THOMSON REUTERS HUMAN RIGHTS LAW CONFERENCE 2014

Privacy, data retention and state surveillance: *Digital Rights Ireland*

Jessica Simor QC

Matrix chambers

1. Anya has spoken about *Costeja*. That case raises extremely difficult questions about where freedom of access to information and freedom of expression stop and where 'privacy' rights begin. What is particularly troubling about it for me is that perfectly lawful information should be rendered inaccessible on the basis of a decision by a search engine as to where the balance between privacy and freedom of information lies.

2. In the context of take-down requests from web-sites, it has of course always been the case that the web-site has to decide whether or not it is right to remove the material. However, the regime of notice and take-down, assumed that the information would only be removed by the relevant site if it was unlawful, for example defamatory or in infringing of copyright or trademarks. The so called 'right to be forgotten' regime goes way beyond that in envisaging not the taking down of unlawful information but the removal of links to lawful information, so that in practice such information cannot be found where that information is no longer 'relevant and adequate'. The potential impact on freedom of expression and public access to information is profound. Unlike web-sites that host content, search engines are unlikely to have any commercial or practical interest in the substantive of the content of the material. A news web-site is likely to seek to defend 'information' or expression rights. But why should a search engine do so ? Whilst it may be that a company like Google is willing to spend on lawyers to litigate the question of whether the search link should be disabled, other smaller search engines will not necessarily be willing or able to do so. This has the potential to increase Google's dominance in the search market or reduce freedom of information/expression. Even assuming search engines are willing to put resources in, are we willing to leave the balancing test to be carried out by unaccountable corporates, with all the moral, ethical and indeed factual questions that such a balance involves.

3. I am going to talk however, about another aspect of privacy and that is the retention of data by communication service providers ("CSPs"), including internet service providers and access to that data by state authorities. Snowden revealed the extent to which the State is able and does access communications data. This is data that shows not the content of communications but rather the fact that the communication took place, the telephone number or the E-mail address, its location, the time of the call or text or E-mail etc. Sometimes it is referred to as metadata

and sometimes as 'traffic data' and arguments are had as to the distinction between such types of data. The regime under which such data is intercepted directly, or retained by CSPs and then sought by administrative authorities, as governed largely by RIPA, is highly complex and necessarily, its detailed operation is not a matter of public knowledge.

4. This year there have been several challenges in relation to it. There is an ongoing challenge in the Investigatory Powers Tribunal brought by Liberty, the ACLU, Privacy International and others. And a similar challenge brought by Big Brother watch before the ECHR. Both of these question the legality of the regime whereby all communications coming from outside the UK can be intercepted under a warrant, with that information then being 'sifted' for particular content. Judgments are pending.

5. In addition, a challenge is afoot to the new legislation requiring CSPs to retain data adopted 'urgently' by Parliament just before the summer recess "to make provision, in consequence of a declaration of invalidity made by the Court of Justice of the European Union in relation to Directive 2006/24/EC" by the *Digital Rights Ireland* case, which I am going to speak about today. This legislation replaced the Data Retention (EC Directive) Regulations 2009 ("2009 Regulations") (C/21/183), which required communications service providers to retain communications data for 12 months. It provides for its own repeal on 31 December 2016.

Retention and Interception of communications data.

6. Practitioners have to a large extent continued to analyse and apply UK interception and surveillance law on a purely domestic basis, without reference to EU law. The reason for this is that both the Data Protection Directive 95/46 ("Directive 95/48") and Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronics communications sector ("Directive 2002/58"), describe their 'scope' as not extending to matters "falling outside the Scope of the Treaty Establishing the European Community," such as those covered by Titles V and VI of the European Union and "in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law": Article 3 Directive 95/46 and Article 1(3) Directive 2002/58. However, both directives contain articles that specifically set out the 'exceptional' basis on which the relevant 'rights' may be 'restricted'. These exceptions are paradoxically the same as the matters that are supposed <u>not</u> to be within the scope of the Directives, namely national security, defence, public security the prevention, investigation, detention and prosecution of criminal offences: see Article 13 Directive 95/46 and Article 15 Directive of Directive 2002/46. To be lawful, the exceptions must comply with the requirements of necessity and proportionality and the Charter on Fundamental Rights and the Convention on Human Rights. Accordingly, it is in

my view unlikely to be correct to say that state security and criminal matters fall outside the scope of the Directives of data protection. Rather, such matters appear to fall within it but can be excluded or subject to restrictions where 'necessary and proportionate' in accordance with their terms. That question, is one of EU law. Any other interpretation would in my view render the exception provisions in the directives otiose. This however, is a highly contentious point, which remains to be determined. As yet, the assumption is that the security services simply fall outside the scope of data protection law.

7. In the UK there is an added complication, which also remains to be litigated and that is the effect Protocol No. 21, the UK opt out in respect of the area of freedom security and justice. What is clear is that where the UK has opted in to a particular measure adopted under Title V, the security and justice title, then the UK must comply with the relevant treaty rules, including those relating to data protection. Article 6a of Protocol No. 21 explicitly states that where there is no opt in, measures adopted under chapters 4 and 5 (judicial and police co-operation respectively) then the UK is <u>not</u> bound by rules laid down on the basis of Article 16 TFEU (the Data Protection provision). Unfortunately, this too is not simple. Neither of the two data protection directives were adopted under Article 16 of the TFEU, nor could they have been. They were adopted under Article 114 TFEU (the internal market provision). Arguably, therefore the-opt out is irrelevant; if the data protection directives apply they apply as a necessary part internal market measure <u>not</u> as a measure adopted under Title V.

8. It seems to me doubtful that one can any longer say that any interference with individual data (through interception, retention etc) is outside the scope of EU law. Increasingly, including in *Costeja*, the Court is treating this area of law as free-standing EU law, initially adopted under the Internal Market provision but increasingly treated as a matter generally within the scope of EU law. Thus, there is in my view great potential for individuals to challenge data retention and interception on the basis of EU law principles and in particular compliance with the Charter of Fundamental Rights, which contains a specific right to privacy, the home and data privacy specifically.

9. The starting point in relation to electronic communications data is Directive 2002/58, which was explicitly adopted by the Council to:

> "particularise[s] and complement[s] Directive 95/46" for the purposes of harmonizing national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communications sector and to ensure the free movement of such data and of electronic communication equipment and services within the Community": Article 1(1)

10. It provides that Member States are obliged to ensure the confidentiality of communications and to prohibit, listening, tapping, storage or other kinds of interception or surveillance, except where such interferences are legally authorized in accordance with Article 15(1): see Article 5(1).

11. Importantly, it contains: (1) a prohibition on data retention: Article 5; and (2) an obligation to ensure that CSPs erase traffic data when it is no longer needed for the purpose of the transmission of the communication: Article 6. The only exception to this is where in so far as necessary the provider of the communication serve may retain traffic data:

    a. for billing purposes but only up until the last date on which the bill may be challenged or payment pursued end of the billing period As regards retention: 6(2);

    b. may use data for marketing but only if the individual has given his consent: 6(3);

12. As to identification of numbers, the CSP is obliged to provide a possibility for the user to prevent caller identification: Article 8. As to location data, this can only be processed on an anonymous basis unless the user has given his/her consent: Article 9.

13. Article 15 permits Member States however, to adopt legislation to restrict the scope of these rights: the right to confidentiality of communications (Article 5); the right to erasure of traffic data (Article 6), the right to non-identification of caller (Article 8) and the right to anonymisation of location and other traffic data (article 9). But such a restriction is only permissible where it:

> "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 unauthorized use of the 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 [which applies to the Charter to EU law]."

14. Pursuant again to the internal market provision of the Treaty (then Article 95 now, 114), the Council and Parliament adopted Directive 2006/24, with the objective of harmonizing data retention laws across the EU. This Directive provided for a derogation from Articles 5, 6 and 9 of Directive 2002/58, (the rights of confidentiality of communications, to erasure of traffic data and to anonymisation of location data respectively), by imposing an obligation on CSPs to retain categories of data as set out in Article 5. Thus, Member States agreed to ensure that a vast quantity of communication data was retained by CSPs for not less than six months but not

more than two years, including (a) data necessary to identify the source of a communication, including caller numbers, identities and addresses, e-mail identities and addresses; (b) data necessary to identify the destination of the communication and (c) data necessary to identify the date, time duration of a communication; (d) location data. In addition, Directive 2006/58 provided that the data was to be retained:

> "in such a way that the data retained and any other necessary information relating to such data can be transmitted upon request to the competence authorities without undue delay": Article 8.

15. The Directive provided for a monitoring authority but for no other judicial oversight and in particular, no judicial oversight in relation to decisions as to data that had to be passed over to the authorities.

16. In April this year, the CJEU struck that Directive down as in grave breach of fundamental rights. The case involved two preliminary references from Ireland and Austria: C-293/12 and C-594/12 respectively. In the first, *Digital Rights Ireland*, the claimant brought an action before the Irish High Court in which it claimed that it owned a mobile phone which had been registered on 3 June 2006 and that it had used that mobile phone since that date. It challenged the legality of national legislative and administrative measures concerning the retention of data relating to electronic communications and asked the national court, in particular, to declare the invalidity of Directive 2006/24 and of Part 7 of the Criminal Justice (Terrorist Offences) Act 2005, which requires telephone communications service providers to retain traffic and location data relating to those providers for a period specified by law in order to prevent, detect, investigate and prosecute crime and safeguard the security of the State. The High Court, considering that it was not able to resolve the questions raised relating to national law unless the validity of Directive 2006/24 had first been examined, decided to stay proceedings and to refer questions relating to its validity to the Court for a preliminary ruling. In the second, *Kärtner Landesregierung, Seitlinger and others,* a large number of applicants brought an action for the annulment of the Austrian law implementing Directive 2006/24.

17. The first question that the Court addressed in respect of both cases was the question of whether Directive 2006/24 was compatible with the Charter of Fundamental Rights. The Court noted that Directive 2006/24 was a derogating Act; it derogated from the derogating provision in Article 15 of Directive 2002/58: see paragraph 32, which refers to the AG's analysis at paragraphs 39-30 of his Opinion. Indeed, it actually amended Article 15 of Directive 2002/58 to add a new paragraph stating that Article 15(1) did not apply in respect of it.

18. The Court was in no doubt that the retention of communication data, even absent content, constituted an interference in private life and data protection, as guaranteed by Articles 7 and

8 of the Charter: paragraphs 33-34. And further, that access to such data by "the competent national authorities", constituted an additional interference: paragraph 35. The Court, considered the interference particularly grave because of the vague sense of surveillance to which it potentially gave rise and the possibility that this could impact on individuals' freedom of expression. As the AG stated at paragraphs 52 and 72 of his Opinion, to which the Court referred at paragraph 37:

> 52. First of all, it is true that it must not be overlooked that the vague feeling of surveillance which implementation of Directive 2006/24 may cause is capable of having a decisive influence on the exercise by European citizens of their freedom of expression and information and that an interference with the right guaranteed by Article 11 of the Charter therefore could well also be found to exist….
>
> 72. …the fact remains that the collection and, above all, the retention, in huge databases, of the large quantities of data generated or processed in connection with most of the everyday electronic communications of citizens of the Union constitute a serious interference with the privacy of those individuals, even if they only establish the conditions allowing retrospective scrutiny of their personal and professional activities. The collection of such data establishes the conditions for surveillance which, although carried out only retrospectively when the data are used, none the less constitutes a permanent threat throughout the data retention period to the right of citizens of the Union to confidentiality in their private lives…."

19. Accordingly, the Court held that justification for that interference was required under Articles 7 and 8 of the Charter. The Court had no doubt that the objective of the legislation was legitimate; to contribute to the fight against serious crime and thus, ultimately to security': paragraph 41-44. As to necessity and proportionality, the Court considered that in light of the matters at issue, namely privacy and data confidentiality, the discretion available to the EU was reduced and its review should be strict: paragraph 48.

20. As regards retention, the Court applied a strict necessity test in determining the legality of the legislation by reference to its earlier case law: paragraph 52.[1] Thus, the Court noted:

> "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).

[1] The Court cited paragraph 39 of Case C-473/12 *IPI* : "According to settled case-law, the protection of the fundamental right to privacy requires that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (Case C‑73/07 *Satakunnan Markkinapörssi and Satamedia* [2008] ECR I‑9831, paragraph 56, and Joined Cases C‑92/09 and C‑93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I‑11063, paragraphs 77 and 86)."

> 55 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).

21. The Court noted that the retention obligation was universal, covering all data without regard to any individual characteristic and thus "entail[ed] an interference with the fundamental rights of practically the entire European population": paragraphs 56-59. In that regard the Court noted that its coverage, being comprehensive, meant that it applied even to those subject to rules of professional secrecy: paragraph 58.

22. As regards, access, the Court held that the legislation failed to provide any objective criteria by which to determine the limits of access by competent authorities. Nor did it contain procedural or substantive safeguards in relation to access: paragraphs 60-61. As the Court noted:

> "62…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.

23. As regards the retention period, the Court noted that the minimum retention period of 6 months existed 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: paragraph 63. Nor did it state the basis on which it could be for a longer period or specify the need for objective criteria in order to ensure that it is limited to what is strictly necessary: paragraph 65.

24. Finally the Court expressed concern that the legislation did not require the data to be retained in the EU, such that the protection of an independent authority guaranteed by Article 8(3) of the Charter was not fully ensured.

25. For the above reasons, the Court found that the legislation did not comply with the principles of proportionality as required by Articles 7, 8 and 52 of the Charter, such that there was no need for it to go on and consider Article 11: paragraph 70.

National responses

26. In Austria, the response was to repeal the legislation adopted to implement Directive 2002/58.

27. In the United Kingdom emergency legislation was enacted to replace the original implementing provisions (the 2009 Regulations) with primary legislation: the Data Retention and Investigatory Powers Act 2014. That legislation empowers the Secretary of State by way of a retention notice to require a telecommunications operator to retain relevant data. Such a notice can relate to a particular operator or a description of operators. It can require the retention of all data or any description of data.

28. As already stated this new legislation is subject to legal challenge. In my view it is impossible to see how it can be compliant with EU law following the judgment of the Court in *Digital Rights Ireland*. It can be no answer for the UK simply to say the legislation falls outside the scope of EU law. That cannot be correct for the obvious reason that if it was, the Council could not have adopted Directive 2006/24. But nobody suggested that that legislation was *ultra-vires* the Treaty on the basis that the subject matter fell outside the scope of EU law. On the contrary, the very reason that the Directive was struck down was because the measures did fall within the scope of EU law and failed adequately to protect individual data protection rights. Moreover, there is a strong argument that the new legislation must comply with Article 15 of Directive 2002/58, which would have little meaning if it did not apply in respect of measures adopted by Member States for 'national security' or 'crime' purposes.

Access to retained data under UK law

29. A communications service provider who retains data pursuant to such a notice cannot disclose the data save as required to do so under Chapter 2 of Part 1 of RIPA or a court order or judicial warrant: s. 1(6). It is the former that has been causing so much recent concern. Chapter 2 of Part 1 of RIPA empowers particular state bodies: police forces, NCA, HMRC, MI5, MI6 and GCHQ (as well as additional public authorities as listed by the Secretary of State in SI 2010/480) to obtain access to communications data by way of a 'self-authorisation' procedure, that is a procedure for which no judicial authorization is involved. The safeguard is that the requester must make a written application to the "single point of contact" ("SPoC") who is an accredited individual who is able to advise on whether the request is appropriate and lawful: see paragraph 3/15-3.21 Code of Practice. The relevant authority can issue a notice to a CSP requiring the disclosure of the relevant data: s. 22(4) RIPA, which the CSP must comply with.

30. Again, this appears to me to give rise to insurmountable problems when considered in the light of the CJEU's judgment in *Digital Rights Ireland.* As explained, the CJEU made clear that judicial authorization or independent review is likely to be a pre-requisite to lawful interference with communications data such as this.

31. Indeed, it is notable that the Interception of Communications Commissioner (IoCC), who carries out reviews of how the system is working has this year expressed concern that there may be overuse (illegitimate use therefore) by law enforcement agencies of the system for obtaining communications data. For the year 2013 , he reported that 514,608 notices and authorizations were issued. This is slightly down on 2012 when 570,135 such notices and authorizations were made. When one considers that each authorization or notice could cover multiple communications, it is clear that even these figures do not reveal the true extent of data sought and obtained. Indeed, Sir Anthony May (the IoCC) states in his annual report that:

> "In my view the unreliability and inadequacy of the statistical requirements is a significant problem, which requires attention."

32. Sir Anthony May expressed concern at the sheer volume of requests at paragraph 4.28 of his report:

> "The communications data statistics given above are liable to be misleading. But taking the 514, 608 number for Part 1 Chapter II authorization and notices at face value it seems to me to be a very large number. It has the feel of being too many. I have accordingly, asked our inspectors take a critical look at the constituents of this bulk to see if there might be a significant institution overuse of the Part 1 Chapter II powers. This may apply in particular to police forces and law enforcement agencies who between them account for approaching 90% of the bulk."

33. As regards the break-down of these (inadequate) statistics, 87.7% of the 2013 notices and authorizations were made by police forces and law enforcement agencies and 11.5% by intelligence agencies. It therefore appears that the police now use their ability to obtain communications data very frequently indeed.

Data stored or sent overseas.

34. Finally, it is also worth mentioning another pending reference, which has drawn on the judgment of the CJEU in *Digital Rights Ireland*: *Schrems v Data Protection Commissioner* [2013] Np. 765JR. In this case the Claimant is complaining about the fact that his data on facebook is transferred to the US where, as has become clear from the Snowden revelations, data protection is not guaranteed. The High Court (Ireland) that made the reference noted at paragraph 42:

> "The Snowden revelations demonstrate – almost beyond peradventure – that the US security services can routinely access the personal data of European citizens which has been so transferred to the United States and, in these circumstances, one may fairly question whether US law and practice in relation to data protection and State security provides for meaningful or effective judicial or legal control."

35. Judge stated:

> "The essence of the right to data privacy is that, so far as national law is concerned and by analogy with protection afforded by Article 40.5 of the Constitution, that privacy should

> remain inviolate and not be interfered with save in the manner provided for by law i.e. by means of a probable cause warrant issued under s. 6 of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993, on the basis that he interception of such communications involving a named individual is necessary in the interests of either the suppression of serious crime of the protection of national security.
>
> …45. …he is certainly entitled to object to a state of affairs where his data are transferred to a jurisdiction which, to all intents and purposes, appears to provide only a limited protection against any interference with that private data by the US security authorities."

36. The question of whether another State provides sufficient data protection guarantees, is a matter that under Directive 95/48 can be conclusively decided by the Commission. In this case, the EU Commission decided in 2000 that the US did provide sufficient guarantees through its 'safe harbour' provisions. Whilst not framed in this way, it is likely that the Court will examine the legality of the relevant Commission Decision in order to determine this reference.

20 October 2014.