. The Code of Practice makes clear the need for such special attention.

The claimants' case on Digital Rights Ireland

69. The Claimants make numerous criticisms of DRIPA on the merits. As we have already observed, we are not concerned with those, but with whether s 1 of the Act is incompatible with the requirements of EU law as interpreted by the CJEU in *Digital Rights Ireland.* Ms Rose's skeleton argument suggested that the CJEU decided that data retention legislation, if it is to be compatible with EU law, must:

i) restrict retention to data which relates to public security, and in particular restrict retention to a particular time period, a geographical area and/or suspects or persons whose data would contribute to the prevention, detection or prosecution of serious criminal offences [paragraph 59];

ii) provide for there to be exceptions for persons whose communications are subject to an "*obligation of professional secrecy*" (including Members of Parliament, lawyers and journalists) [58];

iii) restrict access and use of the data to the purposes of prevention, detection or prosecution of defined, sufficiently serious crimes [60-61];

iv) "*above all*" ensure that an independent administrative or judicial body carries out a prior review of decisions regarding access to the data on the basis of what is strictly necessary [62];

v) ensure destruction of the data when it is no longer required [67]; and

vi) ensure the data is kept within the EU [68].

70. In oral argument Ms Rose modified her stance on point (i). She accepted that the CJEU cannot have meant that CSPs can only lawfully be required to retain the communications data of "suspects or persons whose data would contribute to the prevention, detection or prosecution of serious criminal offences". Such a restriction would be wholly impracticable. Rather the Court must be understood to have held that a general retention regime is unlawful unless it is accompanied by an access regime which has sufficiently stringent safeguards to protect citizens' rights set out in Articles 7 and 8 of the Charter.

The defendant's case on Digital Rights Ireland

71. Mr Eadie submitted that in *Digital Rights Ireland* the CJEU:

i) did not explain why they thought it necessary to go beyond the jurisprudence of the Strasbourg court on the protection of ECHR Article 8 rights, and must therefore be understood not to have intended to do so;

ii) were not dealing with a challenge to any Member State's domestic legislation;

iii) could not have been laying down requirements for access regimes to comply with EU law, since in *Ireland v Parliament* the Court had held that access regimes were not the province of EU law;

iv) decided only that the Data Retention Directive taken as a whole was invalid, not that each specific aspect of it commented on in the judgment was non-compliant with the Charter.

72. Mr Eadie and his team, in their supplementary submissions following the publication of the Anderson report, cited Mr Anderson's observations at 5.78 of his report on *Digital Rights Ireland*. We set out paragraphs 5.77-5.79 in full:

> "5.77. The Grand Chamber of the CJEU is the apex of the judicial pyramid where EU law is concerned, and its conclusions are strictly binding. The extent to which current UK law gives effect to the requirements of *Digital Rights Ireland* is disputed in the MPs' case referred to at 5.75 above, which will be heard in the High Court in June 2015. In the circumstances, it would be inappropriate for me to venture an opinion on its legal compatibility.
>
> 5.78. There are however powerful arguments against an over-broad interpretation of the *Digital Rights Ireland* judgment. In particular:
>
> (a) What the Grand Chamber said about prior independent authorisation (5.68(f), above), seems to go further than the case law of the ECtHR but without explaining why. See, for example, *Kennedy v UK* (not cited by the Grand Chamber), in

which the ECtHR accepted prior authorisation of individual warrants by the Secretary of State even where the interception of content was concerned.

(b) Though the CJEU was prepared to describe data retention as a "*particularly serious*" infringement of fundamental rights, concrete examples of harm are not provided and are not immediately evident.[95] While there may be some for whom the retention of data "*is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance*"(*Digital Rights Ireland*, para 37), the survey evidence suggests that this is putting it rather high.[96]

(c) There is a case for excluding the use of retained communications data in relation to the most trivial of offences (5.67(e) above). But if the mark for "*serious crime*" is set too high, damaging crimes will go needlessly unpunished and public confidence in law enforcement will be reduced.

(d) To limit retention to "*particular persons likely to be involved, in one way or another, in a serious crime*", and/or to "*persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences*"(*Digital Rights Ireland*, para 59), would not only reduce the effectiveness of data retention in identifying targets but would carry other risks, since to seek to apply such nebulous distinctions would be to court allegations of prejudice, profiling and unlawful discrimination.

5.79. The wider implications of the judgment also need to be reflected upon. Though *Digital Rights Ireland* did not concern the bulk interception of content, it is arguable that its principles (including in relation to prior independent authorisation) should apply in that area with at least the same force. Indeed the CJEU stated in terms that the bulk interception of content would be more intrusive, since unlike the Data Retention Directive it would affect the "*essence*" of the fundamental right to privacy (para 39). There may be implications also for other types of surveillance in relation to which types of self-authorisation are practised, in particular by the security and intelligence agencies. All this is subject to EU law being applicable: though to the extent that *Digital Rights Ireland* may in the future be adopted or followed by the ECtHR, that distinction will cease to matter."

The Strasbourg case law

73. We have already noted that it has not been (and could not sensibly be) argued that data protection falls outside the proper scope of EU law. Mr Eadie, however, placed reliance on the jurisprudence of the European Court of Human Rights (ECtHR), which he submitted is required to be applied under EU law and which has approved the UK's regime for access to communications data under RIPA.

74. Mr Eadie's starting point was Recital (2) to the e-Privacy Directive, which states:-

> "This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Article 7 and 8 of that Charter."

75. Clearly Article 7 of the Charter corresponds to Article 8 of the ECHR, and ECtHR jurisprudence is therefore directly material in interpreting it. Mr Eadie cited a number of cases from the ECtHR which concerned telephone tapping, retention of data or access to communications, starting with *Malone v. UK* (1985) 7 EHRR 14. As is the custom in ECtHR judgments, subsequent cases restate the applicable principles; so it is not necessary to refer in this judgment to all of them.

76. The most recent is the decision of a Chamber of the ECtHR in *Kennedy v. UK* (2011) 52 EHRR 4. The claimant had been convicted (he asserted wrongly) of manslaughter. Following his release from prison after serving his sentence, he had involved himself in campaigning against miscarriages of justice. The case before the ECtHR concerned the lawfulness of the use of the RIPA regime to intercept his communications. The Act required all warrants for such interception to have been issued (or, in cases of urgency, authorised) by the Secretary of State personally.

77. In paragraphs 151 to 154 the Court set out the relevant principles:-

> "151. The requirement that any interference must be "in accordance with the law" under Article 8 § 2 will only be met where three conditions are satisfied. First, the impugned measure must have some basis in domestic law. Second, the domestic law must be compatible with the rule of law and accessible to the person concerned. Third, the person affected must be able to foresee the consequences of the domestic law for him (see, among many other authorities, *Rotaru v. Romania*, cited above, § 52; *Liberty and Others*, cited above, § 59; and *Iordachi and Others*, cited above, § 37).
>
> 152. The Court has held on several occasions that the reference to "foreseeability" in the context of interception of communications cannot be the same as in many other fields (see *Malone*, cited above, § 67; *Leander v. Sweden*, 26 March 1987, § 51, Series A no. 116; *Association for European Integration*, cited above, § 79; and *Al-Nashif*, cited above, § 121). In its admissibility decision in *Weber and Saravia*, cited above, §§ 93 to 95, the Court summarised its case-law on the requirement of legal "foreseeability" in this field:

> "93. ... foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly (see, inter alia, *Leander v. Sweden*, judgment of 26 August 1987, Series A no. 116], p. 23, § 51). However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident (see, inter alia, *Malone*, cited above, p. 32, § 67; *Huvig*, cited above, pp. 54-55, § 29; and *Rotaru).* It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated (see *Kopp v. Switzerland*, judgment of 25 March 1998, Reports 1998-II, pp. 542-43, § 72, and *Valenzuela Contreras v. Spain*, judgment of 30 July 1998, Reports 1998-V, pp. 1924-25, § 46). The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (see *Malone*, ibid.; *Kopp*, cited above, p. 541, § 64; *Huvig*, cited above, pp. 54-55, § 29; and *Valenzuela Contreras*, ibid.).
>
> 94. Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see, among other authorities, *Malone*, cited above, pp. 32-33, § 68; *Leander*, cited above, p. 23, § 51; and *Huvig*, cited above, pp. 54-55, § 29).
>
> 95. In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased

> or the tapes destroyed (see, inter alia, *Huvig*, cited above, p. 56, § 34; *Amann*, cited above, § 76; *Valenzuela Contreras*, cited above, pp. 1924-25, § 46; and *Prado Bugallo v. Spain*, no. 58496/00, § 30, 18 February 2003)."
>
> 153. As to the question whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, the Court recalls that powers to instruct secret surveillance of citizens are only tolerated under Article 8 to the extent that they are strictly necessary for safeguarding democratic institutions. In practice, this means that there must be adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law (see *Klass and Others*, cited above, §§ 49 to 50; and *Weber and Saravia*, cited above, § 106).
>
> 154. The Court has acknowledged that the Contracting States enjoy a certain margin of appreciation in assessing the existence and extent of such necessity, but this margin is subject to European supervision. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" to what is "necessary in a democratic society". In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded (see *Kvasnica v. Slovakia*, no. 72094/01, § 80, 9 June 2009)."

78. The Strasbourg court decided that the scheme as set up by RIPA did not contravene Article 8 of the ECHR. Its reasons set out in paragraphs 166 and 167 can be summarised as acceptance of the protection provided by the Interception of Communications Commissioner in his role, which included protection of the public from wrongful access to their data, and the right of any individual who believed his communications were being accessed to make an application to the Investigatory Powers Tribunal.

79. The ECtHR has not considered a case which concerns general retention of communication data, as opposed to access to the data of a particular identified individual. Mr Eadie makes the point that access to the content of communications is more intrusive than access to communications data. But the ECtHR in *Kennedy* was considering only access, and whether it interfered with ECHR Article 8 rights. Different considerations apply to the retention regime and Article 8 of the Charter.

80. The protection of personal data is an aspect of the right to respect for private and family life set out in Article 8 of the ECHR and Article 7 of the Charter: and if Article 7 of the EU Charter were the only aspect of EU law in play, there would be force in the argument that the Strasbourg and Luxembourg courts should be expected to march

in step. However, Article 8 of the Charter clearly goes further, is more specific, and has no counterpart in the ECHR. We therefore reject Mr Eadie's argument that European law requires us to interpret *Digital Rights Ireland* so as to accord with the decisions of the ECtHR culminating in *Kennedy*.

81. In any event there is an obvious difference between the cases. Mr Eadie is right to say that interception of content is more intrusive than access to communications data. But on the other hand a case about the interception of material relating to one individual, pursuant to a case-specific warrant signed personally by a Secretary of State, does not in our view assist much in interpreting the judgment of the CJEU in *Digital Rights Ireland* relating to a general retention regime on a potentially massive scale.

82. As Mr Anderson says in the passage of his report cited by Mr Eadie, the CJEU did not explain why they went further than the case law of the ECtHR. But it was their prerogative not to explain. EU law does not permit a national court to disregard a ruling of the CJEU on the grounds that it is inadequately explained or inadequately reasoned.

No challenge in Digital Rights Ireland to domestic legislation

83. Mr Eadie is also right to say that the CJEU in *Digital Rights Ireland* only ruled on the validity of the Directive. That was what the Irish and Austrian referring courts had asked it to do: it was not asked to consider domestic legislation. But this is an argument which elevates form over substance. The issue was not, as it had been in *Ireland v European Parliament and Council*, a technical (though important) one about the jurisdictional basis of the Directive. Rather it was whether the EU legislature had "exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter" (paragraph 69 of the judgment), and the Court's answer was that it had. It must follow, in our view, that an identically worded domestic statute would have been found to have exceeded the same limits. Similarly, at paragraph 66 the Court had held that the Directive "does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data". Again, it must follow that in the view of the CJEU a domestic statute in identical terms would have had the same failings.

Was the Court pronouncing on the access regime as well as the retention regime?

84. Retention for the purpose of possible access is in itself an interference with rights under Articles 7 and 8 of the Charter and Article 8 of the ECHR: see paragraph 29 of the judgment in *Digital Rights Ireland*. In *Liberty v UK* (2009) 48 EHRR 1 the ECtHR observed at paragraph 56:-

> "Telephone, facsimiles and e-mail communications are covered by the notions of 'private life' and 'correspondence' within the meaning of [ECHR] Article 8. The court recalls its findings in previous cases to the effect that the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This necessarily strikes at freedom of communication between users of the

> telecommunications services and thereby amounts in itself to an interference with the exercise of the applicant's rights under Art.8 irrespective of any measures actually taken against them."

85. In paragraphs 58 and 59 of *Digital Rights Ireland* the Court was not indicating that communications data can *only* be retained if they relate to particular geographical areas, or to particular individuals likely to be involved in serious crime. It was identifying the width of the Directive, which imposed no limits on the power to retain. But the Court was not, as we read the judgment, purporting to lay down any particular limitations on that power, as opposed to conditions of access. To have done so would, apart from being to some extent impracticable, have been inconsistent with the Court's clear conclusion in paragraph 44 of the judgment that "the retention of data for the purpose of allowing the competent national authorities to have possible access to those data…..genuinely satisfies an objective of general interest."

86. Counsel for the Secretary of State reminded us that in *Ireland v European Parliament and Council* the CJEU had held that the provisions of the Data Retention Directive were "essentially limited to the activities of service providers", and did not govern or seek to harmonise provisions on access to data or the use thereof by the police or judicial authorities of the Member States, such matters being excluded from the Directive (paragraphs 80 and 83). Accordingly, Mr Eadie submitted, it is beyond the scope of EU law to lay down minimum provisions for a data access regime, and in *Digital Rights Ireland* the CJEU cannot have been intending to do so.

87. We do not know whether the CJEU in *Digital Rights Ireland* agreed with all that their predecessors had said about the Data Retention Directive in *Ireland v Parliament.* The previous decision is referred to and considered in detail in the Opinion of Advocate General Cruz Villalón in *Digital Rights Ireland* (see paragraphs 42-46, 81-88, 121 & 124). Yet in the judgment of the Court it is not even mentioned. It seems to us quite extraordinary that in the second case to consider (albeit in different respects) the validity of the same Directive the CJEU said nothing about its reasoning in the first such case, decided only five years earlier.

88. What *is* clear, however, is that in *Digital Rights Ireland* the CJEU 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 Charter; and that it failed to provide sufficient safeguards against unlawful access to and use of retained data by public authorities. Paragraphs 57-59 of the judgment concern retention; but paragraphs 60-67 of the judgment concern access. Mr Eadie did not submit that the latter are simply to be discarded or ignored. It was not clear to us how, on the Secretary of State's case, those paragraphs of the judgment are to be treated.

89. The solution to the conundrum, in our view, and the *ratio* of *Digital Rights Ireland*, is that 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.

Was the Court laying down any (and if so what) specific minimum requirements for compatibility with EU law?

90. Mr Eadie was of course right to submit that the *decision* which the CJEU had to make in *Digital Rights Ireland* was binary, namely whether the Directive was valid or invalid. We do not accept that the case is authority for nothing more than that overall verdict, any more than we interpret the judgment as meaning that each criticism or concern which the Court expressed involves a fatal flaw in the legislation. But some points are made with such emphasis that we understand the Court to have laid down mandatory requirements of EU law.

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]

92. The supplementary submissions on behalf of the Defendant also make the point that whereas the Anderson report is the product of a year's work in gathering and assessing a large volume of material, that "can be contrasted with the complete absence of evidence before the CJEU in *Digital Rights Ireland* as to any individual Member State's domestic data retention and access regimes". It is not clear to us how much information the CJEU were given about the domestic regimes in Ireland and Austria: but even if the answer is "little or none", it does not detract from the binding nature of the conclusions of the CJEU as to what is required in order for legislation to comply with the Charter.

93. We repeat that our task is not to say what safeguards we would ourselves consider necessary or desirable, but to interpret the words of the CJEU. Nevertheless, we should mention some arguments addressed to us about practicalities.

94. The requirement that access to and use of the data must be strictly restricted to the purpose of preventing and detecting "precisely defined serious offences" or of conducting criminal prosecutions relating to such offences does not mean that access must be limited to the data of people suspected to have committed serious crime. Mr Regan (in paragraph 56 of his statement) said that investigations against serious criminals would be 'severely hampered if data could only be retained where the data

was already known to be linked to serious crime.' This is because investigation is often needed of lower level individuals whose activities are not themselves considered to have been serious.

95. In some circumstances a wholly innocent person's data might be accessed in order to assist in the detection of serious crime by others. The need for access to data is not limited to data directly attributable to particular individuals suspected of having committed serious crimes. It can be needed in relation to serious crime committed by anyone. The status of the individual in respect of whom access is sought cannot determine whether such access should be permitted, although it may of course be material in considering whether such access is indeed necessary.

96. As to the definition of serious crimes, the CJEU makes it clear that this is a matter for national legislatures, so long as the relevant offences are precisely defined and can properly be regarded as serious. Parliament has not found it difficult in previous criminal justice legislation to draw up schedules of offences considered serious for various purposes and it is unlikely to be difficult to so again in the present context.

97. Turning to the question of the need for judicial or independent review, Mr Eadie drew our attention to reservations expressed by Sir Anthony May, the Interception of Communications Commissioner (ICC). These resulted from consideration of how the requirement of judicial approvals for local authority communications data requests imposed by the Protection of Freedoms Act 2012 was working. Sir Anthony and his predecessor Sir Paul Kennedy had consistently been of the view that the requirement for judicial approval would not be likely to lead to improved standards or 'have any impact other than to introduce unnecessary bureaucracy into the process and increase the costs associated with acquiring the data'. But their criticisms were essentially of lack of training of magistrates, instances of a failure by magistrates to carry out proper scrutiny of applications, failure by the Ministry of Justice to introduce an electronic system to avoid delay and the requirements in some cases for payment of fees.

98. The provisions of RIPA, as applied by DRIPA, require (as we have noted above) that an application for access to communication data must be considered by a senior person who is independent of the investigation. There is already a need for there to be a written request for approval. The need for that approval to be by a judge or official wholly independent of the force or body making the application should not, provided the person responsible is properly trained or experienced, be particularly cumbersome. The views of Sir Anthony May and Sir Paul Kennedy are entitled to respect; but if EU law requires independent approval, as we are satisfied it does, that must be put in place. It is not for us to devise the appropriate system. As to the question of what level of consideration should be given to applications involving access to data involving communications with lawyers, Members of Parliament, or journalists, that too is not for us to determine. We only observe that such cases do require special consideration.

99. We add the important proviso that the requirement of prior approval relates to access, not to retention. We see no reason why the exercise of the power to retain should need prior independent approval, and we do not understand the CJEU to have held that it does.

Retention in the EU

100. In paragraph 68 of its decision in *Digital Rights Ireland*, the court referred to the lack of proper control in that the Directive did not require the data to be retained within the EU. It is obviously important that EU Member States should pass on information which materially assists in dealing with serious crime or terrorism. Equally, such exchange of information should be available to friendly powers outside the EU. But there is a requirement that any provision of information outside the EU should require the Member State supplying it to be satisfied that safeguards which correspond to those required by EU law are in force. It would to say the least be unfortunate if a failure by the UK to comply with EU law as set out by the court should inhibit other Member States from disclosing material information. We do not consider, however, that on a proper interpretation of *Digital Rights Ireland* it is necessary for restrictions on passing on information about communications data outside the EU to be embodied in statute.

Reference to the CJEU

101. In the course of the hearing before us on 4 and 5 June 2015 we asked leading counsel on each side whether their clients were asking us to refer the present case to the CJEU and received negative replies. But on 22 June we received from the solicitor for Mr Davis and Mr Watson a copy of a reference by the Stockholm Administrative Court of Appeals to the CJEU lodged on 4th May 2015 (case C/203/2015) in the case *Tele2 Sverige AB* of the following questions:-

> "Is a general obligation to retain traffic data covering all persons, all means of electronic communication and all traffic data without any distinctions, limitations or exceptions for the purpose of combating crime compatible with Article 15(1) of Directive 2002/58/EC [the E-Privacy Directive] taking account of Articles 7, 8 and 15(1) of the Charter?
>
> If the answer to question 1 is in the negative, may retention nevertheless be permitted where access by the national authorities to the retained data is determined as described below; security requirements are regulated as described below; and all relevant data are to be retained for six months … and subsequently deleted…..?"

102. The court was considering the provisions of three Swedish statutes: they have some similarities to DRIPA but are by no means identical to it.

103. It appears that the Stockholm court making the reference took the view, as we do, that the judgment of the CJEU in *Digital Rights Ireland* does not prohibit the retention of traffic data provided that the requirements of the e-Privacy Directive are met and there is otherwise no infringement of EU law. However, the referring court noted that the parties had differing views as to how the judgment of the CJEU was to be interpreted and wished "to have a clear answer to the question whether the EU court of justice carried out a weighted assessment in that judgment of the scope of retention and the provisions governing data access, period of retention and security".

104. On 23 June 2015 the Treasury Solicitor sent a letter to us, subsequently developed by way of skeleton argument, requesting a reference to the CJEU. The claimants,

understandably, opposed the late request to refer the case to Luxembourg. We heard oral argument on this issue on 9 July 2015.

105. The Swedish case is not the only decision of a domestic court of another Member State concerning *Digital Rights Ireland* to which we have been referred. Mr Welch, solicitor for Mr Davis and Mr Watson, has referred us to four decisions in other Member States, three of them by Constitutional Courts, holding their country's communications data legislation invalid without finding it necessary to make a reference to the CJEU: the Constitutional Court of Slovenia on 3 July 2014; the Constitutional Court of Romania on 8 July 2014; the District Court of The Hague on 11 March 2015 and the Constitutional Court of Belgium on 11 June 2015. Some of the translations we have of those judgments are unofficial, and the details of each country's laws under scrutiny are of course not identical: but the general theme is clear.

106. Mr Eadie relied on the judgment of Sir Thomas Bingham MR in *R v Stock Exchange ex p Else Ltd* [1993] QB 534 at 545, where he said:

> "I understand the correct approach in principle of national courts (other than a final court of appeal) to be quite clear: if the facts had been found and a community law issue is critical to the court's final decision, the appropriate course is ordinarily to refer the issue to the Court of Justice unless the national court can with complete confidence resolve the issue itself. In considering whether it can, with complete confidence resolve the issue itself, the national court must be fully mindful of the differences between national and Community legislation, of the pitfalls which face a national court venturing into what may be an unfamiliar field, of a need for uniform interpretation throughout the community and of the great advantages enjoyed by the Court of Justice in construing Community instruments. If the national court has any real doubt, it should ordinarily refer."

107. It seems to us that in *Else* the Master of the Rolls primarily had in mind issues of EU law which have arisen without there being an existing judgment of the CJEU giving that court's ruling on them. The *dicta* are less obviously applicable where the CJEU has pronounced judgment and the domestic court is being asked to interpret what it meant. In *Trinity Mirror v Commissioners of Customs and Excise* [2001] 2 CMLR 33 Chadwick LJ cited the above passage from *Else* and continued:

> "52. But it is, I think, important to have in mind, also, the observations of the Advocate-General (Mr Francis Jacobs QC) in Case C-338/95, *Wiener SI GmbH v. Hauptzollamt Emmerich*. The question which he thought it necessary to address is stated at paragraph 10 of his Opinion:
>
> … whether it is appropriate—and especially whether it is still appropriate today, in view of developments which I shall mention below—for the Court to be asked

> to rule in every case where a question of interpretation of Community law may arise.
>
> He identified the matter which was of practical concern to the Court of Justice, at paragraph 15:
>
> "Any "application" of a rule of law can be regarded as raising a question of "interpretation"—even if the answer to the question of interpretation may seem obvious. Every national court confronted with a dispute turning on the application of Community law can refer a question which, if more or less properly phrased, this Court is bound to answer after the entire proceedings have taken their course. That will be so even where the question is similar in most respects to an earlier question; the referring court (or the parties' lawyers) may always seek to distinguish the facts of the cases. It will be so even where the question could easily, and with little scope for reasonable doubt, be answered on the basis of existing case law; again the facts may be different, or it may be that a particular condition imposed in earlier case law gives rise to a new legal argument and is regarded as needing further clarification. The net result is that the Court could be called upon to intervene in all cases turning on a point of Community law in any court or tribunal in any of the Member States. It is plain that if the Court were to be so called upon it would collapse under its case-load."
>
> The solution is "a greater measure of self-restraint on the part of both the national courts and the Court of Justice"—see paragraph 18. Where the national court is not a court of last resort, a reference will be most appropriate where the question is one of general importance and where the ruling is likely to promote the uniform application of the law throughout the European Union. A reference will be least appropriate where there is an established body of case law which could readily be transposed to the facts of the instant case..."

108. A reference was refused in *Trinity Mirror* because, as Chadwick LJ put it at [55], "the question of principle has been decided by the Court of Justice and a national court or tribunal can now act in the light of that decision".

109. We take the same view in this case. The Claimants' objections to a reference are well founded for several reasons.

110. Firstly, we are not the domestic court of last resort. We do not doubt that the questions raised in this case are of general importance, but we do not consider that to refer the present case to Luxembourg is likely to promote the uniform application of the law throughout the EU: the CJEU has given general guidance already in *Digital Rights*

Ireland, and it is apparent from the cases cited to us that Member States have different regimes governing the retention of and access to communications data.

111. Secondly, we are not persuaded that the fact that the Swedish court has referred the issue to Luxembourg means that we should do the same. It might just as well be said on the other side that we should follow our colleagues in Slovenia, Romania, the Netherlands and Belgium in holding our domestic legislation to be in breach of EU law without making a reference.

112. Thirdly, the request is made far too late. DRIPA was enacted on 17 July 2014. These proceedings were issued on 13 August 2014. Permission for judicial review was granted on 8 December 2014. If a request was to be made on the grounds that the judgment in *Digital Rights Ireland* was so difficult to comprehend that only the CJEU itself could say what it meant, that application should have been made at an early stage; certainly not after the conclusion of a two day oral hearing, with the parties having incurred substantial costs.

113. Fourthly, and perhaps most importantly of all, DRIPA contains a sunset clause which, as we have noted, means that the Act will expire on 31st December 2016. The CJEU typically takes two years or more to answer a question referred to it for a preliminary ruling. It is most unlikely that an answer to a reference made now would be received before DRIPA has expired, or (far more probably) has been repealed and replaced by a new statute. Either way, the answer would have become academic.

Conclusion

114. 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.

Remedy

115. On 10 July we sent paragraphs 1-114 above to counsel as a draft judgment and invited submissions in writing on remedy.

116. The Secretary of State's submissions ask us to go no further than a declaration; and to suspend any order we do make pending appeal. Mr Eadie relies on *R(Chester) v Secretary of State for Justice* [2014] AC 271, a challenge to the UK's ban on voting by convicted prisoners. The claimants sought to rely *inter alia* on EU law. Lord Mance JSC, giving the leading judgment, said that EU law does not incorporate a right to vote parallel to that recognised by the ECHR. But he added that even if it had,

the Supreme Court would not have granted any relief beyond a declaration. The statutory scheme was complex and it was not for the court to devise an alternative.

117. The Claimants propose an order for disapplication, suspended until 1 January 2016, to give time for compliance. As counsel for Mr Davis and Mr Watson put it in their submissions (with which counsel for Mr Brice and Mr Lewis agree):

> "The Claimants accept that Parliament will need to be afforded a reasonable opportunity to legislate for proper safeguards….. Despite its unlawfulness, the Claimants do not invite the Court to order that the entire DRIPA regime falls with immediate effect. The Claimants are anxious to ensure that serious criminal investigations are not impeded, and that the legislation necessary to resolve the defects in the current situation is not enacted with the same unfortunate haste that DRIPA was."

118. Ms Rose refers to the decision of the Supreme Court given on 29 April 2015 in *R (ClientEarth) v Secretary of State for Environment, Food and Rural Affairs* [2015] UKSC 28. The Secretary of State admitted that the UK was in breach of the air quality standards required by Article 13 of the Air Quality Directive (2008/50/EC). The High Court and Court of Appeal considered that this was a matter for the Commission, not the national courts. All relief was refused. The Supreme Court granted a declaration recording the UK's breach of EU law and made a reference to the CJEU as to (among other things) whether it should order further relief. The CJEU held that national courts must take "*any necessary measure, such as an order in the appropriate terms*" to ensure compliance with EU law (§58).

119. When the case returned to the Supreme Court, they granted a mandatory order requiring the production of air quality plans designed to end the breach, subject to a time limit for production and with liberty to apply. The Supreme Court had "*no hesitation in rejecting*" the submission that mandatory relief was unnecessary (§29). The Court concluded that "*we would… be failing in our duty if we simply accepted* [the Secretary of State's] *assurances without any legal underpinning… the new Government, whatever its political complexion, should be left in no doubt as to the need for immediate action to address this issue*" (§30).

120. The *ClientEarth* case is a significant and recent case on remedies in the UK courts for breaches of EU law. It does not lay down a rule that disapplication or mandatory relief, even with a reasonable time for compliance, must always be the appropriate remedy, but it gives a steer which in our view cannot be ignored.

121. We consider that an order for disapplication is appropriate, but that a date of 1 January 2016 for it to come into effect is too soon. The Government has already announced its intention to legislate in the current session of Parliament to replace DRIPA (as it must, given the sunset clause). Subject to any view different from ours taken by a higher court, it will no doubt seek to ensure that the new statute, unlike section 1 of DRIPA, is compliant with EU law. The courts do not presume to tell Parliament for how long and in what detail Bills should be scrutinised, but it is right to say (to put it no higher) that legislation enacted in haste is more prone to error, and it would be highly desirable to allow the opportunity of thorough scrutiny in both Houses. Moreover, if the route chosen for compliance with part (b) of the declaration

is authorisation by an independent administrative body, that body would have to be appointed after the passing of the new Act and be ready to start work by the time it comes into effect. All this would, we think, take longer than five months.

122. We will make an order disapplying s 1 of DRIPA to the extent that it permits access to retained data which is inconsistent with EU law in the two respects set out in our declaration, but suspend that order until 31 March 2016. The order will be that s 1 is disapplied after that date:

(a) in so far 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

(b) in so far 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 and use of the data to what is strictly necessary for the purpose of attaining the objective pursued.

123. In their submissions on remedy following receipt of our draft judgment counsel for the Defendant raised for the first time the question of whether access to retained data for national security reasons is within the scope of EU law. This was not raised in the oral or written arguments previously addressed to us and we decline to allow it to be raised at this late stage. Whether national security cases should have different provisions for authorisation of access to communications data will no doubt be the subject of careful thought when the new legislation is being drafted.

Costs

124. Counsel and solicitors acting for Mr Davis and Mr Watson, to their very great credit, have acted *pro bono*, and pursuant to an agreement reached with the Government Legal Department they do not seek a *pro bono* costs order. In their case, therefore, there will be no order as to costs. Mr Brice and Mr Lewis are legally aided: it is accepted that in their case the Defendant must pay their costs, with the usual order for detailed legal aid assessment. The interveners will bear their own costs in accordance with the terms of the orders allowing them to intervene.

Permission to appeal

125. The Secretary of State seeks permission to appeal. Plainly the public importance of the case justifies the grant of permission, as the Claimants accept. We are prepared to grant permission subject to the condition in the case of Mr Davis and Mr Watson, who do not have the protection of a legal aid certificate, that the Defendant shall not be entitled to seek an order against them for costs either in this court or on appeal.

126. We express our gratitude to leading and junior counsel and solicitors for all parties for the exemplary assistance we have received in this case.

APPENDIX

Judgment of the CJEU in *Digital Rights Ireland* paragraphs 23-71

Consideration of the questions referred

The second question, parts (b) to (d), in Case C 293/12 and the first question in Case C 594/12

23. By the second question, parts (b) to (d), in Case C 293/12 and the first question in Case C 594/12, which should be examined together, the referring courts are essentially asking the Court to examine the validity of Directive 2006/24 in the light of Articles 7, 8 and 11 of the Charter.

24. *The relevance of Articles 7, 8 and 11 of the Charter with regard to the question of the validity of Directive 2006/24*

25. It follows from Article 1 and recitals 4, 5, 7 to 11, 21 and 22 of Directive 2006/24 that the main objective of that directive is to harmonise Member States' provisions concerning the retention, by providers of publicly available electronic communications services or of public communications networks, of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the prevention, investigation, detection and prosecution of serious crime, such as organised crime and terrorism, in compliance with the rights laid down in Articles 7 and 8 of the Charter.

26. The obligation, under Article 3 of Directive 2006/24, on providers of publicly available electronic communications services or of public communications networks to retain the data listed in Article 5 of the directive for the purpose of making them accessible, if necessary, to the competent national authorities raises questions relating to respect for private life and communications under Article 7 of the Charter, the protection of personal data under Article 8 of the Charter and respect for freedom of expression under Article 11 of the Charter.

27. In that regard, it should be observed that the data which providers of publicly available electronic communications services or of public communications networks must retain, pursuant to Articles 3 and 5 of Directive 2006/24, include data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to identify the location of mobile communication equipment, data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services. Those data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.

28. Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.

29. In such circumstances, even though, as is apparent from Article 1(2) and Article 5(2) of Directive 2006/24, the directive does not permit the retention of the content of the communication or of information consulted using an electronic communications network, it is not inconceivable that the retention of the data in question might have an effect on the use, by subscribers or registered users, of the means of communication covered by that directive and, consequently, on their exercise of the freedom of expression guaranteed by Article 11 of the Charter.

30. The retention of data for the purpose of possible access to them by the competent national authorities, as provided for by Directive 2006/24, directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 of the Charter. Furthermore, such a retention of data also falls under Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, therefore, necessarily has to satisfy the data protection requirements arising from that article (Cases C 92/09 and C 93/09 *Volker und Markus Schecke and Eifert* EU:C:2010:662, paragraph 47).

31. Whereas the references for a preliminary ruling in the present cases raise, in particular, the question of principle as to whether or not, in the light of Article 7 of the Charter, the data of subscribers and registered users may be retained, they also concern the question of principle as to whether Directive 2006/24 meets the requirements for the protection of personal data arising from Article 8 of the Charter.

32. In the light of the foregoing considerations, it is appropriate, for the purposes of answering the second question, parts (b) to (d), in Case C 293/12 and the first question in Case C 594/12, to examine the validity of the directive in the light of Articles 7 and 8 of the Charter.

Interference with the rights laid down in Articles 7 and 8 of the Charter

33. 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, as the Advocate General has pointed out, in particular, in paragraphs 39 and 40 of his Opinion, 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.

34. To establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way (see, to that

effect, Cases C 465/00, C 138/01 and C 139/01 *Österreichischer Rundfunk and Others* EU:C:2003:294, paragraph 75).

35. As a result, the obligation imposed by Articles 3 and 6 of Directive 2006/24 on providers of publicly available electronic communications services or of public communications networks to retain, for a certain period, data relating to a person's private life and to his communications, such as those referred to in Article 5 of the directive, constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter.

36. Furthermore, the access of the competent national authorities to the data constitutes a further interference with that fundamental right (see, as regards Article 8 of the ECHR, Eur. Court H.R., *Leander v. Sweden*, 26 March 1987, § 48, Series A no 116; *Rotaru v. Romania* [GC], no. 28341/95, § 46, ECHR 2000-V; and *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 79, ECHR 2006-XI). Accordingly, Articles 4 and 8 of Directive 2006/24 laying down rules relating to the access of the competent national authorities to the data also constitute an interference with the rights guaranteed by Article 7 of the Charter.

37. Likewise, Directive 2006/24 constitutes an interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter because it provides for the processing of personal data.

38. It must be stated that the interference caused by Directive 2006/24 with the fundamental rights laid down in Articles 7 and 8 of the Charter is, as the Advocate General's Opinion, wide-ranging, and it must be considered to be particularly serious. Furthermore, as the Advocate General has pointed out in paragraphs 52 and 72 of his Opinion, the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.

39. *Justification of the interference with the rights guaranteed by Articles 7 and 8 of the Charter*

40. Article 52(1) of the Charter provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

41. So far as concerns the essence of the fundamental right to privacy and the other rights laid down in Article 7 of the Charter, it must be held that, even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference with those rights, it is not such as to adversely affect the essence of those rights given that, as follows from Article 1(2) of the directive, the directive does not permit the acquisition of knowledge of the content of the electronic communications as such.

42. Nor is that retention of data such as to adversely affect the essence of the fundamental right to the protection of personal data enshrined in Article 8 of the Charter, because

Article 7 of Directive 2006/24 provides, in relation to data protection and data security, that, without prejudice to the provisions adopted pursuant to Directives 95/46 and 2002/58, certain principles of data protection and data security must be respected by providers of publicly available electronic communications services or of public communications networks. According to those principles, Member States are to ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data.

43. As regards the question of whether that interference satisfies an objective of general interest, it should be observed that, whilst Directive 2006/24 aims to harmonise Member States' provisions concerning the obligations of those providers with respect to the retention of certain data which are generated or processed by them, the material objective of that directive is, as follows from Article 1(1) thereof, 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 material objective of that directive is, therefore, to contribute to the fight against serious crime and thus, ultimately, to public security.

44. It is apparent from the case-law of the Court that the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest (see, to that effect, Cases C 402/05 P and C 415/05 P *Kadi and Al Barakaat International Foundation v Council and Commission* EU:C:2008:461, paragraph 363, and Cases C 539/10 P and C 550/10 P *Al-Aqsa v Council* EU:C:2012:711, paragraph 130). The same is true of the fight against serious crime in order to ensure public security (see, to that effect, Case C 145/09 *Tsakouridis* EU:C:2010:708, paragraphs 46 and 47). Furthermore, it should be noted, in this respect, that Article 6 of the Charter lays down the right of any person not only to liberty, but also to security.

45. In this respect, it is apparent from recital 7 in the preamble to Directive 2006/24 that, because of the significant growth in the possibilities afforded by electronic communications, the Justice and Home Affairs Council of 19 December 2002 concluded that data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention of offences and the fight against crime, in particular organised crime.

46. It must therefore be held that the retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by Directive 2006/24, genuinely satisfies an objective of general interest.

47. In those circumstances, it is necessary to verify the proportionality of the interference found to exist.

48. In that regard, according to the settled case-law of the Court, the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives (see, to that effect, Case C 343/09 *Afton Chemical* EU:C:2010:419, paragraph 45; *Volker und Markus Schecke and Eifert* EU:C:2010:662, paragraph 74; Cases C 581/10 and C 629/10 *Nelson and Others* EU:C:2012:657, paragraph 71; Case C 283/11 *Sky*

Österreich EU:C:2013:28, paragraph 50; and Case C 101/12 *Schaible* EU:C:2013:661, paragraph 29).

49. With regard to judicial review of compliance with those conditions, where interferences with fundamental rights are at issue, the extent of the EU legislature's discretion may prove to be limited, depending on a number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference (see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 102, ECHR 2008-V).

50. In the present case, in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by Directive 2006/24, the EU legislature's discretion is reduced, with the result that review of that discretion should be strict.

51. As regards the question of whether the retention of data is appropriate for attaining the objective pursued by Directive 2006/24, it must be held that, having regard to the growing importance of means of electronic communication, data which must be retained pursuant to that directive allow the national authorities which are competent for criminal prosecutions to have additional opportunities to shed light on serious crime and, in this respect, they are therefore a valuable tool for criminal investigations. Consequently, the retention of such data may be considered to be appropriate for attaining the objective pursued by that directive.

52. That assessment cannot be called into question by the fact relied upon in particular by Mr Tschohl and Mr Seitlinger and by the Portuguese Government in their written observations submitted to the Court that there are several methods of electronic communication which do not fall within the scope of Directive 2006/24 or which allow anonymous communication. Whilst, admittedly, that fact is such as to limit the ability of the data retention measure to attain the objective pursued, it is not, however, such as to make that measure inappropriate, as the Advocate General's Opinion.

53. As regards the necessity for the retention of data required by Directive 2006/24, it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight.

54. So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (Case C 473/12 IPI EU:C:2013:715, paragraph 39 and the case-law cited).

55. In that regard, it should be noted that the protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of the Charter.

56. 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 ECHR, Eur. Court H.R., Liberty and Others v. the United Kingdom, 1 July 2008, no. 58243/00, § 62 and 63; Rotaru v. Romania, § 57 to 59, and S. and Marper v. the United Kingdom, § 99).

57. The need for such safeguards is all the greater where, as laid down in Directive 2006/24, personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data (see, by analogy, as regards Article 8 of the ECHR, *S. and Marper v. the United Kingdom*, § 103, and *M. K. v. France*, 18 April 2013, no. 19522/09, § 35).

58. As for the question of whether the interference caused by Directive 2006/24 is limited to what is strictly necessary, it should be observed that, in accordance with Article 3 read in conjunction with Article 5(1) of that directive, the directive requires the retention of all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony. It therefore applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives. Furthermore, in accordance with Article 3 of Directive 2006/24, the directive covers all subscribers and registered users. It therefore entails an interference with the fundamental rights of practically the entire European population.

59. 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.

60. 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.

61. 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.

62. 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.

63. 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.

64. 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.

65. Thirdly, so far as concerns the data retention period, Article 6 of Directive 2006/24 requires that those data be retained for a period of at least six months, without any distinction being made between the categories of data set out in Article 5 of that directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned.

66. Furthermore, that period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.

67. 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. Moreover, as far as concerns the rules relating to the security and protection of data retained by providers of publicly available electronic communications services or of public communications networks, it must be held that Directive 2006/24 does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. In the first place, Article 7 of Directive 2006/24 does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down.

69. Article 7 of Directive 2006/24, read in conjunction with Article 4(1) of Directive 2002/58 and the second subparagraph of Article 17(1) of Directive 95/46, does not ensure that a particularly high level of protection and security is applied by those providers by means of technical and organisational measures, but permits those providers in particular to have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures. In particular, Directive 2006/24 does not ensure the irreversible destruction of the data at the end of the data retention period.

70. 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 paragraphs, 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, to that effect, Case C 614/10 *Commission v Austria* EU:C:2012:631, paragraph 37).

71. Having regard to all the foregoing considerations, it must be held that, by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter.

72. In those circumstances, there is no need to examine the validity of Directive 2006/24 in the light of Article 11 of the Charter.

73. Consequently, the answer to the second question, parts (b) to (d), in Case C 293/12 and the first question in Case C 594/12 is that Directive 2006/24 is invalid.