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

CO ref: CO/3794/2014

B E T W E E N:

THE QUEEN (on the application of):
(1) DAVID DAVIS MP;
(2) TOM WATSON MP

Claimants

v.

SECRETARY OF STATE FOR THE HOME DEPARTMENT

Defendant

(1) OPEN RIGHTS GROUP;
(2) PRIVACY INTERNATIONAL

Co-Interveners

INTERVENERS' SUBMISSIONS

I. Introduction

1. This claim concerns extensive new powers of data retention introduced by expedited primary and secondary legislation and raises the fundamental question of their compatibility with the Charter of Fundamental Rights of the European Union ("**CFR**") and the European Convention of Human Rights ("**ECHR**"). These issues are of particular significance in light of "*the important role played by the internet* [...] *in modern society*" (Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (nyr) (ECLI:EU:C:2014:317) ("**Google Spain**") at [80]), in which it has become "*both ubiquitous and increasingly intimate*"[1]. In 2011, the European Commission noted that "[t]*he volume of both telecommunications traffic and requests for access to traffic data is increasing*", with "*over 2 million data requests* [...] *submitted each year*"[2].

2. In its report of Evidence for the Investigatory Powers Review (dated 5 December 2014)[3], the Interception of Communications Commissioner's Office ("**the IOCCO Report**") noted

---

[1] "*The right to privacy in the digital age*", Report of the Office of the United Nations High Commissioner for Human Rights, 20 June 2014, A/HRC/27/37 available at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.
[2] "*Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*" COM(2011) 224 final, Brussels, 18.4.2011, available at http://www.statewatch.org/news/2011/apr/eu-com-data-retention-report-225-11.pdf.
[3] Available at http://www.iocco-uk.info/docs/IOCCO%20Evidence%20for%20the%20Investigatory%20Powers%20Review.pdf.

that "[t]*he volumes and detail contained, especially in traffic data, are at a level not envisaged* [when legislation was introduced] *in 2000*". The capacity of modern mobile devices to access data and materials "*is staggering and so is the volume and detail of the data generated as a result, especially relating to the location of a mobile phone/end user device.*" (§3.2.8).

3. On 8 April 2014, by a judgment in Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger* (ECLI:EU:C:2014:238) (not yet reported) ("***DRI***"), the Grand Chamber of the Court of Justice of the European Union ("**CJEU**") concluded that the Data Retention Directive ("**DRD**")[4] involved a disproportionate interference with individual rights to privacy and data protection, as guaranteed by Articles 7 CFR and 8 ECHR (privacy) and Article 8 CFR (data protection). As a consequence it annulled the DRD, *ab initio*.

4. In response to this ruling, the UK introduced the *Data Retention and Investigatory Powers Act 2014* ("**the 2014 Act**") and the *Data Retention Regulations 2014* ("**the 2014 Regulations**") – together "**the relevant provisions**". In essence, the relevant provisions maintained the regime which had been based on the DRD with minor alterations.

5. The co-interveners, the Open Rights Group ("**ORG**") and Privacy International ("**PI**"), are leading non-governmental organisations which are active in the fields of privacy, in particular freedom of expression, privacy, innovation, consumer rights and creativity on the Internet. They support the claim. They submit that the relevant provisions are contrary to EU law and in particular, in breach of the Data Protection Directive 1995/46 ("**DPD**")[5] and the Directive on privacy and electronic communications 2002/58/EC ("**PECD**"),[6] which provide for directly effective rights to erasure, anonymised data, non-identification of callers and prohibit the retention of location data.[7]

---

[4] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).
[5] 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 (Official Journal L.281, 23.11.1995 at pp.31-50), implemented in the UK by the *Data Protection Act 1998* ("**DPA**").
[6] 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 (Official Journal L.201, 31.07.2002 at pp.37-47), implemented in the United Kingdom by the *Privacy and Electronic Communications (EC Directive) Regulations 2003* (the "**PEC Regulations**").
[7] Cf. Joined Cases C-468/10 and C-469/10, *(ASNEF) v Administración del Estado*, judgment 24 November 2011 ("*ASNEF*") §§50-55.

6. By this intervention, the co-interveners draw the Court's attention to (i) the substantial and carefully calibrated EU rules in the field of data retention, (ii) the seriousness of data retention as an interference with the relevant CFR and ECHR rights and (iii) the inconsistency between the relevant provisions and the strict requirements of EU law.

II. The importance of the EU legal framework

7. There is an extensive EU framework for the regulation of data protection and privacy, including in the digital sector. The DPD and the PECD both regulate the extent and manner in which personal data can be processed. The DPD, which establishes the core requirements of the regime is intended to: "*ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data* (see, to this effect, *IPI* EU:C:2013:715, paragraph 28)." (*Google Spain* at [66]).

8. Section 1 of the 2014 Act is concerned with the retention of "*communications data*" (otherwise referred to as 'metadata'). This data is defined under s.21(4) of the *Regulation of Investigatory Powers Act* ("**RIPA**") as being traffic data and any data *relating to* the communication save for its *contents*, including location data. The starting point in relation to such data is the PECD, which provides for EU-wide harmonisation of the level of protection to be afforded by national laws to the processing of personal data in the electronic communications and telecommunications sectors.[8] Its provisions complement and particularise those provided in the DPD: Article 1 PECD. Crucially, the DPD and PECD were adopted because the Council of Ministers considered that "*the establishment and functioning of the internal market* [were] *liable to be seriously affected by differences in national rules applicable to the processing of personal data*", such that it was necessary to <u>fully</u> harmonise those rules, including those relating to retention and storage of data, and to ensure a high level of protection for fundamental rights, most importantly, the right to privacy: see Recital 7 DPD, *ASNEF* (above) §§27-30; Case C-101/01 *Lindqvist* [2003] ECR I-12971, §§79 and 96.

9. The PECD provides an individual right to confidentiality, erasure and anonymity in

[8] It amended and replaced 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, which also provided for a prohibition on retention and a right to erasure/anonymisation.

respect of one's 'communications' or 'traffic data.'[9] Indeed, it obliges Member States to:

9.1. ensure the confidentiality of such data through the adoption of national legislation to prohibit 'storage' or 'other kinds of interception or surveillance' without the user's consent, save where legally authorised in accordance with Article 15(1): **Article 5(1)-(3) PECD** (see recital (3) of the DRD);

9.2. require electronic communications providers to erase traffic data relating to subscribers and users or make it anonymous when it is no longer needed for the purpose of the transmission of the communication, save where it is necessary to retain the data for billing purposes and/or where legally authorised under Article 15(1): **Article 6 PECD** (recital (3) DRD);

9.3. require service providers to offer the possibility of non-identification for callers (**Article 8**); and

9.4. prohibit the processing (including retention), of location data unless that data is made anonymous or is processed with the user's consent and even then the user must "*continue to have the possibility, using simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication*": **Article 9 PECD** (recital (3) DRD).[10]

10. There was a reason for adopting those rights on an EU-wide basis. Data is not a 'national phenomenon'; it travels across borders and ensures free commerce and free communication. It was for that reason that harmonisation of rules relating to its processing was considered so important for the internal market. In the context of what is being considered in this case, a UK resident may receive a call from a German resident, which will then form part of the UK resident's data, which may be retained. Or a UK resident may search a German internet site or travel to France and send a text. Again that

---

[9] 'Traffic data' is defined in Article 2(b) PECD as data processed for the purpose of the conveyance of a communication on an electronic communications network or for the purposes of billing. 'Electronic communications network' is defined in Directive 2002/21 as a common regulatory framework for electronic communications, networks and services: see Article 2 PECD.

[10] These provisions are implemented by the PEC Regulations. However, r.28 exempts communications providers from its requirements where exemption is required for the purpose of safeguarding national security, which is determined by the issue of a certificate signed by a Minister of the Crown, which "*shall be conclusive evidence of that fact*". It also provides for certain questions relating to such certificates to be determined by the Information Tribunal referred to in section 6 of the DPA.

data will be retained as 'his' data. The data relating to these communications are cross-border data; they give rise to rights not only in the UK but also of those outside the UK. One person's data is also likely to be that of another's. A German resident needs to be sure that when contacting a UK resident, his data rights will be fully protected. This Court is obliged therefore to consider the legality of the relevant provisions on the basis of their inter-state effects; this is not a purely domestic matter.

11. Further, as the CJEU made clear in *DRI*, the DPD and PECD essentially concern three inter-related but distinct aspects of a retention regime: (a) the *retention* of data (including on a mass scale); (b) the *access* regime for such data; and (c) the *storage* and potential *transfer* of such data, including outside the EU. Whilst as explained below, the 'retention' on its own gives rise to very serious issues irrespective of the risk of access/disclosure, it is nevertheless necessary for the Court to consider retention in the light of the existing access/storage regimes. This is particularly because data should not be retained outside the EU under the DPD/PECD. In this regard, the interveners draw the Court's attention to a number of historic legal instruments that appear to provide for the wide circulation and sharing of such data to the United States, for example:

    11.1. The EU-US Passenger Name Record ("PNR") Agreement (OJ 2012, L.215/5) allows PNRs to be collected and transferred to the US authorities in relation to passengers travelling to or from the US for the purpose of the prevention, detection, investigation and prosecution of crime. Such data can be retained for up to 6 months before being depersonalised and retained for a further five years and a total of 15 years in a 'dormant' database;

    11.2. The EU-US agreement on the processing and transfer of Financial Messaging Data (or "**TFTP Agreement**"), which allows the transfer of "financial payment messages" (including the identity of the sender, date and time of transfer, amounts transferred, the purpose, etc.) stored by SWIFT to databases in the US for the purpose of the prevention investigation and prosecution of terrorism or terrorist financing; and

    11.3. Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441), OJ L 215, p.7 ("**the Safe Harbour Decision**") permits the free transfer of personal information from EU Member States to companies in the US

which have signed up to Privacy Principles issued by the Department of Commerce of the United States in circumstances where the transfer would otherwise not meet the EU standards for adequate data protection. The regime relies on commitments and self-certification of adhering companies.[11]

Derogations from the data protection principles

12. By Article 15 of the PECD, Member States can exceptionally restrict the rights set out in Articles 5, 6, 8(1)-(4) and 9 when "*necessary, appropriate and proportionate* [...] *to safeguard national security (i.e State security), defence, public security, and the prevention, investigation, detention and prosecution of criminal offences or of unauthorised use of the electronic communications system, as referred to in Article 13(1) of Directive 95/46*". The Article 29 Working Party Data Protection Group[12] stated in its Opinion 5/2002[13] that the:

> "..retention of traffic data for purposes of law enforcement should meet strict conditions under Article 15 (1)..: i.e. in each case only for a limited period and where necessary, appropriate and proportionate in a democratic society. Where traffic data are to be retained in specific cases, there must therefore be a demonstrable need, the period of retention must be as short as possible and the practice must be clearly regulated by law, in a way that provides sufficient safeguards against unlawful access and any other abuse. Systematic retention of all kinds of traffic data for a period of one year or more would be clearly disproportionate and therefore unacceptable in any case." (emphasis added)

13. That statement reflects the settled case-law of the Court that 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-473/12, *Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert*, judgment of 7 November 2013, §39, citing Case C-73/07 *Satakunnan Markkinapörssi and Satamedia* [2008] ECR I-9831, §56, and Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063, §§77 and 86.

14. Member States are not obliged by the DPA or PECD to adopt any derogations from data processing rights, including the right not to have one's data retained and the right to

---

[11] The legality of the transfer of data out of the EU on the basis of this 'safe harbour decision' is currently being considered by the Court in a preliminary reference from the High Court of Ireland made on 25 July 2014 – Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* (OJ C 351, 06.10.2014, p.5).

[12] Article 29 of the DPD provided for the establishment of this Working Group.

[13] Concerning the precursor to the DRD (Draft Council Framework Decision, Doc 8958/04).

erasure/anonymisation of data. The possibility for derogation under Article 13 of the DPD or Article 15 of the PECD is voluntary and indeed can only be invoked where strictly necessary: see Case C-275/06 *Promusicae* [2008] ECR I-271 and *IPI* (cited above). Further, when invoked, any derogation must comply with the general principles of Union law, including those mentioned in Article 6(1) and (2) of the Treaty on European Union (TEU) (ibid). As the Court stated at paragraph 70 in *Promusicae*:

> "...Member States must, when transposing the directives mentioned above, take care to rely on an interpretation of the directives which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order. Further, when implementing the measures transposing those directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality (see, to that effect, Lindqvist, paragraph 87, and Case C-305/05 Ordre des barreaux francophones et germanophone and Others [2007] ECR I-0000, paragraph 28)."

15. Accordingly, following the adoption of the PECD, there was necessarily disagreement between Member States as to whether the requirements of Article 13 DPD and 15 PECD could be met, that is, whether retention of communications data could be justified under those exceptional provisions. Accordingly, Member States adopted a further Directive, the DRD, as a means of <u>requiring</u> Member States to oblige communications providers to retain data and provide state access to it. The DRD did not purport to comply with the strict requirements of Article 15 of the PECD and indeed was specifically adopted to derogate from Articles 5, 6 and 9 of the PECD: (Article 3 DRD). Further it amended the PECD so as to disapply the strict exception requirements of Article 15 in relation to that data: Article 15(1a) PECD (Article 11 DRD). As AG Cruz Villalón stated in his opinion of 12 December 2013 in *DRI* it "*derogate*[d] *from the derogating rules which are laid down in Article 15(1) of* [the PECD]".

16. The Secretary of State ("**S/S**") accepts that the PECD applies to the communications data at issue but says that the relevant provisions comply with the strict requirements of Article 15: §26 Summary Grounds. The question for this court therefore, is whether that is so. The interveners submit that it is not, for the reasons set out below.

III. The significance of retention of data *per se*

17. The claimants emphasise the importance of access and the inter-relationship between *retention*, *access* and *transfer* of data. The co-interveners also wish to emphasise that, as the CJEU made clear in *DRI*, data interception and retention in itself gives rise to a very serious interference with fundamental rights, irrespective of whether access is subsequently sought or indeed could be subsequently sought. This is because the very fact of retention is likely affect individuals' sense of freedom and impact directly on private behaviour. As the AG and CJEU noted in *DRI*, knowledge that all one's data is being retained is likely to alter how individuals behave and communicate and create a sense of being subject to surveillance that potentially has profound implications for individual freedom within the private sphere.[14] This is so whether or not there is a true or realistic risk that that data will ever be accessed. What matters is the fact of retention; it is this that potentially affects private behaviour and thus interferes with private life[15].

18. As the AG noted in *DRI*, the collection of metadata includes a wide range of information which enables a detailed picture to be painted of an individual's activities, beliefs and relationships to others. The CJEU in *DRI* stressed that:

> "[26] [...] the data [...] 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

---

[14] See, for instance, ORG's report "*Digital Surveillance - Why the Snoopers' Charter is the wrong approach: A call for targeted and accountable investigatory powers*" available at https://www.openrightsgroup.org/assets/files/pdfs/reports/digital-surveillance.pdf.
See further the Witness statement of Edward W. Felten (Director of the Center for Information Technology Policy, Princeton University) in *ACLU & others v James R. Clapper & others* on the sensitive nature of metadata: https://www.aclu.org/files/pdfs/natsec/clapper/2013.08.26%20ACLU%20PI%20Brief%20-%20Declaration%20-%20Felten.pdf.
See also the Council of Europe Commissioner for Human Rights Issue Paper, *The Rule of Law on the Internet and in the Wider Digital World*, December 2014 (p.115, and note the conclusion at p. 117): https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2654047&SecMode=1&DocId=2216804&Usage=2

[15] The German Constitutional Court referred to this as the "*diffusely threatening feeling of being watched*", see https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html.

also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.

27 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."

19. Similarly, the UN High Commissioner for Human rights has stressed that the distinction between the seriousness of interception of metadata and content is "*not persuasive*" and "*any capture of communications data is potentially an interference with privacy* [...] *whether or not those data are subsequently consulted or used*". The mere fact of such capture may indeed have a "*potential chilling effect on rights, including those to free expression and association*"[16]. The Commissioner concluded that "[m]*andatory third-party data retention* [...] *appears neither necessary nor proportionate*" (paragraph [26] at p.9).

20. The S/S's response that "[...] *that having one's communications retained by a telecommunications operator* [...] *is relatively minor*" wholly fails to address the above points. Indeed, it is directly contrary to the statements of the CJEU in *DRI*. The AG considered the interference that retention involved to be "*particularly serious*": §70 and the CJEU considered it potentially so great that it could in fact have an effect on the use of communications and consequently on freedom of expression: §§27-28, creating as it does a '*vague sense of surveillance*': Opinion AG Cruz Villalón §§52, 72.

21. The co-interveners submit that the retention of vast swathes of metadata, including in relation to persons for whom there is no suspicion of criminal behaviour or that they pose a threat to national security, is a serious interference with Articles 7 and 8 CFR and Article 8 ECHR. Indeed, the relevant provisions of the new UK regime potentially entail "*an interference with the fundamental rights of practically the entire European population*" and certainly the entire UK population given that they relate to any "*communications data*" within the meaning of RIPA.

---

[16] "*The right to privacy in the digital age*", *supra* n.1, paragraphs [19]-[20] at pp.6-7. See also "*Surveillance of Emergent Associations: Freedom of Association in a Network Society*", K. J. Strandburg, December 2007 at p.1, available at http://works.bepress.com/katherine_strandburg/11.

22. The S/S says that the objective pursued by her could only be achieved by the retention of all data by communications service providers, since the reason for retaining data is so that it can be used to verify/provide support for allegations, particularly in the context of criminal investigations. Thus it would not be sufficient for data to be collected only in relation to individuals already under investigation, which if necessary could be done pursuant to a warrant[17]. Accordingly, whilst it remains unclear, it appears likely to the interveners that the S/S has issued or will issue notices to all communication service providers in the United Kingdom requiring them to retain all meta-data for all persons to whom it provides communications services for a specified period.[18] Certainly, there is nothing in the terms of the relevant provisions that would prevent her from exercising her powers in this way. When considering the proportionality of these provisions and their compatibility with the requirements of EU law, it is essential that significant weight is given to the seriousness and scale of this interference.

IV. The Requirements of EU law

A. Exceptions to the Directives must be narrowly construed;

23. In *DRI*, the CJEU reiterated that provisions governing data processing and retention - liable to infringe fundamental freedoms in particular the right to privacy - "*must necessarily be interpreted in the light of fundamental rights*" (at [68]). In construing Article 15 and deciding whether the relevant provisions comply with it, the Court must ensure protection for individual rights under Articles 7 and 8 CFR and Article 8 ECHR: Case C-390/12 *Pfleger and ors* 30 April 2014 at §36.

24. Further, as noted above, the Court must interpret the exceptions in Article 15 PECD strictly (see also Case C-119/12 *Josef Probst v mr.nexnet GmbH* (judgment 22 November 2012), at §23). In other words, the relevant provisions must go no further than is strictly necessary to achieve the relevant purpose.

---

[17] See the S/S's evidence to the "*Privacy And Security Inquiry*" of the Intelligence and Security Committee of Parliament on 16 October 2014, Public Evidence Session 7, A7: "[t]*he description of the haystack is a good one, because if you are searching for the needle in the haystack you need to have the haystack in the first place, in order to be able to look for that needle*" available at http://isc.independent.gov.uk/public-evidence.

[18] If this is incorrect and the notices are in fact person specific, the S/S will no doubt state this to be the case and explain not only when she will issue notices but also, the scope of such notices.

B. Substantive requirements:

25. Firstly, for *inter alia* all the reasons set out by the Claimants, the relevant provisions do not comply with Articles 7 and 8 of the Charter or Article 8 ECHR, which they must do in order to meet the requirements of Article 15 PECD and EU law generally.

26. Secondly, the relevant provisions largely duplicate/re-enact the UK regime under the *Data Retention (EC Directive) Regulations 2009 SI 859/2009* ("**the 2009 Regulations**") that implemented the DRD.[19] Indeed, the Government notes to the Bill state that the "*legislation will mirror the provisions of the existing Data Retention Regulations, and create a clear basis in domestic law for the retention of communications data*". This was considered necessary to avoid data held by companies being deleted following the judgment in *DRI*.[20] Thus, the scope of the data to which retention obligations may apply under the relevant provisions is identical to that under the 2009 Regulations: (s.2(1) 2014 Act definition of 'relevant communications data'), as are the extremely broad purposes for which these powers may be exercised (those set out in s.22(2) RIPA (s.1(1) DRIPA)). It is difficult to see how these are any narrower than the generic objective of the "*investigation, detection and prosecution of serious crime*" criticised by the CJEU at [60] of *DRI*, indeed they range wider than the crime and national security grounds referred to in the DPD. Just as was the case under the 2009 Regulations, under the new regime a telecommunications operator is only required to retain data when the S/S issues a notice requiring it to do so, which may set out the extent to which the relevant data retention requirements are to apply: see r.10 of the 2009 Regulations and s.1 of the 2014 Act. Importantly, retention notices adopted under the 2009 Regulations which were not revoked prior to the 2014 Regulations entering into force continue to have effect: r.14 of the 2014 Regulations. Accordingly, in reality, the 2014 Regulations do little more than continue the regime that was intended to implement the DRD[21]. The DRD has been declared unlawful by the

---

[19] The DRD was first implemented by *The Data Retention (EC Directive) Regulations 2007* (revoked and superseded by the 2009 Regulations) with respect to fixed network and mobile telephony. Pursuant to Article 15.3 of the DRD the UK had postponed its application to the retention of communications data relating to internet access, internet telephony and internet e-mail (these in fact being covered by the *Retention of Communications Data (Code of Practice) Order 2003* (adopted under Part 11 of the *Anti-Terrorism, Crime and Security Act 2001*)). The 2009 Regulations covered all these data forms.

[20] They are set out by the Government in notes published by the Home Office on its website https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/330510/Factsheet_Data_Retention.pdf.

[21] Even if such notices expire on 1/1/2015 (see r.14(4)), r.14(6) appears to envisage their re-issue on the same terms.

CJEU in *DRI*, such that the original 2009 Regulations (and the 'notices' issued thereunder) necessarily fail, as do the relevant provisions, which are in essence the same.[22]

27. Thirdly, the Government's position is that "*the new regime contains a series of safeguards that were not present in the Directive*": §4 Summary Grounds. In reality those safeguards are neither 'new' nor come close to meeting the objections of the CJEU to the DRD. Most obviously, as stated above, existing retention notices, which provide for widespread and systematic retention as mandated by the DRD, continue in force. Indeed, following the judgment of the CJEU the Government advised communications providers to carry on retaining data as required by the 2009 Regulations.[23] 'New' safeguards have no relevance to that position; the mandatory requirements of the DRD are given effect by notices issued under the 2009 Regulations.

28. As regards the safeguards said to be provided in the relevant provisions (set out in §§7-8 Summary Grounds), these do not meet the criticisms of the CJEU in *DRI*. Most importantly, they fail entirely to specify restrictions on the S/S's entitlement to issue a retention notice. The new regime does not lay down the clear and precise rules that the CJEU has said are needed to govern the scope and application of the measure in question and to impose minimum safeguards: §§54-55, 65 *DRI*. In particular, there is nothing in the relevant provisions that requires a retention notice issued by the S/S:

    a. to be person- or crime- specific. Indeed there is no obligation on the S/S to satisfy herself that there is any connection (even indirect) between the person whose data is being collected and a situation which is liable to give rise to criminal prosecutions. The data retention obligation in the notice not only can but, having regard to the stated purpose behind the legislation, is likely to capture the data of persons for whom there is no evidence capable of suggesting their conduct might have a link, even an indirect or remote one, with a serious crime, which the Court explicitly criticised: §58 - 59 *DRI*. This breadth renders the relevant provisions arbitrary - "*it will not be enough that the measures are targeted to find certain needles in a*

[22] It is understood this is subject to legal challenge in *R (Cosgrove) v S/S for the Home Department* CO 7701/2011.
[23] HC Deb June 2014 c445W.

haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate"[24].

b. to exclude persons whose communications are subject to professional secrecy obligations: §58 *ibid*;

c. to be confined to the minimum period 'strictly necessary': §62 *ibid*. In particular, the retention of "*subscriber data*" (i.e. the data falling within the 'catch-all' provision of s.21(4)(c) RIPA, per r.2) is authorised for up to 12 months after "*the day on which the person concerned leaves the telecommunications service concerned or (if earlier) the day on which the data is changed*" (r.4(2)(b)). This could potentially be a very lengthy period – and it is entirely unclear why a period longer than 12 months is necessary (as noted by the AG at [149] of his Opinion in *DRI*);

d. to ensure that the data is retained within the EU: §68 *ibid*[25]. Indeed, as noted above in *Schrems*, the CJEU is faced with a preliminary reference in relation to the compatibility of the Safe Harbour Decision with Articles 7, 8 and 47 CFR. It is therefore clear that there is increasing concern about the ultimate destination and use of data which is retained. This must necessarily be limited to what is proportionate in order to pursue a legitimate aim.

29. Finally, rules governing restrictions on access to retained data are insufficient. Under Part II of RIPA a wide range of public authorities can obtain access and do so for purposes not confined to safeguarding national security or the prevention, detection or prosecution of defined, sufficiently serious crimes: §§60-62 *ibid*. Indeed, the Interception of Communications Commissioner (the Rt Hon. Sir Anthony May) in his 2013 report (p.38)[26] noted that 514,608 authorisations and notices requesting retained data were issued in 2013 and raised the question whether there is currently an "institutional overuse" of such authorisations and notices. The IOCCO Report noted that "[t]*here is an absence of consolidated guidance as to what may be done with the data outside the boundary of the justifications as to why the data was acquired in the first instance*" (§3.10.4).

---

[24] "*The right to privacy in the digital age*", *supra* n.1, paragraph [25] at p.9.
[25] See also, *ibid.*, paragraph [27] at p.9.
[26] Available at http://www.iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf.

30. The co-interveners are both parties to proceedings challenging the lawfulness of related access regimes which have come to light, namely the receipt and use of data from the NSA's "PRISM" and "UPSTREAM" programmes by British intelligence services and GCHQ's acquisition of communications under broad and rolling warrants of data transmitted on transatlantic fibre-optic cables under the "TEMPORA" programme. ORG is currently an applicant in a case before the European Court of Human Rights (*Big Brother Watch, Open Rights Group, English PEN & Constanze Kurz v United Kingdom* (Application No. 58170/13)). PI is an applicant in a case against the British security services, and Foreign and Home Secretaries, in the Investigatory Powers Tribunal ("**IPT**") (*Privacy International v The Secretary of State for Foreign and Commonwealth Affairs and Ors* IPT/13/92/CH). Judgment was handed down on some of the issues in that case on 5 December 2014 ([2014] UKPITrib 13_77H) but the determination of legality of the access regime remains outstanding. The existence of a power for bulk retention of data, in light of this extensive and unconstrained access regime, is a particularly serious interference with the rights protected by Article 7 and 8 CFR and 8 ECHR.

V. Conclusion

31. The co-interveners respectfully invite the Court to grant the relief sought, in particular an order disapplying s.1 of DRIPA and the 2014 Regulations, in light of their failure to comply with EU law.

32. In the co-interveners' view, the matters before the Court are *acte claire*, which should be determined without the Court needing to refer the matter to the CJEU, given that the *DRI* judgment is clear as to the requirements with which legislation governing data retention must comply. In other words "[t]*he correct application of* [EU] *law* [is] *so obvious as to leave no scope for any reasonable doubt as to the manner in which the question raised is to be resolved*" (Case 283/81, *CILFIT Srl v Ministero della Sanità* [1983] 1 C.M.L.R.472, p.491 at [16]-[18]; applied by the House of Lords in *Factortame Ltd. and Others Appellants v Secretary of State for Transport (No 1)* [1990] 2 A.C. 85 at p.152C-D per Lord Bridge of Harwich). Before reaching this conclusion, "*the national court* [...] *must be convinced that the matter is equally obvious to the courts of the other member-States and to the Court of Justice*".

33. The co-interveners submit that the CJEU's position has been recently and authoritatively elaborated. The relevant provisions do not sufficiently address the serious concerns

identified therein and would therefore fall foul of the *DRI* test. As to the other Member States, the co-interveners have initiated research into the response to the *DRI* judgment in other Member States of the Union[27] and refer the Court to other existing analysis of the comparative position[28]. It is instructive to note that similar legislation has been struck down by the highest administrative and constitutional courts in Germany, Bulgaria, Romania, Cyprus, the Czech Republic, Slovenia and Austria without any need for a reference to the CJEU. Other proceedings are ongoing. In particular, the Austrian decision (27 June 2014) upon return of the preliminary ruling in *DRI* is a recent example of the application of *DRI* to national implementing legislation finding breaches of the CFR and ECHR. Other Member States have indicated their intention to enact new legislation revising their data retention regimes. Accordingly, the position is *acte clair* and the relevant provisions should be disapplied.

34. To the extent that the Court retains doubts as to the compatibility of the relevant provisions *with the DRI principles*, however, then it would be appropriate for the matter to be referred to the CJEU to clarify how the *DRI* requirements apply outside the context of the DRD, and within the scope of Article 15 PECD. Indeed, in case of such doubt, the co-interveners submit that the Court would be bound to refer the matter to the CJEU as "*a decision on the question is necessary to enable it to give judgment*" (per Article 267 TFEU). The co-interveners would wish to be joined to any such reference (see *R (Philip Morris Brands Sarl and ors) v Secretary of State for Health* [2014] EWHC 3669).

23 December 2014

JESSICA SIMOR QC
Matrix Chambers

RAVI S. MEHTA
Blackstone Chambers

DEIGHTON PIERCE GLYNN

Acting *pro bono*

---

[27] Available at: https://www.openrightsgroup.org/ourwork/reports/status-of-data-retention-in-the-eu-following-the-cjeu-ruling.
[28] See, e.g. "*Data Retention after the Judgement of the Court of Justice of the European Union*", Boehm & Cole, Münster/Luxembourg, 30 June 2014, available at http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf.

CO ref: CO/3794/2014

IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
ADMINISTRATIVE COURT
B E T W E E N:

THE QUEEN on the application of

(1) DAVID DAVIS MP

(2) TOM WATSON MP

Claimants

- and -

SECRETARY OF STATE FOR THE HOME DEPARTMENT

Defendant

- and -

(1) OPEN RIGHTS GROUP

(2) PRIVACY INTERNATIONAL

Co-Interveners

INTERVENERS' SUBMISSIONS

Deighton Pierce Glynn
Centre Gate, Colston Avenue
Bristol
BS1 4TR

Tel: 0117 317 8133
Fax: 0117 317 8093
Ref: DC/2515/001

Solicitors to the Co-Interveners