your ref 1012115 EN
our ref AH/DC/2515/001/LCA
25 February 2016

dpg
deighton pierce glynn

Court of Justice of the European Union
Registry
L – 2925 LUXEMBOURG

Also Sent by Email: ecj.registry@curia.europa.eu

And by Fax: 00 352 43 37 66

Dear Sir/Madam

Reference for a Preliminary Ruling C-698/15
Davis, Watson, Brice & Lewis v Secretary of State for the Home Department (Open Rights Group, Privacy International and the Law Society intervening)
Court of Appeal (England & Wales) (Civil Division) – United Kingdom

We represent the Open Rights Group and Privacy International ('the NGO Interveners') in the above reference. Thank you for your letter of 27 January 2016 inviting Written Observations by today's date. We **enclose** the NGO Interveners' Written Observations, together **with** Annexes.

Please note that the NGO Interveners intend to be represented at the hearing, by the representatives shown on the first page of their Written Observations.

Thank you for your prompt attention in this matter.

Yours faithfully

DEIGHTON PIERCE GLYNN

Encs

Deighton Pierce Glynn
Suite 201 QC30
30 Queen Charlotte Street
Bristol BS1 4HJ
DX 7859 BRISTOL

t: 0117 332 3598
f: 0117 370 1036
e: bristol@dpglaw.co.uk
w: dpglaw.co.uk

IN THE COURT OF JUSTICE OF THE EUROPEAN UNION
CASE C-698/15

ON A REFERENCE FROM
THE COURT OF APPEAL OF ENGLAND & WALES (CIVIL DIVISION)

Neutral citation: [2015] EWCA Civ 1185

B E T W E E N:

SECRETARY OF STATE FOR THE HOME DEPARTMENT

Appellant

v.

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

Respondents

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

Interveners

WRITTEN OBSERVATIONS OF OPEN RIGHTS GROUP & PRIVACY INTERNATIONAL ("the NGO Interveners")

Submitted by:

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

Tel: +44 117 317 8133
Fax: +44 117 317 8093
Ref: DC/2515/001

Solicitors to the NGO Interveners

JESSICA SIMOR QC
Matrix Chambers

RAVI MEHTA
Blackstone Chambers

25 February 2016

I. INTRODUCTION

1. These are the observations of Open Rights Group and Privacy International ("**the NGO Interveners**"), leading non-governmental organisations active in the fields of privacy, freedom of expression, innovation, consumer rights and creativity on the Internet.

2. The reference concerns data retention powers introduced by the UK following the Court's judgment on 8 April 2014 in Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger* (ECLI:EU:C:2014:238) ("***DRI***"). It has been expedited to be heard on the same day as Case C-203/15 *Tele2 Sverige AB* ("***Tele2***"). These references raise fundamental questions regarding the legality of national data retention and access regimes. The Court dealt fully with these questions very recently in *DRI*, in which it struck down the Data Retention Directive ("**DRD**")[1], which provided for harmonised national powers of retention and access, in derogation from the provisions of the Directive on privacy and electronic communications ("**PECD**")[2] and the Data Protection Directive ("**DPD**")[3]. The consequence of *DRI* was that the UK's measures implementing the DRD[4] were deprived of a legal basis. Accordingly, by way of expedited procedure, the UK Parliament enacted almost identical legislation by way of primary and secondary legislation: the *Data Retention and Investigatory Powers Act 2014* ("**DRIPA**") and the *Data Retention Regulations 2014* ("**the Regulations**").

3. There is no dispute that this legislation falls within the scope of EU law and accordingly must comply with its fundamental principles, including the protection of human rights as set out in the Charter of Fundamental Rights of the European Union[5] ("**CFR**") and the European Convention of Human Rights ("**ECHR**"). By this reference, and that in *Tele2*, the Court is in effect being asked to consider again its recent and clear ruling in *DRI*. This is so despite the Court having already provided further clarification in its judgment in Case C-362/14 *Maximillian Schrems v Data Protection Commissioner*

---

[1] Directive 2006/24/EC, 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 (OJEU 2006 L105, pp.54-63).

[2] Directive 2002/58/EC, concerning the processing of personal data and the protection of privacy in the electronic communications sector (OJEC L.201, 31.07.2002, pp.37-47).

[3] Directive 95/46/EC, on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJEC L.281, 23.11.1995, pp.31-50).

[4] The *Data Retention (EC Directive) Regulations 2009* (S.I. 859/2009) ("**the 2009 Regulations**").

[5] Consolidated version, OJEU C326, 26.10.2012, pp.391–407.

(ECLI:EU:C:2015:650), ("***Schrems***"). In those two cases the Court tackled the difficult questions raised not only by the "*the important role played by the internet* [...] *in modern society*" (see Case C-131/12, *Google Spain SL* (ECLI:EU:C:2014:317) ("***Google Spain***") at [80]), in which it has become "*both ubiquitous and increasingly intimate*"[6] but also, the challenges faced by the need to provide security and prevent acts of terrorism. The latter had been the driving force behind the enactment of the DRD, following the attacks in Madrid in 2004 and London in 2005: see recitals 8 and 10. It is somewhat surprising that so soon after *DRI* and *Schrems*, the Court is being asked to reconsider the compatibility of "*automatic processing*", on a "*generalised basis*", of "*all means of electronic communication* [...of] *practically the entire European population* [...]", (*DRI* at *Schrems* at [91]).

4. The NGO Interveners submit that - as found by the CJEU in *DRI* and the High Court in this case - the relevant provisions of national law breach the DPD and PECD, interpreted consistently with Articles 7 and 8 of the CFR, which prohibit wholesale data retention and provide for directly effective rights to erasure, anonymised data and non-identification of callers[7].

II. FACTUAL BACKGROUND

5. The NGO Interveners adopt the factual background set out in paragraphs 1-10 of the Order for Reference. However, they would add the following points of emphasis.

6. As accepted by the Secretary of State in the national proceedings, the relevant provisions largely duplicate/re-enact the pre-existing UK regime implementing the DRD. Indeed, the Government notes to the Bill introducing DRIPA stated 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*"[8]. Retention notices adopted under the 2009 Regulations, which were not revoked prior to the Regulations entering into force,

---

[6] "*The right to privacy in the digital age*", Report of the Office of the United Nations High Commissioner for Human Rights ("**UNHCHR**"), 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 at §1 (**Annex 1**).

[7] See, e.g. Joined Cases C-468/10 and C-469/10, *(ASNEF) v Administración del Estado* [2011] ECR I-12181 (ECLI:EU:C:2011:777) ("***ASNEF***") at [50]-[55].

[8] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/330510/Factsheet_Data_Retention.pdf (**Annex 2**).

continued to have effect until 1 January 2015: r.14 of the Regulations.

7. Pursuant to Chapter II of Part I of the *Regulation of Investigatory Powers Act 2000* ("**RIPA**"), a wide range of public authorities can obtain access to retained data and can do so for purposes that are not confined to the safeguarding of national security or the prevention, detection or prosecution of defined, sufficiently serious crimes. The Interception of Communications Commissioner, in his 2014 report (p.47)[9], recorded 517,236 authorisations and notices requesting retained data issued in 2014 alone.

III. RELEVANT PROVISIONS OF NATIONAL AND EU LAW

Relevant national law provisions

8. The summary of national legal provisions is set out at paragraphs 11-29 of the Order for Reference. The UK notified the legislation to the European Commission under the Technical Standards Directive[10], specifically stating that "*the legislation implements within the UK a derogation under Article 15 from the e-Privacy Directive*"[11].

Relevant EU Law

9. The DPD, which establishes the core requirements of the EU's data protection 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*" (*Google Spain* at [66]; *Schrems* at [39]).

10. The PECD builds on that level of protection in the context of electronic communications. It provides an individual right to confidentiality, erasure and anonymity in respect of one's 'communications' or 'traffic data' . Indeed, it obliges Member States to:

(a) 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

---

[9] Available at http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf (**Annex 3**).

[10] Directive 98/34/EC, laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services (OJEC L 204, 21.7.1998, p. 37) (as amended).

[11] See notification 2014/0354/UK - V00T, available at http://ec.europa.eu/enterprise/tris/pisa/app/search/index.cfm?fuseaction=pisa_notif_overview&iYear=2014&inum=354&lang=EN&sNLang=EN&CFID=11189550&CFTOKEN=a9a85accc7e038be-9D441D00-07FC-E917-D8ADDE023E16B0FD.

consent, save where legally authorised in accordance with Article 15(1): **Article 5(1)-(3) PECD** (see recital (3) of the DRD);

(b) 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);

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

(d) 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).

11. As the Court made clear in *DRI* (at [32], [35] and [68]) and *Schrems* (at [93]-[94]), the DPD and PECD concern three inter-related, 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) its *storage* and potential *transfer*, including outside the EU. Whilst as explained below, '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.

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 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 that the:

[12] Established under Article 29 DPD.

"..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. [...] 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 apply only insofar as is strictly necessary: (see Case C-212/13 *Ryneš v Úřad pro ochranu osobních údajů* (ECLI:EU:C:2014:2428) at [28]). On 10 April 2014, the Working Party published its "*Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes*" (819/14/EN WP 215)[13], in which it reiterated, *inter alia*, that:

"[...] massive and indiscriminate surveillance programs are incompatible with our fundamental laws and cannot be justified by the fight against terrorism or other important threats to national security." (p.1)

14. Derogations under Article 15 of the PECD can only be invoked where strictly necessary: see Case C-275/06 *Promusicae* [2008] ECR I-271 (ECLI:EU:C:2008:54). If invoked, the derogation must comply with the specific provisions of Articles 15 PECD, as well as the general principles of Union law, including the protection of fundamental rights: Article 6(1) and (2) of the Treaty on European Union ("**TEU**"). As the Court stated in *Promusicae* (at [70]):

"...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[...]"

15. The CFR also applies by virtue of Article 51, which provides that it applies to Members States when they are "*implementing EU law*", i.e. whenever a Member State is acting

[13] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf (**Annex 4**).

"*within the material scope of EU law*"[14]. Articles 7 (respect for private and family life) 8 (the right to protection of personal data) are at issue in this context.

16. As the Explanations set out (at p.20), Article 7 CFR corresponds to Article 8 ECHR, and Article 8 CFR corresponds closely to the rights protected under Article 16 of the Treaty on the Functioning of the European Union ("**TFEU**") and Article 39 TEU, as well as the DPD/PECD.

IV. THE FIRST QUESTION REFERRED

17. The Court is asked whether the principles that it laid down in its judgment in *DRI* and in particular the conditions set out in paragraphs 60-62 are mandatory requirements of EU law that apply to national regimes for data retention and access. The Interveners submit that they plainly are and that absence compliance with those conditions, national measures breach Article 15 PECD and Articles 7 and 8 of the CFR. There are no bases for suggesting otherwise, as reflected in the finding of numerous national courts, including the High Court in this case and Courts in Austria[15], Belgium[16], Bulgaria[17], Netherlands[18], Poland[19], Romania[20], Slovakia[21], and Slovenia.[22] Even prior to *DRI*, the highest administrative or constitutional courts of Bulgaria[23], Cyprus[24], the Czech Republic[25], Germany[26] and Romania[27] declared the whole or parts of national legislation implementing the EU Data Retention Directive void[28].

---

[14] See the Explanations Relating to the Charter of Fundamental Rights (2007/C 303/02) OJ 2007 C303/17, p.32.

15 Decision No. G 47/2012, http://fra.europa.eu/en/caselaw-reference/austria-constitutional-court-g472012-ua.

16 http://www.const-court.be/public/f/2015/2015-084f.pdf [in French].

17 http://constcourt.bg/caseframe/caseid/477 [in Bulgarian].

18 *Privacy First Foundation et al. v. the State of the Netherlands*, case number C-09/480009/KG ZA 14/1575, http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2015:2498 [in Dutch].

19 http://trybunal.gov.pl/sprawy-w-trybunale/art/2013-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani-4/ [in Polish].

20 Press release, http://www.ccr.ro/noutati/COMUNICAT-DE-PRES-99 [in Romanian]

21 http://www.eisionline.org/images/Data_retention_rozhodnutie_PL_US_10_2014.pdf [in Slovak] and see also https://edri.org/slovakia-mass-surveillance-of-citizens-is-unconstitutional/.

22 https://www.ip-rs.si/fileadmin/user_upload/Pdf/sodbe/US_RS_ZEKom-1_3julij2014.tif [In Slovenian] and see also https://edri.org/slovenia-data-retention-unconstitutional/.

23 See http://www.aip-bg.org/documents/data_retention_campaign_11122008eng.htm.

24 See judgment here: http://www.supremecourt.gov.cy/Judicial/SC.nsf/All/5B67A764B86AA78EC225782F004F6D28/$file/65-09.pdf [in Greek].

25 See https://edri.org/czech-decision-data-retention/.

26 Judgment of the *Bundesverfassungsgericht* of 2 March 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html [in German].

A. The Scope of EU law:

18. Member States are obliged to give effect through national implementing legislation to the rights and protections identified at paragraph [10] above as specified in the PECD (and DPD). The UK accepts that the relevant legislation must comply with the terms of the PECD, as evidenced by its notification to the Commission at paragraph 8 above.

19. The PECD and DPD recognise that data protection must be ensured 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. 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 pursuant to the national regime. But this data is also that of someone outside the UK. Put another way, one person's data is likely to include that of another's. Similarly, two German citizens may communicate via an internet service, or an EU citizen may use a website, which is hosted or transits servers in the UK. Given the UK's importance as a hub of global internet traffic, neither scenario is unlikely. These citizens need to be sure that when contacting others or using the internet, their data rights will be fully protected. This Court should therefore (consistently with its well-established case law) consider the legality of the relevant provisions on the basis of their inter-state effects.

20. The purpose and effect of DRIPA and the Regulations is to provide for retained data to which access may be gained by relevant authorities. The retention of and access to data under the DRIPA regime includes data relating to cross-border communications. It is wrong therefore to suggest that somehow 'access' measures can be taken outside of the scope of EU law and examined as if they were solely 'national' measures with no cross-border effects. As is clear from the PECD, 'national security' is a ground on which Member States may restrict the relevant rights but only in so far as strictly necessary and proportionate as provided in Articles 15 PECD. These rules are designed to ensure that – within the rules of the EU – a balance may be struck between the interests at play. It

---

27 http://www.legi-internet.ro/fileadmin/editor_folder/pdf/Decizie_curtea_constitutionala_pastrarea_datelor_de_trafic.pdf [In Romanian.]

28 See the table of Member State Decisions at **Annex 5.**

follows that the Court's analysis in *DRI* of the CFR's requirements when applied to an EU harmonising measure applies by analogy to national measures occupying substantially the same field.

21. In that regard, the Council of Europe's Commissioner for Human Rights[29] correctly concluded that as a result of *DRI* "*untargeted compulsory data retention may therefore no longer be applied under EU law, or under national laws implementing EU law. Since national data-retention laws explicitly do exactly that, they will all have to be fundamentally reviewed and replaced with targeted surveillance measures*" (p.116, emphasis added).

B. The seriousness of mass retention:

22. As the Court made clear in *DRI*, interception and retention on a mass/generalised basis of communications or metadata 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[30]. This is because the very fact of retention will affect how individuals communicate, impacting directly on private behaviour. As noted by the Advocate General and the Court in *DRI* a sense of being subject to surveillance has potentially profound implications for individual freedom within the private sphere. What matters is the fact of retention; it is this that potentially affects private behaviour and thus interferes with private life[31].

23. Regard must also be had to the reason why data is being retained. The single greatest restraint on powers of access and transmission is the effective limitation of the data retained, as recognised by the Court in *DRI*.

24. Nor is that interference reduced by it not including the content of communications. 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: as the Court

---

[29] "*The rule of law on the internet and in the wider digital world*", 8 December 2014, https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2654047&SecMode=1&DocId=2216804&Usage=2 (**Annex 6**).

[30] See e.g. judgment of the Grand Chamber of the ECTHR in *S and Marper v UK* Nos. 30562/04, (2009) 48 E.H.R.R. 50, (4 December 2008).

[31] 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.

noted in *DRI* (at [26]-[27]). Similarly, the UNHCHR has stressed[32] 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*". The Commissioner concluded that "[m]*andatory third-party data retention* [...] *appears neither necessary nor proportionate*" (paragraph [26] at

25. Further, as the Council of Europe's Commissioner has noted, "*extensive research has failed to show any significant positive effect on clear-up rates for crime, and especially not for terrorism-related crime, as a result of compulsory data retention*" (report *supra*). As he stressed, metadata can be "*unreliable and can unwittingly lead to discrimination on grounds of race, gender, religion or nationality. These profiles are constituted in such complex ways that the decisions based on them can be effectively unchallengeable: even those implementing the decisions do not fully comprehend the underlying reasoning*" (p.8). Alternatives to mass data retention exist, including targeted preservation orders. Under this model, public authorities would request the preservation of communications data of specific individuals based on an investigation or proceedings. Flexibility exists within this model for developing enhanced preservation requirements in emergency situations and sensitive contexts.

26. The NGO 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.

27. There can be no doubt that a regime providing for retention, with no effective rules on limiting access to retained data, would be unlawful under PECD. This approach has recently been confirmed by the European Court of Human Rights ("**ECtHR**") in its judgments in *Zakharov v Russia*[34] ("***Zakharov***") and *Szabó and Vissy v Hungary*[35]

---

[32] In its report published on 30 June 2014, *"The right to privacy in the digital age*" (A/HRC/37), see fn.6.
[33] See also the report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson QC, UN doc. (A/69/397) at [55] (**Annex 7**).
[34] (Application no. 47143/06), Decision of the Grand Chamber, 4 December 2015.

("***Szabó***"), examined in detail at paragraph 34 below. In *Szabó*, the ECtHR specifically noted that "*the possibility occurring on the side of Governments to acquire a detailed profile* [...] *of the most intimate aspects of citizens' lives may result in particularly interferences with private life*", which must "*be subjected to very close scrutiny both on domestic level and under the Convention*" (at [70]).

28. The Court's conclusions in *DRI* articulate minimum requirements of EU law in relation to a data retention regime within the scope of EU law. Similarly, this Court's decision in *Schrems*, at [88] and [94], recently confirmed such an approach in relation to the position in the United States, noting that "*legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications* [...] *compromis*[es] *the essence of the fundamental right to respect for private life*".

29. These 'downstream' aspects of retention are of particular relevance in light of the current proposed reform to the UK's legislative framework for the acquisition and retention of communications data, including on a bulk and generalised basis. The *Investigatory Powers Bill*, currently before the UK Parliament, envisages placing, on an explicit statutory footing, powers to acquire communications data and intercept communications on a bulk, generalised basis. The Bill foresees the retention of new categories of information such as "*internet connection records*" (i.e. data used to identify a telecommunications service to which a communication is transmitted through a telecommunication system such as each website visited by an EU citizen using the service) and adds an additional power to require telecommunications operators to begin to capture and retain data which they would not otherwise require, with no prior judicial authorisation, relying instead upon internal reviews by public authorities able to exercise powers under the legislation.

C. Article 15 PECD:

30. Article 15 is the *lex specialis* for the exercise by Member States of any derogation or exception from the rights and protections guaranteed in the PECD, only when strictly necessary for the purposes set out in that provision. Thus, Article 15(1) provides for the possibility of Member States adopting "*legislative measures providing for the retention of*

---

[35] (Application no. 37138/14), Decision of the Fourth Section, 12 January 2016.

data for a limited period justified on the grounds laid down [therein]". The relevant grounds include "*national security, and the prevention, investigation, detection and prosecution of criminal offences.*" Article 15(1) expressly refers in that regard to the need to ensure that any derogating measures adopted by a national authority complies with "*general principles of Community law, including those referred to in Article 6(1) and 6(2) of the* [TEU]."

31. The grounds on which data can be retained and thereafter accessed under DRIPA are wider than those set out in Article 15 PECD; on the UK's admission they mirror the previous legislation that implemented the DRD, which has since been struck down by the Court as incompatible with Articles 7 and 8 CFR. In support of its contention that it is not limited to the grounds set out in Article 15 PECD, the UK relies on a decision of the English Court of Appeal: *R (British Telecommunications PLC) v Secretary of State for Culture, Olympics, Media and Sport* [2012] EWCA Civ 232; in which it held that "*the grounds for derogation under article 15(1) of* [the PECD] *included the purposes listed in article 13(1) of the* [DPD]" (at §63). Whether or not that is correct, it does not assist. Article 13(1) must also be applied in a way that is compatible with Articles 7 and 8 CFR. To the extent that the Court's decision in *Promusicae* (at [53]) can be said to have expanded the grounds specified in Article 15, it is submitted that the Court was not in that case in any sense allowing for the kind of general and widespread measures that it ruled unlawful in *DRI*. Indeed that case preceded *DRI*. Article 15 PECD must be interpreted in such a way as to reflect the object and purpose of the PECD and the seriousness of the interference with fundamental rights guaranteed by EU law.

V. THE SECOND QUESTION REFERRED

32. By its second question, the referring Court is seeking to identify the requirements of Articles 7 and 8 CFR in this field, and determine whether these go further than those of the ECHR. The NGO Interveners submit that:

(a) The Court made clear in its Opinion 2/13 (ECLI:EU:C:2014:2454) that EU law forms an autonomous body of law over which the CJEU has jurisdiction, including in relation to fundamental rights and freedoms: see [166]-[177] and [201]-[244].

(b) Article 52(3) CFR is explicit in providing that insofar as rights set out in the CFR

correspond to those in the ECHR their meaning and scope shall be same as laid down by the latter, albeit that there is nothing that prevents EU law providing for *greater* rights protection and nothing in the CFR shall be taken as restricting or adversely affecting existing rights: Article 52(3) and 53.

(c) In this case, Article 15 PECD provides the specific EU rules in relation to restrictions on rights guaranteed by the PECD. Article 8 of the CFR, moreover, concerns a right not contained in the ECHR.

(d) In any event, however, nothing in the Court's approach in *DRI* was in conflict or went beyond any ruling by the ECtHR. The NGO Interveners emphasise that the requirements of Art.8 ECHR are entirely consistent with those which this Court has identified in *DRI* and *Schrems*.

33. In *Zakharov*, the Grand Chamber of the ECtHR recently re-iterated its well-established case-law in the context of surveillance measures (at [227]-[232]). The Court held that the security interests on which the State could rely under national law were too wide, rendering the legal framework unforeseeable (at [246]-[248]). It identified the risk of "*automatic storage of clearly irrelevant data*" (at [255] and [302]). Moreover, it emphasised that "*it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure*", provided the scope of that control was wide enough and effective to provide scrutiny of the relevant powers (at [233], [249] and [258]-[261]).

34. In *Szabó,* the ECtHR explicitly endorsed this Court's recent case-law (see [73]), particularly in the absence of individualised suspicion (see [71]). The Court noted that "[g]*iven the technological advances since the* Klass and Others *case, the potential interferences with email, mobile phone and Internet services as well as those of mass surveillance attract the Convention protection of private life even more acutely*" (at [53]). Referring to this Court's jurisprudence, it also raised concerns about the use of widespread surveillance operations, which could amount to "*unfettered executive power intruding into citizens' private spheres*" (at [68]). It distinguished the *Kennedy* case on the basis that the UK's impugned legislative provisions there did "*not allow for "indisicriminate capturing of vast amounts of communications*"" (at [69]). The Court reiterated the importance of

judicial supervision (at [75]-[79]).

35. Accordingly, the NGO Interveners submit that the scope of Article 7 CFR, which corresponds to Article 8 ECHR, is entirely consistent with this Court's analysis in *DRI*.

36. Article 8 CFR as an independent right: Further and in any event, as the referring Court correctly concluded, Article 8 CFR does not correspond precisely to Art.8 ECHR. This is clearly set out in the Explanations to the Charter (p.20). To the extent that the Court's reasoning and conclusions in *DRI* go beyond that article of the Convention (which is denied), then the Court was perfectly entitled to derive the relevant requirements from Art. 8 CFR, which recognises the importance of data protection under EU law.

37. Proportionality: Finally, the NGO Interveners submit that the features of the domestic regime at issue in these proceedings are inherently disproportionate, such that the application of the *DRI* principles to that regime would not go beyond the scope of Art. 8 ECHR.

38. The UK's legislation relies upon vague concepts such as "*national security*", which is a notion of considerable breadth and uncertainty. In its 2014 Opinion, the Working Party highlighted the fact that, "[t]*here is currently no common* [EU-wide] *understanding of is meant by national security*" (p.14). Whilst national security remains within the competence of individual Member States, this Court has regularly insisted, since its seminal decision in *Van Duyn v Home Office*[36], that concepts such as "*public policy*" or "*public security*", relied upon to derogate from fundamental freedoms, "*must be interpreted strictly*" and "*cannot be determined unilaterally by each Member State without being subject to control by the institutions of the* [Union]". The Court has also regularly emphasised that concepts such as '*risk to public policy*' or "*public security*", presuppose the existence, in addition to the perturbation of the social order which any infringement of the law involves, of a genuine, present and sufficiently serious threat affecting one of the fundamental interests of society and denote a threat to the functioning of the institutions and essential public services and the survival of the population, as well as the risk of a serious disturbance to foreign relations or to peaceful coexistence of nations, or a risk to

[36] Case 41/74 [1974] E.C.R. 1337 (ECLI:EU:C:1974:133) at [18]. See also Case C-348/09 *PI v Oberburgermeisterin der Stadt Remscheid* (ECLI:EU:C:2012:300), at [23] and the case-law cited therein.

military interests, may affect public security, (see, e.g. Case C-601/15 PPU *J.N. v Staatssecretaris van Veiligheid en Justitie* (ECLI:EU:C:2016:84) (at [65]-[67])).

39. In the context of DRIPA, this proposition is particularly important. The retention of data envisaged by DRIPA is widespread, indiscriminate and not specifically targeted at a group of persons. It is unlikely that such broad, wholesale retention of communications data is permissible at all under Article 15 PECD/Articles 7 and 8 CFR. In that regard, Advocate General Cruz Villalón in *DRI* expressed particular concern about the potential for wholesale retention to create a "*feeling of surveillance*": (see [69], [72]-[74]). As he noted (at [52]) this is "*capable of having a decisive influence on the exercise by European citizens of their freedom of expression and information*": see also judgment of the Court to the same effect at [28]. This approach has now been confirmed in *Schrems*, where the Court noted that the derogation provision in the Safe Harbour Decision was "*too general*" and therefore "*not limited to what is strictly necessary*" (at [87]).

VI. CONCLUSION

40. For the reasons set out above, the NGO Interveners respectfully invite the Court to answer the questions referred as follows:

    1. The Court's judgment in *DRI* must be interpreted as meaning that it lays down requirements, in the light of Articles 7 and 8 of the Charter, which are applicable to a national regime governing retention of electronic communications data and access to such data.

    2. Articles 7 and 8 of the Charter must be interpreted as meaning that their requirements are at least as strict as those stemming from Article 8 ECHR, and particularly in relation to Article 8 of the Charter and Article 15 of the PECD (which must be read in the light of the specific guarantees from which it provides a power of derogation), may be more strict than such requirements.

25 FEBRUARY 2016

DEIGHTON PIERCE GLYNN

JESSICA SIMOR QC

Matrix Chambers

RAVI MEHTA

Blackstone Chambers

SCHEDULE OF ANNEXES TO

WRITTEN OBSERVATIONS OF NGO INTERVENERS

Annex Reference	Description	Length	Page and para. number of reference to annex
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	16	2(§3), FN6
2	Data Retention and Investigatory Powers Bill Factsheet #1	2	2 (§6), FN8
3	Report of the Interception of Communications Commissioner March 2015 (excerpts)	8	4 (§7), FN9
4	*Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes* (819/14/EN WP 215)	16	6 (§13), FN13
5	NGO Interveners' Table of comparison of national decisions concerning *DRI* and data retention legislation	3	7 (§17), FN28
6	Council of Europe Commissioner for Human Rights, "*The rule of law on the internet and in the wider digital world*" report (8 December 2014) (excerpts)	3	9 (§21), FN29
7	Report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson QC, UN doc. (A/69/397) (excerpts)	3	10 (§24), FN33

IN THE COURT OF JUSTICE OF THE EUROPEAN UNION
CASE C-698/15

ON A REFERENCE FROM
THE COURT OF APPEAL OF ENGLAND & WALES (CIVIL DIVISION)

Neutral citation: [2015] EWCA Civ 1185

B E T W E E N:

SECRETARY OF STATE FOR THE HOME DEPARTMENT

Appellant

v.

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

Respondents

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

Interveners

WRITTEN OBSERVATIONS OF NGO INTERVENERS

ANNEX 1

A/HRC/27/37

Advance Edited Version

Distr.: General
30 June 2014

Original: English

Human Rights Council
Twenty-seventh session
Agenda items 2 and 3
Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General

Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

The right to privacy in the digital age

Report of the Office of the United Nations High Commissioner for Human Rights

Summary

In its resolution 68/167, the General Assembly requested the United Nations High Commissioner for Human Rights to submit a report on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale, to the Human Rights Council at its twenty-seventh session and to the General Assembly at its sixty-ninth session, with views and recommendations, to be considered by Member States. The present report is submitted pursuant to that request. The Office of the High Commissioner will also submit the report to the General Assembly at its sixty-ninth session, pursuant to the request of the Assembly.

Contents

I. Introduction

1. Digital communications technologies, such as the Internet, mobile smartphones and WiFi-enabled devices, have become part of everyday life. By dramatically improving access to information and real-time communication, innovations in communications technology have boosted freedom of expression, facilitated global debate and fostered democratic participation. By amplifying the voices of human rights defenders and providing them with new tools to document and expose abuses, these powerful technologies offer the promise of improved enjoyment of human rights. As contemporary life is played out ever more online, the Internet has become both ubiquitous and increasingly intimate.

2. In the digital era, communications technologies also have enhanced the capacity of Governments, enterprises and individuals to conduct surveillance, interception and data collection. As noted by the Special Rapporteur on the right to freedom of expression and opinion, technological advancements mean that the State's effectiveness in conducting surveillance is no longer limited by scale or duration. Declining costs of technology and data storage have eradicated financial or practical disincentives to conducting surveillance. The State now has a greater capability to conduct simultaneous, invasive, targeted and broad-scale surveillance than ever before.[1] In other words, the technological platforms upon which global political, economic and social life are increasingly reliant are not only vulnerable to mass surveillance, they may actually facilitate it.

3. Deep concerns have been expressed as policies and practices that exploit the vulnerability of digital communications technologies to electronic surveillance and interception in countries across the globe have been exposed. Examples of overt and covert digital surveillance in jurisdictions around the world have proliferated, with governmental mass surveillance emerging as a dangerous habit rather than an exceptional measure. Governments reportedly have threatened to ban the services of telecommunication and wireless equipment companies unless given direct access to communication traffic, tapped fibre-optic cables for surveillance purposes, and required companies systematically to disclose bulk information on customers and employees. Furthermore, some have reportedly made use of surveillance of telecommunications networks to target political opposition members and/or political dissidents. There are reports that authorities in some States routinely record all phone calls and retain them for analysis, while the monitoring by host Governments of communications at global events has been reported. Authorities in one State reportedly require all personal computers sold in the country to be equipped with filtering software that may have other surveillance capabilities. Even non-State groups are now reportedly developing sophisticated digital surveillance capabilities. Mass surveillance technologies are now entering the global market, raising the risk that digital surveillance will escape governmental controls.

4. Concerns have been amplified following revelations in 2013 and 2014 that suggested that, together, the National Security Agency in the United States of America and General Communications Headquarters in the United Kingdom of Great Britain and Northern Ireland have developed technologies allowing access to much global internet traffic, calling records in the United States, individuals' electronic address books and huge volumes of other digital communications content. These technologies have reportedly been deployed through a transnational network comprising strategic intelligence relationships between Governments, regulatory control of private companies and commercial contracts.

[1] A/HRC/23/40, para. 33.

5. Following on the concerns of Member States and other stakeholders at the negative impact of these surveillance practices on human rights, in December 2013 the General Assembly adopted resolution 68/167, without a vote, on the right to privacy in the digital age. In the resolution, which was co-sponsored by 57 Member States, the Assembly affirmed that the rights held by people offline must also be protected online, and called upon all States to respect and protect the right to privacy in digital communication. It further called upon all States to review their procedures, practices and legislation related to communications surveillance, interception and collection of personal data, emphasizing the need for States to ensure the full and effective implementation of their obligations under international human rights law.

6. Also in resolution 68/167, the General Assembly requested the United Nations High Commissioner for Human Rights to submit a report on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale, to the Human Rights Council at its twenty-seventh session and to the General Assembly at its sixty-ninth session, with views and recommendations, to be considered by Member States. The present report is submitted pursuant to that request. As mandated by resolution 68/167, the Office of the High Commissioner (OHCHR) will also submit the report to the Assembly at its sixty-ninth session.

II. Background and methodology

7. Bearing in mind resolution 68/167, OHCHR participated in a number of events and gathered information from a broad range of sources. On 24 February 2014, the High Commissioner delivered a keynote presentation at an expert seminar on "The right to privacy in the digital age", which was co-sponsored by Austria, Brazil, Germany, Liechtenstein, Mexico, Norway and Switzerland, and facilitated by the Geneva Academy on International Humanitarian Law and Human Rights.

8. From November 2013 to March 2014, OHCHR engaged the United Nations University in a research project on the application of international human rights law to national regimes overseeing governmental digital surveillance. OHCHR is grateful to the University, and acknowledges its major substantive contribution to the preparation of the present report through the research project.

9. As part of an open consultation, on 27 February 2014, OHCHR addressed a questionnaire to Member States through their Permanent Missions in Geneva and in New York; international and regional organizations; national human rights institutions; non-governmental organizations; and business entities. In its questionnaire, OHCHR invited inputs on the issues as addressed by the General Assembly in its resolution 68/167. A dedicated OHCHR webpage was created in order to make available the questionnaire and all contributions for public consultation, as well as to provide further opportunity for input. Contributions were received from 29 Member States from all regions, five international and/or regional organizations, three national human rights institutions, 16 non-governmental organizations and two private sector initiatives.[2]

10. Many of the contributions referred in detail to existing national legislative frameworks and to other measures taken to ensure respect for and protection of the right to privacy in the digital age, as well as to initiatives to establish and implement procedural safeguards and effective oversight. Some contributions referred to challenges encountered

[2] All contributions are available at www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.

in the implementation of the right to privacy in the digital age, and provided suggestions for initiatives at the international level. They included encouragement to the Human Rights Committee to update its relevant general comments, in particular on article 17 of the International Covenant on Civil and Political Rights; the establishment by the Human Rights Council of a special procedures mandate on the right to privacy; and/or the engagement of existing relevant special procedures mandate holders in joint or individual initiatives to address issues related to the right to privacy in the context of digital surveillance and to provide good-practice guidance.

11. Pursuant to the request made in General Assembly resolution 68/167, the present report offers reflections and recommendations based on an assessment of information available at the time of drafting, drawing also on the wealth of material reflected in the diverse range of contributions received.

III. Issues relating to the right to privacy in the digital age

12. As recalled by the General Assembly in its resolution 68/167, international human rights law provides the universal framework against which any interference in individual privacy rights must be assessed. Article 12 of the Universal Declaration of Human Rights provides that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." The International Covenant on Civil and Political Rights, to date ratified by 167 States, provides in article 17 that "no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation". It further states that "everyone has the right to the protection of the law against such interference or attacks."

13. Other international human rights instruments contain similar provisions. Laws at the regional and national levels also reflect the right of all people to respect for their private and family life, home and correspondence or the right to recognition and respect for their dignity, personal integrity or reputation. In other words, there is universal recognition of the fundamental importance, and enduring relevance, of the right to privacy and of the need to ensure that it is safeguarded, in law and in practice.

14. While the mandate for the present report focused on the right to privacy, it should be underscored that other rights also may be affected by mass surveillance, the interception of digital communications and the collection of personal data. These include the rights to freedom of opinion and expression, and to seek, receive and impart information; to freedom of peaceful assembly and association; and to family life – rights all linked closely with the right to privacy and, increasingly, exercised through digital media. Other rights, such as the right to health, may also be affected by digital surveillance practices, for example where an individual refrains from seeking or communicating sensitive health-related information for fear that his or her anonymity may be compromised. There are credible indications to suggest that digital technologies have been used to gather information that has then led to torture and other ill-treatment. Reports also indicate that metadata derived from electronic surveillance have been analysed to identify the location of targets for lethal drone strikes. Such strikes continue to raise grave concerns over compliance with international human rights law and humanitarian law, and accountability for any violations thereof. The linkages between mass surveillance and these other effects on human rights, while beyond the scope of the present report, merit further consideration.

A. The right to protection against arbitrary or unlawful interference with privacy, family, home or correspondence

15. Several contributions highlighted that, when conducted in compliance with the law, including international human rights law, surveillance of electronic communications data can be a necessary and effective measure for legitimate law enforcement or intelligence purposes. Revelations about digital mass surveillance have, however, raised questions around the extent to which such measures are consistent with international legal standards and whether stronger surveillance safeguards are needed to protect against violations of human rights. Specifically, surveillance measures must not arbitrarily or unlawfully interfere with an individual's privacy, family, home or correspondence; Governments must take specific measures to ensure protection of the law against such interference.

16. A review of the various contributions received revealed that addressing these questions requires an assessment of what constitutes interference with privacy in the context of digital communications; of the meaning of "arbitrary and unlawful"; and of whose rights are protected under international human rights law, and where. The sections below address issues that were highlighted in various contributions.

1. Interference with privacy

17. International and regional human rights treaty bodies, courts, commissions and independent experts have all provided relevant guidance with regard to the scope and content of the right to privacy, including the meaning of "interference" with an individual's privacy. In its general comment No. 16, the Human Rights Committee underlined that compliance with article 17 of the International Covenant on Civil and Political Rights required that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. "Correspondence should be delivered to the addressee without interception and without being opened or otherwise read".[3]

18. It has been suggested by some that the conveyance and exchange of personal information via electronic means is part of a conscious compromise through which individuals voluntarily surrender information about themselves and their relationships in return for digital access to goods, services and information. Serious questions arise, however, about the extent to which consumers are truly aware of what data they are sharing, how and with whom, and to what use they will be put. According to one report, "a reality of big data is that once data is collected, it can be very difficult to keep anonymous. While there are promising research efforts underway to obscure personally identifiable information within large data sets, far more advanced efforts are presently in use to re-identify seemingly 'anonymous' data. Collective investment in the capability to fuse data is many times greater than investment in technologies that will enhance privacy." Furthermore, the authors of the report noted that "focusing on controlling the collection and retention of personal data, while important, may no longer be sufficient to protect personal privacy", in part because "big data enables new, non-obvious, unexpectedly powerful uses of data".[4]

19. In a similar vein, it has been suggested that the interception or collection of data about a communication, as opposed to the content of the communication, does not on its

[3] *Official Records of the General Assembly, Forty-third Session, Supplement No. 40* (A/43/40), annex VI, para. 8.

[4] Executive Office of the President of the United States, "Big Data: Seizing Opportunities, Preserving Values", May 2014 (available from www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf), p. 54.

own constitute an interference with privacy. From the perspective of the right to privacy, this distinction is not persuasive. The aggregation of information commonly referred to as "metadata" may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication. As the European Union Court of Justice recently observed, communications metadata "taken as a whole may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained."[5] Recognition of this evolution has prompted initiatives to reform existing policies and practices to ensure stronger protection of privacy.

20. It follows that any capture of communications data is potentially an interference with privacy and, further, that the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used. Even the mere possibility of communications information being captured creates an interference with privacy,[6] with a potential chilling effect on rights, including those to free expression and association. The very existence of a mass surveillance programme thus creates an interference with privacy. The onus would be on the State to demonstrate that such interference is neither arbitrary nor unlawful.

2. What is "arbitrary" or "unlawful"?

21. Interference with an individual's right to privacy is only permissible under international human rights law if it is neither arbitrary nor unlawful. In its general comment No. 16, the Human Rights Committee explained that the term "unlawful" implied that no interference could take place "except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant".[7] In other words, interference that is permissible under national law may nonetheless be "unlawful" if that national law is in conflict with the provisions of the International Covenant on Civil and Political Rights. The expression "arbitrary interference" can also extend to interference provided for under the law. The introduction of this concept, the Committee explained, "is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances".[8] The Committee interpreted the concept of reasonableness to indicate that "any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case".[9]

22. Unlike certain other provisions of the Covenant, article 17 does not include an explicit limitations clause. Guidance on the meaning of the qualifying words "arbitrary or unlawful" nonetheless can be drawn from the Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights;[10] the practice of the Human Rights Committee as reflected in its general comments, including

---

[5] Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Judgment of 8 April 2014, paras. 26-27, and 37. See also Executive Office of the President, "Big Data and Privacy: A Technological Perspective" (available from www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf), p. 19.

[6] See European Court of Human Rights, Weber and Saravia, para. 78; Malone v. UK, para. 64.

[7] *Official Records of the General Assembly* (see footnote 3), para. 3.

[8] Ibid., para. 4.

[9] Communication No. 488/1992, Toonan v Australia, para. 8.3; see also communications Nos. 903/1999, para 7.3, and 1482/2006, paras. 10.1 and 10.2.

[10] See E/CN.4/1985/4, annex.

Nos. 16, 27, 29, 34, and 31, findings on individual communications[11] and concluding observations;[12] regional and national case law;[13] and the views of independent experts.[14] In its general comment No. 31 on the nature of the general legal obligation on States parties to the Covenant, for example, the Human Rights Committee provides that States parties must refrain from violation of the rights recognized by the Covenant, and that "any restrictions on any of [those] rights must be permissible under the relevant provisions of the Covenant. Where such restrictions are made, States must demonstrate their necessity and only take such measures as are proportionate to the pursuance of legitimate aims in order to ensure continuous and effective protection of Covenant rights."[15] The Committee further underscored that "in no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right."

23. These authoritative sources point to the overarching principles of legality, necessity and proportionality, the importance of which also was highlighted in many of the contributions received. To begin with, any limitation to privacy rights reflected in article 17 must be provided for by law, and the law must be sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances. The limitation must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available.[16] Moreover, the limitation placed on the right (an interference with privacy, for example, for the purposes of protecting national security or the right to life of others) must be shown to have some chance of achieving that goal. The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim. Furthermore, any limitation to the right to privacy must not render the essence of the right meaningless and must be consistent with other human rights, including the prohibition of discrimination. Where the limitation does not meet these criteria, the limitation would be unlawful and/or the interference with the right to privacy would be arbitrary.

24. Governments frequently justify digital communications surveillance programmes on the grounds of national security, including the risks posed by terrorism. Several contributions suggested that since digital communications technologies can be, and have been, used by individuals for criminal objectives (including recruitment for and the financing and commission of terrorist acts), the lawful, targeted surveillance of digital communication may constitute a necessary and effective measure for intelligence and/or law enforcement entities when conducted in compliance with international and domestic law. Surveillance on the grounds of national security or for the prevention of terrorism or other crime may be a "legitimate aim" for purposes of an assessment from the viewpoint of article 17 of the Covenant. The degree of interference must, however, be assessed against the necessity of the measure to achieve that aim and the actual benefit it yields towards such a purpose.

25. In assessing the necessity of a measure, the Human Rights Committee, in its general comment No. 27, on article 12 of the International Covenant on Civil and Political Rights, stressed that that "the restrictions must not impair the essence of the right [...]; the relation

[11] For example, communication No. 903/1999, 2004, Van Hulst v. The Netherlands.

[12] CCPR /C/USA/CO/4.

[13] For example, European Court of Human Rights, Uzun v. Germany, 2 September 2010, and Weber and Soravia v. Germany, para. 4; and Inter-American Court of Human Rights, Escher v. Brazil, Judgment, 20 Nov. 2009.

[14] See A/HRC/13/37 and A/HRC/23/40. See also International Principles on the Application of Human Rights to Communications Surveillance, available at https://en.necessaryandproportionate.org/text.

[15] CCPR/C/21/Rev.1/Add. 13, para. 6.

[16] CCPR/C/21/Rev.1/Add.9, paras. 11 – 16. See also A/HRC/14/46, annex, practice 20.

between right and restriction, between norm and exception, must not be reversed."[17] The Committee further explained that "it is not sufficient that the restrictions serve the permissible purposes; they must also be necessary to protect them." Moreover, such measures must be proportionate: "the least intrusive instrument amongst those which might achieve the desired result".[18] Where there is a legitimate aim and appropriate safeguards are in place, a State might be allowed to engage in quite intrusive surveillance; however, the onus is on the Government to demonstrate that interference is both necessary and proportionate to the specific risk being addressed. Mass or "bulk" surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime. In other words, it will not be enough that the measures are targeted to find certain needles in a 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.

26. Concerns about whether access to and use of data are tailored to specific legitimate aims also raise questions about the increasing reliance of Governments on private sector actors to retain data "just in case" it is needed for government purposes. Mandatory third-party data retention – a recurring feature of surveillance regimes in many States, where Governments require telephone companies and Internet service providers to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access – appears neither necessary nor proportionate.[19]

27. One factor that must be considered in determining proportionality is what is done with bulk data and who may have access to them once collected. Many national frameworks lack "use limitations", instead allowing the collection of data for one legitimate aim, but subsequent use for others. The absence of effective use limitations has been exacerbated since 11 September 2001, with the line between criminal justice and protection of national security blurring significantly. The resulting sharing of data between law enforcement agencies, intelligence bodies and other State organs risks violating article 17 of the Covenant, because surveillance measures that may be necessary and proportionate for one legitimate aim may not be so for the purposes of another. A review of national practice in government access to third-party data found "when combined with the greater ease with which national security and law enforcement gain access to private-sector data in the first place, the expanding freedom to share that information among agencies and use it for purposes beyond those for which it was collected represents a substantial weakening of traditional data protections."[20] In several States, data-sharing regimes have been struck down by judicial review on such a basis. Others have suggested that such use limitations are a good practice to ensure the effective discharge of a State's obligations under article 17 of the Covenant,[21] with meaningful sanctions for their violation.

---

[17] CCPR/C/21/Rev.1/Add.9, paras. 11 – 16. See also European Court of Human Rights, Handyside v. the United Kingdom, para. 48; and Klass v. Germany, para. 42.

[18] CCPR/C/21/Rev.1/Add.9, paras. 11 – 16.

[19] See opinion of the Advocate-General Cruz Villalón of the Court of Justice of the European Union in joint cases C-293/12 and C-594/12, which suggests that the Directive 2006/24/EU (on the retention of data generated or processed in connection with the provision of electronic communications services) is "as a whole" in violation of the Charter of Fundamental Rights of the European Union because it fails to impose strict limits on such data retention. See also CCPR/C/USA/CO/4, para. 22.

[20] Fred H. Cate, James X. Dempsey and Ira S. Rubinstein, "Systematic government access to private-sector data", *International Data Privacy Law*, vol. 2, No. 4, 2012, p. 198.

[21] See A/HRC/14/46, annex, practice 23.

B. Protection of the law

28. Paragraph 2 of article 17 of the International Covenant on Civil and Political Rights explicitly states that everyone has the right to the protection of the law against unlawful or arbitrary interference with their privacy. This implies that any communications surveillance programme must be conducted on the basis of a publicly accessible law, which in turn must comply with the State's own constitutional regime and international human rights law.[22] "Accessibility" requires not only that the law is published, but that it is sufficiently precise to enable the affected person to regulate his or her conduct, with foresight of the consequences that a given action may entail. The State must ensure that any interference with the right to privacy, family, home or correspondence is authorized by laws that (a) are publicly accessible; (b) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (c) are sufficiently precise, specifying in detail the precise circumstances in which any such interference may be permitted, the procedures for authorizing, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures for the use and storage of the data collected; and (d) provide for effective safeguards against abuse. [23]

29. Consequently, secret rules and secret interpretations – even secret judicial interpretations – of law do not have the necessary qualities of "law".[24] Neither do laws or rules that give the executive authorities, such as security and intelligence services, excessive discretion; the scope and manner of exercise of authoritative discretion granted must be indicated (in the law itself, or in binding, published guidelines) with reasonable clarity. A law that is accessible, but that does not have foreseeable effects, will not be adequate. The secret nature of specific surveillance powers brings with it a greater risk of arbitrary exercise of discretion which, in turn, demands greater precision in the rule governing the exercise of discretion, and additional oversight. Several States also require that the legal framework be established through primary legislation debated in parliament rather than simply subsidiary regulations enacted by the executive – a requirement that helps to ensure that the legal framework is not only accessible to the public concerned after its adoption, but also during its development, in accordance with article 25 of the International Covenant on Civil and Political Rights.[25]

30. The requirement of accessibility is also relevant when assessing the emerging practice of States to outsource surveillance tasks to others. There is credible information to suggest that some Governments systematically have routed data collection and analytical tasks through jurisdictions with weaker safeguards for privacy. Reportedly, some Governments have operated a transnational network of intelligence agencies through interlocking legal loopholes, involving the coordination of surveillance practice to outflank the protections provided by domestic legal regimes. Such practice arguably fails the test of lawfulness because, as some contributions for the present report pointed out, it makes the operation of the surveillance regime unforeseeable for those affected by it. It may undermine the essence of the right protected by article 17 of the International Covenant on Civil and Political Rights, and would therefore be prohibited by article 5 thereof. States have also failed to take effective measures to protect individuals within their jurisdiction

[22] See ibid., annex.

[23] CCPR /C/USA/CO/4, para. 22. See also European Court of Human Rights, Malone v the United Kingdom, No. 8691/79, 2 August 1984, paras. 67 and 68; and Weber and Saravia v Germany, application no. 54934/00, 29 June 2006, in which the Court lists minimum safeguards that should be set out in statute law.

[24] See CCPR /C/USA/CO/4, para. 22.

[25] See also A/HRC/14/46.

against illegal surveillance practices by other States or business entities, in breach of their own human rights obligations.

C. Who is protected, and where?

31. The extraterritorial application of the International Covenant on Civil and Political Rights to digital surveillance was addressed in several of the contributions received. Whereas it is clear that certain aspects of the recently revealed surveillance programmes, for instance, will trigger the territorial obligations of States conducting surveillance, additional concerns have been expressed in relation to extraterritorial surveillance and the interception of communications.

32. Article 2 of the International Covenant on Civil and Political Rights requires each State party to respect and ensure to all persons within its territory and subject to its jurisdiction the rights recognized in the Covenant without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. The Human Rights Committee, in its general comment No. 31, affirmed that States parties are required by article 2, paragraph 1, to respect and to ensure the Covenant rights to all persons who may be within their territory and to all persons subject to their jurisdiction. This means that a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party."[26] This extends to persons within their "authority".[27]

33. The Human Rights Committee has been guided by the principle, as expressed even in its earliest jurisprudence, that a State may not avoid its international human rights obligations by taking action outside its territory that it would be prohibited from taking "at home".[28] This position is consonant with the views of the International Court of Justice, which has affirmed that the International Covenant on Civil and Political Rights is applicable in respect of acts done by a State "in the exercise of its jurisdiction outside its own territory",[29] as well as articles 31 and 32 of the Vienna Convention on the Law of Treaties. The notions of "power" and "effective control" are indicators of whether a State is exercising "jurisdiction" or governmental powers, the abuse of which human rights protections are intended to constrain. A State cannot avoid its human rights responsibilities simply by refraining from bringing those powers within the bounds of law. To conclude otherwise would not only undermine the universality and essence of the rights protected by international human rights law, but may also create structural incentives for States to outsource surveillance to each other.

34. It follows that digital surveillance therefore may engage a State's human rights obligations if that surveillance involves the State's exercise of power or effective control in

---

[26] CCPR/C/21/Rev.1/Add.13, para. 10.

[27] See *Official Records of the General Assembly, Thirty-sixth Session, Supplement No. 40* (A/36/40), annex XIX, para. 12.2; see also annex XX. See also CCPR/CO/78/ISR, para. 11; CCPR/CO/72/NET, para. 8; CCPR/CO/81/BEL, para. 6; and Inter-American Commission of Human Rights, Coard et al. v. the United States, case No. 10.951, Report No. 109/99, 29 September 1999, paras. 37, 39, 41 and 43.

[28] See *Official Records of the General Assembly, Thirty-sixth Session* (see footnote 27), annex XIX, paras. 12.2-12.3, and annex XX, para. 10.3.

[29] Advisory opinion of the International Court of Justice on the *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, of 9 July 2004 (A/ES-10/273 and Corr.1), paras. 107-111. See also International Court of Justice, case concerning *Armed Activities on the Territory of the Congo* (Democratic Republic of the Congo v. Uganda), judgment, 2005, p. 168.

relation to digital communications infrastructure, wherever found, for example, through direct tapping or penetration of that infrastructure. Equally, where the State exercises regulatory jurisdiction over a third party that physically controls the data, that State also would have obligations under the Covenant. If a country seeks to assert jurisdiction over the data of private companies as a result of the incorporation of those companies in that country, then human rights protections must be extended to those whose privacy is being interfered with, whether in the country of incorporation or beyond. This holds whether or not such an exercise of jurisdiction is lawful in the first place, or in fact violates another State's sovereignty.

35. This conclusion is equally important in the light of ongoing discussions on whether "foreigners" and "citizens" should have equal access to privacy protections within national security surveillance oversight regimes. Several legal regimes distinguish between the obligations owed to nationals or those within a State's territories, and non-nationals and those outside,[30] or otherwise provide foreign or external communications with lower levels of protection. If there is uncertainty around whether data are foreign or domestic, intelligence agencies will often treat the data as foreign (since digital communications regularly pass "off-shore" at some point) and thus allow them to be collected and retained. The result is significantly weaker – or even non-existent – privacy protection for foreigners and non-citizens, as compared with those of citizens.

36. International human rights law is explicit with regard to the principle of non-discrimination. Article 26 of the International Covenant on Civil and Political Rights provides that "all persons are equal before the law and are entitled without any discrimination to the equal protection of the law" and, further, that "in this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status." These provisions are to be read together with articles 17, which provides that "no one shall be subjected to arbitrary interference with his privacy" and that "everyone has the right to the protection of the law against such interference or attacks" , as well as with article 2, paragraph 1. In this regard, the Human Rights Committee has underscored the importance of "measures to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity regardless of the nationality or location of individuals whose communications are under direct surveillance."[31]

D. Procedural safeguards and effective oversight

37. Article 17, paragraph 2 of the International Covenant on Civil and Political Rights states that everyone has the right to the protection of the law against unlawful or arbitrary interference or attacks. The "protection of the law" must be given life through effective procedural safeguards, including effective, adequately resourced institutional arrangements. It is clear, however, that a lack of effective oversight has contributed to a lack of accountability for arbitrary or unlawful intrusions on the right to privacy in the digital environment. Internal safeguards without independent, external monitoring in particular have proven ineffective against unlawful or arbitrary surveillance methods. While these safeguards may take a variety of forms, the involvement of all branches of government in

[30] See for example, in the United States, the Foreign Intelligence Surveillance Act S1881(a); in the United Kingdom, the Regulation of Investigatory Powers Act 2000, s8(4); in New Zealand, the Government Security Bureau Act 2003, s. 15A; in Australia, the Intelligence Services Act S. 9; and in Canada, the National Defence Act, S. 273.64 (1).

[31] CCPR /C/USA/CO/4, para. 22.

the oversight of surveillance programmes, as well as of an independent civilian oversight agency, is essential to ensure the effective protection of the law.

38. Judicial involvement that meets international standards relating to independence, impartiality and transparency can help to make it more likely that the overall statutory regime will meet the minimum standards that international human rights law requires. At the same time, judicial involvement in oversight should not be viewed as a panacea; in several countries, judicial warranting or review of the digital surveillance activities of intelligence and/or law enforcement agencies have amounted effectively to an exercise in rubber-stamping. Attention is therefore turning increasingly towards mixed models of administrative, judicial and parliamentary oversight, a point highlighted in several contributions for the present report. There is particular interest in the creation of "public interest advocacy" positions within surveillance authorization processes. Given the growing role of third parties, such as Internet service providers, consideration may also need to be given to allowing such parties to participate in the authorization of surveillance measures affecting their interests or allowing them to challenge existing measures. The utility of independent advice, monitoring and/or review to help to ensure strict scrutiny of measures imposed under a statutory surveillance regime has been highlighted positively in relevant jurisprudence. Parliamentary committees also can play an important role; however, they may also lack the independence, resources or willingness to discover abuse, and may be subject to regulatory capture. Jurisprudence at the regional level has emphasized the utility of an entirely independent oversight body, particularly to monitor the execution of approved surveillance measures.[32] In 2009, the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism suggested, therefore, that "there must be no secret surveillance system that is not under review of an independent oversight body and all interferences must be authorized through an independent body."[33]

E. Right to an effective remedy

39. The International Covenant on Civil and Political Rights requires States parties to ensure that victims of violations of the Covenant have an effective remedy. Article 2, paragraph 3 (b) further specifies that States parties to the Covenant undertake "to ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy". States must also ensure that the competent authorities enforce such remedies when granted. As the Human Rights Committee emphasized in its general comment No. 31, failure by a State party to investigate allegations of violations could in and of itself give rise to a separate breach of the Covenant.[34] Moreover, cessation of an ongoing violation is an essential element of the right to an effective remedy.

40. Effective remedies for violations of privacy through digital surveillance can thus come in a variety of judicial, legislative or administrative forms. Effective remedies typically share certain characteristics. First, those remedies must be known and accessible to anyone with an arguable claim that their rights have been violated. Notice (that either a general surveillance regime or specific surveillance measures are in place) and standing (to

[32] See for example European Court of Human Rights, Ekimdzhiev v Bulgaria, application No. 62540/00, 28 June 2007.

[33] A/HRC/13/37, para. 62.

[34] CCPR/C/21/Rev.1/Add. 13, para. 15.

challenge such measures) thus become critical issues in determining access to effective remedy. States take different approaches to notification: while some require post facto notification of surveillance targets, once investigations have concluded, many regimes do not provide for notification. Some may also formally require such notification in criminal cases; however, in practice, this stricture appears to be regularly ignored. There are also variable approaches at national level to the issue of an individual's standing to bring a judicial challenge. The European Court of Human Rights ruled that, while the existence of a surveillance regime might interfere with privacy, a claim that this created a rights violation was justiciable only where there was a "reasonable likelihood" that a person had actually been subjected to unlawful surveillance.[35]

41. Second, effective remedies will involve prompt, thorough and impartial investigation of alleged violations. This may be provided through the provision of an "independent oversight body [...] governed by sufficient due process guarantees and judicial oversight, within the limitations permissible in a democratic society."[36] Third, for remedies to be effective, they must be capable of ending ongoing violations, for example, through ordering deletion of data or other reparation.[37] Such remedial bodies must have "full and unhindered access to all relevant information, the necessary resources and expertise to conduct investigations, and the capacity to issue binding orders".[38] Fourth, where human rights violations rise to the level of gross violations, non-judicial remedies will not be adequate, as criminal prosecution will be required.[39]

IV. What role for business?

42. There is strong evidence of a growing reliance by Governments on the private sector to conduct and facilitate digital surveillance. On every continent, Governments have used both formal legal mechanisms and covert methods to gain access to content, as well as to metadata. This process is increasingly formalized: as telecommunications service provision shifts from the public sector to the private sector, there has been a "delegation of law enforcement and quasi-judicial responsibilities to Internet intermediaries under the guise of 'self-regulation' or 'cooperation'".[40] The enactment of statutory requirements for companies to make their networks "wiretap-ready" is a particular concern, not least because it creates an environment that facilitates sweeping surveillance measures.

---

[35] See Esbester v. the United Kingdom, application No. 18601/91, Commission decision of 2 April 1993; Redgrave v. the United Kingdom, application No. 202711/92, Commission decision of 1 September 1993; and Matthews v. the United Kingdom, application No. 28576/95, Commission decision of 16 October 1996.

[36] "Joint declaration on surveillance programs and their impact on freedom of expression", issued by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, June 2013 (available from www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1), para. 9.

[37] See for example European Court of Human Rights, Segersted-Wiber and others v. Sweden, application No. 62332/00, 6 June 2006. See also CCPR/C/21/Rev.1/Add. 13, paras. 15-17.

[38] A/HRC/14/46.

[39] Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law (General Assembly resolution 60/147, annex).

[40] See European Digital Rights, "The Slide from 'Self-Regulation' to Corporate Censorship", Brussels, January 2011, available at www.edri.org/files/EDRI_selfreg_final_20110124.pdf.

43. There may be legitimate reasons for a State to require that an information and communications technology company provide user data; however, when a company supplies data or user information to a State in response to a request that contravenes the right to privacy under international law, a company provides mass surveillance technology or equipment to States without adequate safeguards in place or where the information is otherwise used in violation of human rights, that company risks being complicit in or otherwise involved with human rights abuses. The Guiding Principles on Business and Human Rights, endorsed by the Human Rights Council in 2011, provide a global standard for preventing and addressing adverse effects on human rights linked to business activity. The responsibility to respect human rights applies throughout a company's global operations regardless of where its users are located, and exists independently of whether the State meets its own human rights obligations.

44. Important multi-stakeholder efforts have been made to clarify the application of the Guiding Principles in the communications and information technology sector. Enterprises that provide content or Internet services, or supply the technology and equipment that make digital communications possible, for example, should adopt an explicit policy statement outlining their commitment to respect human rights throughout the company's activities. They should also have in place appropriate due diligence policies to identify, assess, prevent and mitigate any adverse impact. Companies should assess whether and how their terms of service, or their policies for gathering and sharing customer data, may result in an adverse impact on the human rights of their users.

45. Where enterprises are faced with government demands for access to data that do not comply with international human rights standards, they are expected to seek to honour the principles of human rights to the greatest extent possible, and to be able to demonstrate their ongoing efforts to do so. This can mean interpreting government demands as narrowly as possible, seeking clarification from a Government with regard to the scope and legal foundation for the demand, requiring a court order before meeting government requests for data, and communicating transparently with users about risks and compliance with government demands. There are positive examples of industry action in this regard, both by individual enterprises and through multi-stakeholder initiatives.

46. A central part of human rights due diligence as defined by the Guiding Principles is meaningful consultation with affected stakeholders. In the context of information and communications technology companies, this also includes ensuring that users have meaningful transparency about how their data are being gathered, stored, used and potentially shared with others, so that they are able to raise concerns and make informed decisions. The Guiding Principles clarify that, where enterprises identify that they have caused or contributed to an adverse human rights impact, they have a responsibility to ensure remediation by providing remedy directly or cooperating with legitimate remedy processes. To enable remediation at the earliest possible stage, enterprises should establish operational-level grievance mechanisms. Such mechanisms may be particularly important in operating countries where rights are not adequately protected or where access to judicial and non-judicial remedies is lacking. In addition to such elements as compensation and restitution, remedy should include information about which data have been shared with State authorities, and how.

V. Conclusions and recommendations

47. **International human rights law provides a clear and universal framework for the promotion and protection of the right to privacy, including in the context of domestic and extraterritorial surveillance, the interception of digital communications and the collection of personal data. Practices in many States have, however, revealed a**

lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight, all of which have contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy.

48. In addressing the significant gaps in implementation of the right to privacy, two observations are warranted. The first is that information relating to domestic and extraterritorial surveillance policies and practices continues to emerge. Inquiries are ongoing with a view to gather information on electronic surveillance and the collection and storage of personal data, as well as to assess its impact on human rights. Courts at the national and regional levels are engaged in examining the legality of electronic surveillance policies and measures. Any assessment of surveillance policies and practices against international human rights law must necessarily be tempered against the evolving nature of the issue. A second and related observation concerns the disturbing lack of governmental transparency associated with surveillance policies, laws and practices, which hinders any effort to assess their coherence with international human rights law and to ensure accountability.

49. Effectively addressing the challenges related to the right to privacy in the context of modern communications technology will require an ongoing, concerted multi-stakeholder engagement. This process should include a dialogue involving all interested stakeholders, including Member States, civil society, scientific and technical communities, the business sector, academics and human rights experts. As communication technologies continue to evolve, leadership will be critical to ensuring that these technologies are used to deliver on their potential towards the improved enjoyment of the human rights enshrined in the international legal framework.

50. Bearing the above observations in mind, there is a clear and pressing need for vigilance in ensuring the compliance of any surveillance policy or practice with international human rights law, including the right to privacy, through the development of effective safeguards against abuses. As an immediate measure, States should review their own national laws, policies and practices to ensure full conformity with international human rights law. Where there are shortcomings, States should take steps to address them, including through the adoption of a clear, precise, accessible, comprehensive and non-discriminatory legislative framework. Steps should be taken to ensure that effective and independent oversight regimes and practices are in place, with attention to the right of victims to an effective remedy.

51. There are a number of important practical challenges to the promotion and protection of the right to privacy in the digital age. Building upon the initial exploration of some of these issues in the present report, there is a need for further discussion and in-depth study of issues relating to the effective protection of the law, procedural safeguards, effective oversight, and remedies. An in-depth analysis of these issues would help to provide further practical guidance, grounded in international human rights law, on the principles of necessity, proportionality and legitimacy in relation to surveillance practices; on measures for effective, independent and impartial oversight; and on remedial measures. Further analysis also would assist business entities in meeting their responsibility to respect human rights, including due diligence and risk management safeguards, as well as on their role in providing effective remedies.

IN THE COURT OF JUSTICE OF THE EUROPEAN UNION
CASE C-698/15

ON A REFERENCE FROM
THE COURT OF APPEAL OF ENGLAND & WALES (CIVIL DIVISION)

Neutral citation: [2015] EWCA Civ 1185

B E T W E E N:

SECRETARY OF STATE FOR THE HOME DEPARTMENT

Appellant

v.

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

Respondents

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

Interveners

WRITTEN OBSERVATIONS OF NGO INTERVENERS

ANNEX 2

Data Retention and Investigatory Powers Bill

Top Lines

- Communications data (CD) is the context, but not the content of a communication: who was communicating, when, how, from where, and with whom.
- Law enforcement and the intelligence and security agencies use this data to investigate crimes, bring offenders to justice and to save lives.
- On 8 April 2014, the European Court of Justice (ECJ) declared the EU Data Retention Directive (DRD) invalid. We must ensure that communications service providers (CSPs) continue to retain communications data in the future. If they do not, it will not be available to the police when they need it for an investigation.
- This legislation will ensure a clear basis in domestic law for the retention of communications data in the UK. It will, in practice, maintain the status quo, while also responding to the ECJ judgment.
- This Bill does not replicate the proposals from the Draft Communications Data Bill, published in 2012.
- The Bill is compatible with the ECHR and will contain the normal statement to this effect from the Home Secretary.

For information relating to other investigatory powers please see the separate factsheet.

What is Communications Data?

- Communications data is the who, when, where and how of a communication, but not its content.
- The police use it to prove or disprove alibis, identify associations between suspects, and tie an individual to a particular location or crime scene.
- Communications data has played a significant role in every Security Service counter terrorism operation over the last decade.
- It is regularly used in court: notably, in 95% of serious and organised crime investigations handled by the CPS.
- It has also played a significant role in the investigation of a very large number of serious and widely reported crimes, including the Oxford and Rochdale child grooming cases, murder of Holly Wells and Jessica Chapman, and 2007 Glasgow Airport terror attack.
- Communications data will often be the only investigative lead. If this data is not retained, these cases will go unsolved.

Why do we need to legislate?

- Communications data is held by companies for their own business purposes (usually three months) and where mandated to do so in law.
- It can then be accessed by the police under the Regulation of Investigatory Powers Act 2000 (RIPA), where it is necessary and proportionate to do so for a specific investigation, subject to stringent safeguards.
- On 8 April, the ECJ declared the EU Data Retention Directive (DRD) invalid. Although the UK's own Data Retention Regulations remain in force, we need a clear legal basis for mandatory data retention in UK law.
- Otherwise, companies may soon start deleting data that is essential for law enforcement and national security.
- This 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.
- It will also make changes to the regime to respond to elements of the ECJ judgment.

What do law enforcement need?

- Senior officers are clear that, without the data currently being retained under law, crucial investigations will become impossible. The data types in question are listed in a Schedule to the draft regulations published alongside the Bill.
- These are identical to the existing Regulations and include items like names, addresses, telephone numbers, dates and times of messages, device (i.e. phone or computer) identifiers and cell location information.

What about the Draft Communications Data Bill?

- This Bill does not replicate the proposals from the Draft Communications Data Bill.
- There remains a pressing need to update legislation to ensure that data for new types of internet communication are available in the future, as data for telephony has been in the past. The Joint Committee on the Draft Communications Data Bill accepted this requirement, subject to the appropriate safeguards.
- The Prime Minister has been clear that we will need to return to these issues in the next Parliament.

"Communications data is still overwhelmingly the most powerful tool available to those investigating child sexual exploitation and identifying and safeguarding its victims and potential victims."
Keith Bristow, Director General, National Crime Agency

"It is regularly used to tackle criminals whose activities affect the wider community, such as repeat burglars, robbers and drugs dealers. Put simply, the police need access to this information to keep up with the criminals who bring so much harm to victims and our society."
Sir Bernard Hogan-Howe, Commissioner, Metropolitan Police

"For cases such as counter-terrorism, organised crime and large-scale fraud, I would go as far to say that communications data is so important that any reduction in capability would create a real risk to future prosecutions."
Sir Keir Starmer, (former) Director of Public Prosecutions

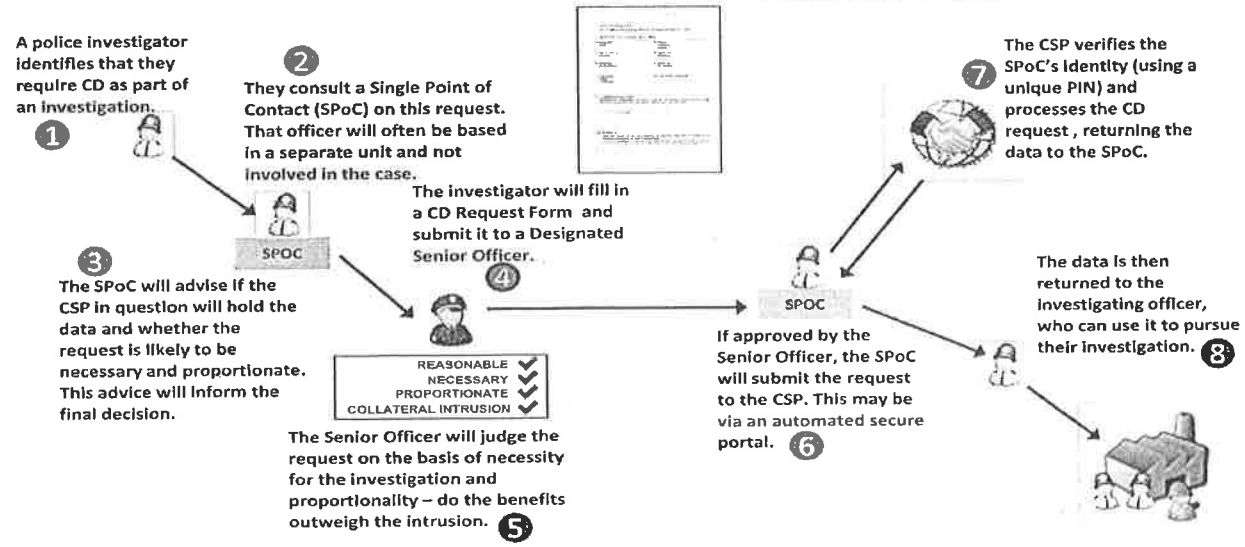
Data Retention and Investigatory Powers Bill

How are we responding to the ECJ judgment?

- The ECJ struck down the European Data Retention Directive, not our own laws. The judgment upheld the principle that data could be retained at the request of government, but found that the Directive itself lacked proper safeguards.
- It did not consider the robust safeguards that already exist in the UK's communications data regime. We believe that our internationally-respected retention and access regime already addresses most of the ECJ's criticisms.
- The Bill is compatible with the ECHR and will contain the normal statement to this effect from the Home Secretary.
- However, in order to respond to elements of the judgment and to ensure the Bill is compliant with ECHR, we are extending the existing safeguards in a number of ways. Many of these changes are set out in the regulations that accompany the Bill rather than on the face of the Bill itself:
  - Ministers will need to consider necessity and proportionality before issuing retention notices, as well as the impact of the notice on the provider.
  - There will be a maximum, rather than absolute, retention period of 12 months – data may be retained for less if it is not necessary or proportionate to keep it for longer.
  - There will be a clear requirement for the Secretary of State to keep notices under review.
  - Data retention notices will, as at present, be limited to a strict list of data types. This will be identical to the existing list in the 2009 Data Retention Regulations.
  - The content of the new notices will be far more specific e.g. setting out the data categories and services this retention applies to.
  - Access to data retained under this Bill will be limited to requests under RIPA and court orders.
  - Data security requirements will be set out in notices requiring a CSP to retain data, and will be enforceable.
  - The Information Commissioner's duties will be clarified, so that he oversees all relevant aspects of data retention.
  - We will create a Code of Practice on Data Retention, putting best-practice guidance on a statutory footing.
  - We will amend the data acquisition Code of Practice, ensuring (i) where there may be concerns relating to professions that handle privileged information (e.g. lawyers or journalists), law enforcement should give additional consideration of the level of intrusion; and (ii) making it clearer that the officer authorising access to data should be independent of the investigation.

What safeguards control access to communications data?

- RIPA provides for an ECHR-compliant regime governing the access to communications data. Specifically:
  - Data may only be acquired by public bodies that have been approved by Parliament to do so, and for specific statutory purposes (prevention/detection crime, national security, preventing death or injury etc.).
  - Data is obtained on a case by case basis and must be authorised by a senior officer (who is independent from the investigation) at a rank stipulated by Parliament. That authorising officer may only authorise a request for communications data if the tests of necessity and proportionality are met.
  - The full authorisations process is shown in the **diagram below**. The Joint Committee on the Draft CD Bill concluded that this was the '*right model*'.
  - Local authorities' requests for communications data must also be approved by a magistrate.
  - The Interception of Communications Commissioner provides independent oversight of the acquisition of communications data by public authorities. He conducts robust inspections and publishes an annual report.
  - The Information Commissioner oversees the processing and security of personal information held by CSPs, including communications data.



IN THE COURT OF JUSTICE OF THE EUROPEAN UNION
CASE C-698/15

ON A REFERENCE FROM
THE COURT OF APPEAL OF ENGLAND & WALES (CIVIL DIVISION)

Neutral citation: [2015] EWCA Civ 1185

B E T W E E N:

SECRETARY OF STATE FOR THE HOME DEPARTMENT

Appellant

v.

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

Respondents

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

Interveners

WRITTEN OBSERVATIONS OF NGO INTERVENERS

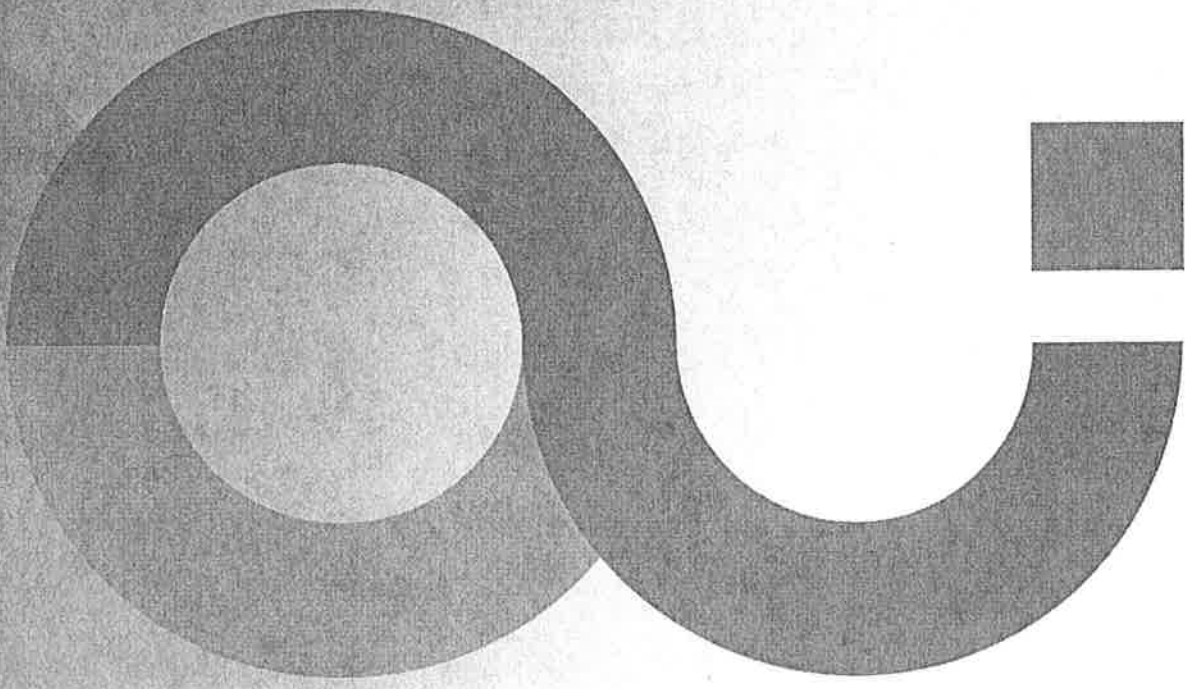
ANNEX 3

Report of the Interception of Communications Commissioner

March 2015

(covering the period January to December 2014)

**The Rt Hon.
Sir Anthony May**



Report of the Interception of Communications Commissioner

March 2015

(covering the period January to December 2014)

Presented to Parliament pursuant to Section 58(6) of the Regulation of Investigatory Powers Act 2000

Ordered by the House of Commons to be printed on 12th March 2015

Laid before the Scottish Parliament by the Scottish Ministers 12th March 2015

HC 1113

SG/2015/28

INTERCEPTION OF COMMUNICATIONS COMMISSIONER'S OFFICE

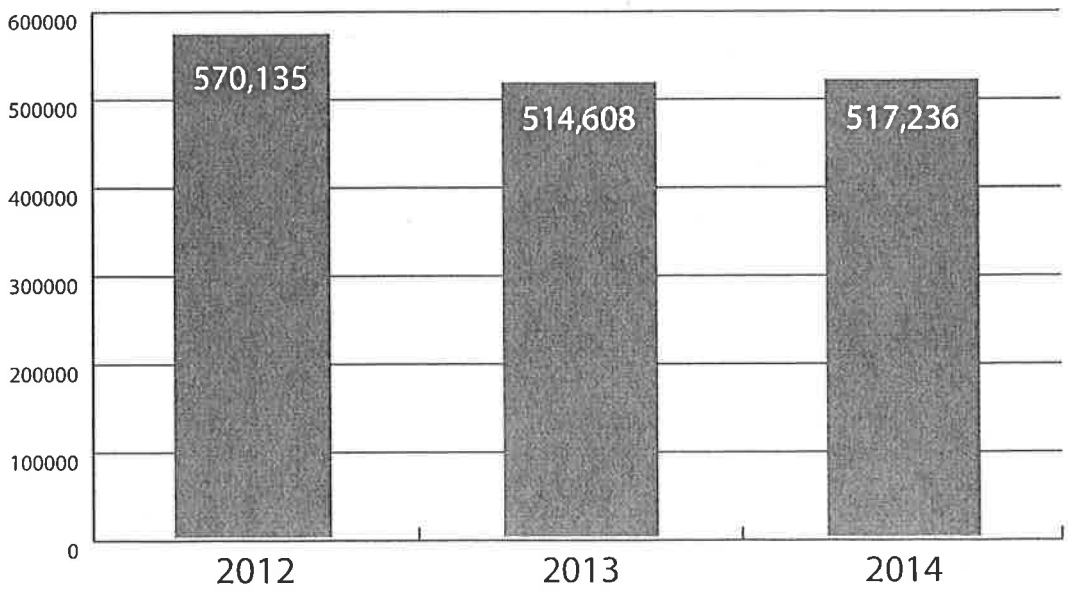
be obtained by other less intrusive means. Applications for communications data are refused (or not applied for) where it is judged that the necessity does not outweigh the intrusion. For example, an application is more likely to be granted for a mobile telephone which a suspect is known to use for criminal purposes than if the telephone may also be used by other members of the individual's family as well. In such cases the acquisition of unconnected and intrusive data might be unavoidable. Judging the likely intrusion in advance is not an exact science.

Statistics for Communications Data

7.20 My office has previously referred to the inadequacy of the statistical requirements in the Acquisition and Disclosure of Communications Data code of practice. The Home Office recently included a more comprehensive set of statistical requirements in the amended draft code of practice[32]. These new requirements will improve transparency and provide for more meaningful analysis. Public authorities are currently working to ensure their recording systems are amended to fulfil the new statistical requirements from April 1st 2015, including the ability to capture information not previously recorded.

7.21 Figure 5 shows the number of authorisations and notices for communications data over the previous three years (excluding urgent oral applications). The total number

Figure 5 *2012-2014 Total Authorisations & Notices under Chapter II of Part I RIPA 2000 (ex urgent oral applications)*



32 https://www.gov.uk/government/publications/communications-data-draft-codes-of-practice-acquisition-disclosure-and-retention

issued or granted in 2014 was 517,236 which although higher than the previous year, does not represent a significant increase.

7.22 The urgent oral process is used to acquire communications data where there is no time to complete the normal written process. For example, in circumstances where there is an immediate threat to life, an urgent operational requirement relating to serious crime or a credible threat to national security. In 2014 there were 55,346 notices and authorisations given orally. This represents an increase on the 42,293 notices and authorisations given orally in 2013. Our inspections have identified that much of this increase is due to the police providing an enhanced emergency response to trace missing children at risk of sexual exploitation. I note that the draft code of practice has clarified that the section 22(2)(g) statutory purpose[33] may be used in circumstances where there is serious concern for the welfare of a vulnerable person.

7.23 Annex B of this report provides a breakdown of the 517,236 notices and authorisations by public authority. The number of notices given and authorisations granted by public authorities is only indicative of the amount of communications data acquired and must be treated with caution for the reasons I outlined in paragraph 4.19 of my 2013 Annual Report. Essentially it would be inappropriate to draw comparisons between the public authorities as they apply different counting mechanisms and rules. It is important therefore that the numbers are not used to produce league table comparisons.

7.24 The new statistical requirements in the amended draft code of practice will require public authorities to record the number of applications for communications data and the individual items of data requested. The latter of which should be a more meaningful figure than the number of authorisations and notices. It is also likely to be higher. In November 2014 my office published a diagram to assist understanding as to the relationship and ratio between the number of notices & authorisations and applications[34]. Our estimate at that time was that the ratio was an average of 2.5:1 notices & authorisations to applications.

7.25 This year I used my power under section 58(1) of RIPA 2000 to require public authorities to collate the number of applications for communications data that were approved. Previously my office had only been able to estimate this statistic from limited data sets. In total there were 267,373 applications and so the actual ratio of notices & authorisations to applications in 2014 was 2:1.

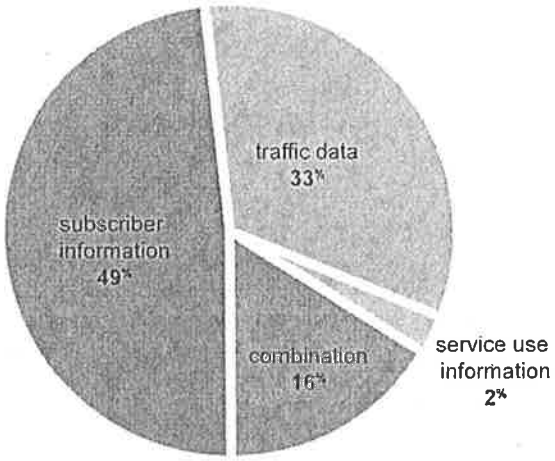
7.26 Figure 6 shows the breakdown of notices and authorisations by type of data under section 21(4). Almost half of the requirements were for subscriber information under section 21(4)(c). The breakdown is much the same as for 2012 and 2013.

7.27 Figure 7 shows the breakdown of the 517,236 notices and authorisations by type of public authority. 88.9% of these were made by police forces and law enforcement

33 RIPA 2000 s.22(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;

34 http://www.iocco-uk.info/docs/Relationship%20between%20applications,%20authorisations,%20notices%20and%20items%20of%20data.pdf

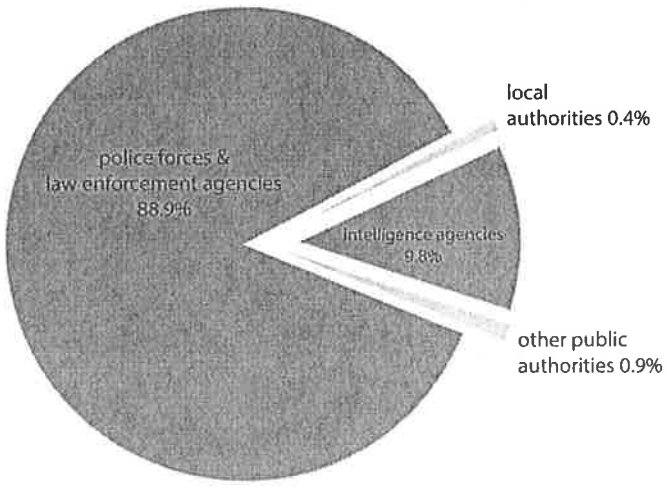
Figure 6 *2014 RIPA 2000 Part I Chapter II Authorisations & Notices by Data Type*



agencies. Less than 2% were made by local authorities and 'other' public authorities. 'Other' public authorities include regulatory bodies with statutory functions to investigate criminal offences and smaller bodies with niche functions. Of particular note is that no Fire & Rescue Authorities or Ambulance Trusts reported using their powers in 2014. Just over a fifth of Local Authorities reported using their powers in 2014.

7.28 Finally, this year my office repeated an exercise conducted for my 2013 Annual Report to provide some further statistical information in relation to the statutory necessity purposes under which data is required in order to better inform the public about how

Figure 7 *Chapter II of Part I RIPA 2000 Authorisations & Notices by Public Authority Type (2014)*



the powers are being used. This statistic is particularly important as there has in the past been legitimate public concern expressed in relation to the allegedly large number of statutory necessity purposes for acquiring communications data. Figure 8 shows that just half a percent of all the requests were for purposes other than the prevention and detection of crime or the prevention of disorder, in the interests of national security, or in an emergency to prevent death or injury. Figure 8 also reiterates the point I have made elsewhere[35] that it is inaccurate and unhelpful to refer to RIPA 2000 as anti-terrorist legislation and infer that its use for non-terrorist related matters is inappropriate.

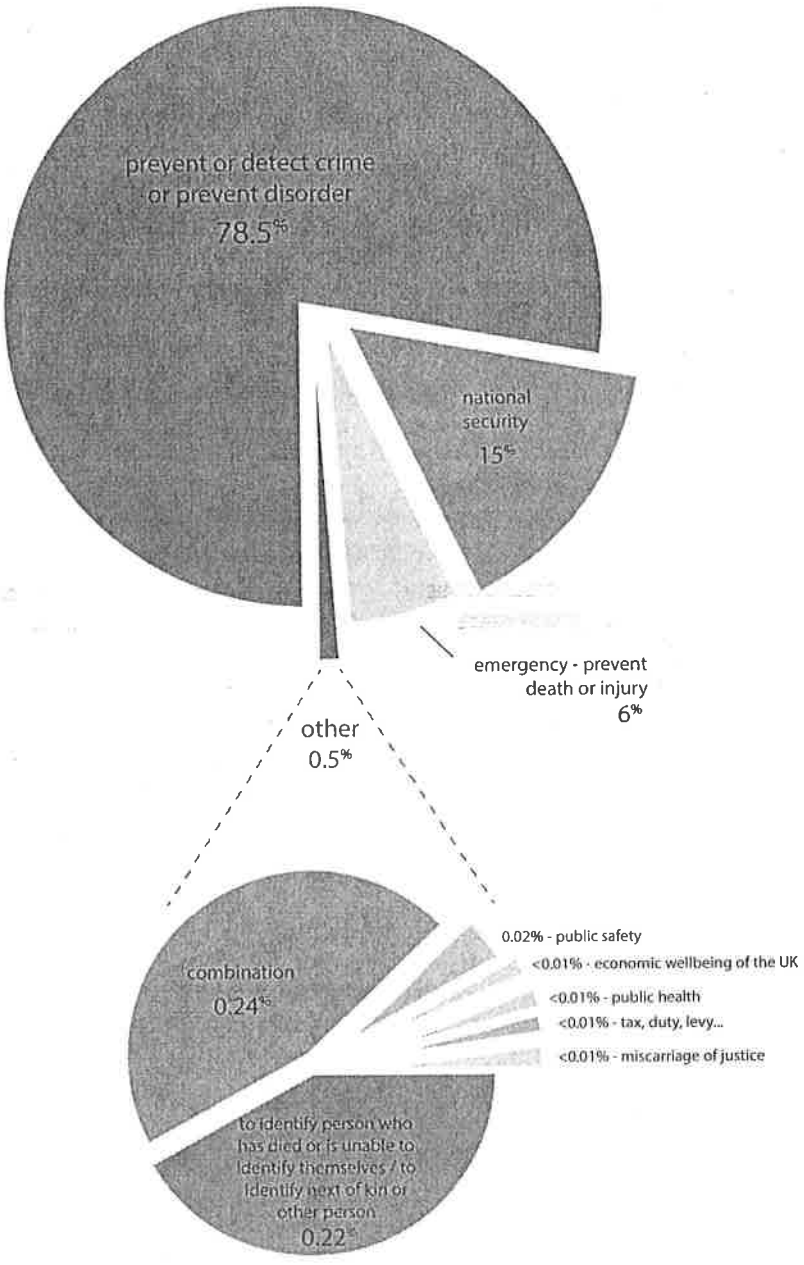
7.29 It is not possible to report the number of individuals to whom the 517,236 notices and authorisations relate. What we can say is that number would be much smaller as public authorities often make multiple requests for communications data in the course of a single investigation, and also make multiple requests for communications data in relation to the same individual. We note that the Home Office has not included a requirement for this statistic to be collected in the revised code of practice.

7.30 Although this would undoubtedly be an informative statistic, in our view there are a number of compelling reasons as to why the collection of this statistic is likely to be prohibitively difficult. For example, one notice or authorisation may include data requirements that relate to different individuals; there is not always a one-to-one relationship between a communications address and an individual; a large number of requests are unsuccessful in conclusively attributing a communications address to an individual; there would be duplicates for a number of reasons, for example, different police forces might be investigating and acquiring data on the same individuals (and even when those individuals had been identified those requests might not be linked). Furthermore the statistics that are currently collected by public authorities are all recorded at the start of the process or at the point of requesting the data. At this point of the process the individual on whom data is being acquired is often unknown, and this might well be the reason why the data is being acquired in the first place (i.e. to identify an unknown individual).

7.31 The best chance therefore of comprehensively attributing communications addresses to individuals would be at the termination of an investigation where various sources of information in addition to communications data could be drawn upon. But even at the end of the investigation there might still be a large degree of ambiguity or a number of communications addresses that have not been attributed successfully because it was not possible to do so or, because it was no longer a relevant line of inquiry to pursue and therefore it was not appropriate for the public authority to identify to whom the particular communications address relates to. Such retrospective recording of information would represent a major shift from the current statistical recording practices and, in our view, would be an onerous administrative burden. My office would also be concerned about the unintended consequence whereby a greater amount of communications data might be sought than was actually necessary in order to satisfy the statistical requirements of linking a communications address to an individual. This year during our operational reviews, which we will discuss later in this section of the report,

35 http://www.iocco-uk.info/docs/IOCCO%20Communications%20Data%20Journalist%20Inquiry%20Report%204Feb15.pdf

Figure 8 *2014 Chapter II of Part I RIPA 2000 Applications by Statutory Purpose*



Caveat: This chart is created to give indicative proportions of which statutory purpose the approved applications in 2014 were for. It is indiciative because a small minority of police forces were unable to provide an accurate breakdown. Their contribution to the total has been extrapolated from the majority of police forces that were able to give an accurate breakdown.

my office collected statistics in relation to whether the data that was acquired related to a suspect, victim, witness or other category of individual, and this more achievable statistic goes some way to better inform the public about how the powers are being used. I note that the Home Office has included this statistical requirement in the revised code of practice.

Inspection Regime

7.32 My office's communications data inspections are structured to ensure that key areas derived from Chapter II of Part I of RIPA 2000 and the code of practice are scrutinised. A typical inspection may include the following:

- the supply of a pre-inspection pack (two months prior to our visit) to the head of the public authority to require information and arrange interviews with operational teams;
- a review of the action points or recommendations from the previous inspection and their implementation;
- an audit of the information supplied by the CSPs detailing the requests that public authorities have made for disclosure of data. This information is compared against the applications held by the SPoC to verify that the necessary approvals were given to acquire the data;
- random examination of individual applications for communications data to assess whether they were necessary in the first instance and then whether the requests met the necessity and proportionality requirements;
- query based examination of applications, via interrogation of the secure auditable computer systems used by the larger public authorities, to identify trends, patterns and compliance issues in key parts of the process across large volumes of applications;
- scrutinising at least one investigation or operation from start to end to assess whether the communications data strategy and the justifications for acquiring all of the data were proportionate;
- examination of the urgent oral approvals to check the process was justified and used appropriately;
- a review of the errors reported or recorded, including checking that the measures put in place to prevent recurrence are sufficient; and,
- the compilation of a detailed inspection report and action plan setting out the findings, recommendations and overall level of compliance. This is sent to the head of the relevant public authority, i.e. the Chief Constable or Chief Executive.

7.33 **Number of inspections.** In 2014 my office conducted 90 communications data inspections broken down as follows: 51 police force and law enforcement agency, 3 intelligence agency, 18 local authority and 18 'other' public authority inspections. In 2014 my office moved to conduct annual inspections of the public authorities that acquire

IN THE COURT OF JUSTICE OF THE EUROPEAN UNION
CASE C-698/15

ON A REFERENCE FROM
THE COURT OF APPEAL OF ENGLAND & WALES (CIVIL DIVISION)

Neutral citation: [2015] EWCA Civ 1185

B E T W E E N:

SECRETARY OF STATE FOR THE HOME DEPARTMENT

Appellant

v.

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

Respondents

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

Interveners

WRITTEN OBSERVATIONS OF NGO INTERVENERS

ANNEX 4

ARTICLE 29 DATA PROTECTION WORKING PARTY

819/14/EN
WP 215

Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes

Adopted on 10 April 2014

Executive Summary

Since the summer of 2013, several international media outlets have reported widely on surveillance activities from intelligence services, both in the United States and in the European Union based on documents primarily provided by Edward Snowden. The revelations have sparked an international debate on the consequences of such large-scale surveillance for citizens' privacy. The way intelligence services make use of data on our day-to-day communications as well as the content of those communications underlines the need to set limits to the scale of surveillance.

The right to privacy and to the protection of personal data is a fundamental right enshrined in the International Covenant on Civil and Political Rights, the European Convention on Human rights and the European Union Charter on Fundamental Rights. It follows that respecting the rule of law necessarily implies that this right is afforded the highest possible level of protection.

From its analysis, the Working Party concludes that secret, massive and indiscriminate surveillance programs are incompatible with our fundamental laws and cannot be justified by the fight against terrorism or other important threats to national security. Restrictions to the fundamental rights of all citizens could only be accepted if the measure is strictly necessary and proportionate in a democratic society.

This is why the Working Party recommends several measures in order for the rule of law to be guaranteed and respected.

First, the Working Party calls for more transparency on how surveillance programmes work. Being transparent contributes to enhancing and restoring trust between citizens and governments and private entities. Such transparency includes better information to individuals when access to data has been given to intelligence services. In order to better inform individuals on the consequences the use of online and offline electronic communication services may have as well as how they can better protect themselves, the Working Party intends to organise a conference on surveillance in the second half of 2014 bringing together all relevant stakeholders.

In addition, the Working Party strongly advocates for more meaningful oversight of surveillance activities. Effective and independent supervision on the intelligence services, including on processing of personal data, is key to ensure that no abuse of these programmes will take place. Therefore, the Working Party considers that an effective and independent supervision of intelligence services implies a genuine involvement of the data protection authorities.

The Working Party further recommends enforcing the existing obligations of EU Member States and of Parties to the ECHR to protect the rights of respect for private life and to protection of one's personal data. Moreover the Working Party recalls that controllers subject to EU jurisdiction shall comply with existing applicable EU data protection legislation. The Working Party furthermore recalls that data protection authorities may suspend data flows and

should decide according to their national competence if sanctions are in order in a specific situation.

Neither Safe Harbor, nor Standard Contractual Clauses, nor BCRs could serve as a legal basis to justify the transfer of personal data to a third country authority for the purpose of massive and indiscriminate surveillance. In fact, the exceptions included in these instruments are limited in scope and should be interpreted restrictively. They should never be implemented to the detriment of the level of protection guaranteed by EU rules and instruments governing transfers.

The Working Party urges the EU institutions to finalise the negotiations on the data protection reform package. It welcomes in particular the proposal of the European Parliament for a new article 43a, providing for mandatory information to individuals when access to data has been given to a public authority in the last twelve months. Being transparent about these practices will greatly enhance trust. .

Furthermore, the Working Party considers that the scope of the national security exemption should be clarified in order to give legal certainty regarding the scope of application of EU law. To date, no clear definition of the concept of national security has been adopted by the European legislator, nor is the case law of the European courts conclusive.

Finally, the Working Party recommends the quick start of negotiations on an international agreement to grant adequate data protection safeguards to individuals when intelligence activities are carried out. The Working Party also supports the development of a global instrument providing for enforceable, high level privacy and data protection principles.

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 19951,

Having regard to Articles 29 and 30(1)(c) and (3) of that Directive,

Having regard to its Rules of Procedure and in particular to Articles 12 and 14 thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. Introduction

Since the summer of 2013, several international media outlets have reported widely on electronic surveillance activities from intelligence services, both in the United States (US), in the European Union (EU), and further across the globe, primarily based on documents provided by Edward Snowden. The revelations have sparked an international debate on the consequences of such large-scale electronic surveillance for citizens' privacy. Also, questions have been raised as to how far intelligence services should be legally allowed to go, both in collection and use of information on our daily lives. This opinion contain the results of the legal analyses of the data protection authorities in the EU, united in the Article 29 Working Party (the Working Party), of the implications of electronic surveillance programmes for the protection of the fundamental right to data protection and privacy.

The main task of data protection authorities is to protect the fundamental right to data protection for all individuals and ensure the relevant provisions in law are respected by data controllers. However, with regard to intelligence services, many data protection authorities have only limited or even no supervisory powers. For their supervision, including on the processing of personal data, other arrangements have been made by the Member States. The Working Party has therefore made an inventarisation of the various arrangements in the EU for supervision over the intelligence services, which is included in this opinion.

This Opinion does not address scenarios related to cable bound interception of personal data. At this stage, the Working Party has insufficient information available about this alleged situation to assess the applicable legal regime, even in a hypothetical manner.

2. Metadata

To assess the scope of the possible infringement of data protection rules, it first needs to be clear what we are dealing with. Government officials refer oftentimes to the collection of metadata, implying this is less serious than the collection of content. That is not a correct assumption. Metadata are all data about a communication taking place, except for the content of the conversation. They may include the phone number or IP address of the person placing a call or sending an e-mail, time and location information, the subject, the addressee, etc. Its analysis may reveal sensitive data about persons, for example because certain information

numbers for medical or religious centres are dialed. As stated by the European Court of Human Rights already in the Malone case[1], the processing of metadata, in this case 'metering', "is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts [...] to an interference with a right guaranteed by Article 8." The Court has maintained this position throughout the years.

It is also particularly important to note that metadata often yield information more easily than the actual contents of our communications do.[2] They are easy to aggregate and analyse because of their structured nature. Sophisticated computing tools permit the analysis of large datasets to identify embedded patterns and relationships, including personal details, habits and behaviours. This is not the case for the conversations, which can take place in any form or language. Sophisticated computing tools permit the analysis of large datasets to identify embedded patterns and relationships, including personal details, habits and behaviours.

According to Article 2(a) Directive 95/46/EC, personal data is "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly". A similar definition is given in article 2(a) of Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data. Therefore, unlike in other countries, in Europe metadata are personal data and should be protected.[3]

In the recent judgment in the data retention cases, the Court of Justice of the European Union confirmed that "[telecommunications] data, taken as a whole, may allow very precise conclusion to be drawn concerning the private lives of the persons whose data has been retained".[4] And finally in that judgment the Court found "that the obligation to retain for a certain period, data relating to a person's private life and to his communications, constitutes in itself an interference with the right guaranteed by Article 7 of the Charter. Furthermore, the access of the competent national authorities to the data constitutes a further interference with that fundamental right. [...] 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"[5]

---

[1] ECHR, Malone v. UK, 2 August 1984

[2] ACLU v. Clapper, Case No. 13-3994 (WHP) – Written declaration of professor Edward W. Felten before the United States District Court for the Southern District of New York

[3] This is a long standing interpretation of data protection law. In its Opinion 4/2007 on the concept of personal data, the Working Party has already stated that also "in cases where prima facie the extent of the identifiers available does not allow anyone to single out a particular person, that person might still be 'identifiable' because that information combined with other pieces of information (whether the latter is retained by the data controller or not) will allow the individual to be distinguished from others".

[4] See ECJ, Joined Cases C-293/12 and C-594/12, 8 April 2014, §27

[5] See ECJ, Joined Cases C-293/12 and C-594/12, 8 April 2014, §34, 35 and 37

3. Key points

The Snowden revelations have been a hard wake-up call for many. Never before the existence of so many different surveillance programmes run by intelligence services and able to collect data about virtually everyone, had been disclosed. Some cases have emerged before, but now for the first time extensive evidence about their pervasiveness has been brought into the debate. The way intelligence services make use of data on our day-to-day communications as well as the content of those communications underlines the need to set limits on the scale of surveillance.

Even those who are careful about how they run their online lives can currently not protect themselves against mass surveillance programmes. And given the many legal, technical and practical challenges, also data protection authorities around the world cannot provide a satisfactory protection. Change is therefore in order.

In the following chapters the Article 29 Working Party analyses the mass data collection by intelligence services in the light of their surveillance programmes. From a legal perspective, a distinction needs to be made between surveillance programmes run by intelligence services of the Member States and those carried out by intelligence services of third countries making use of data of EU citizens.

Surveillance programmes run by the EU Member States will in general not be subject to EU law, following the national security exemption written into the European treaties, as well as – following this decision of the contracting Member States – several EU regulations and directives, including the EU data protection directive 95/46/EC. That does not mean however such programmes are only subject to national law. The analysis of the WP29 shows, that even though EU law in general and the data protection directive in particular do not apply, the data protection principles[6] following the European Convention on Human Rights and Council of Europe Convention 108 on the protection of personal data will for the most part still need to be respected by the intelligence services in order to lawfully perform their duties. These principles are oftentimes also included in the national constitutions of the Member States. Under no circumstance surveillance programmes based on the indiscriminate, blanket collection of personal data can meet the requirements of necessity and proportionality set out in these data protection principles. Limitations to fundamental rights have to be interpreted restrictively, following case law from the European Court of Human Rights (ECtHR)[7] and the Court of Justice of the European Union (ECJ)[8]. This includes the need for all intrusions to be necessary and proportionate in relation to the purpose to be achieved. Also, it should be kept in mind that there is no automatic presumption that the national security argument used by a national authority exists and is valid. This has to be demonstrated.

---

[6] The main data protection principles are: fair and lawful processing, purpose limitation, necessity and proportionality, accuracy, transparency, respect for the rights of individuals and adequate data security.

[7] See ECtHR, Delcourt, 17 January 1970, and Klass, 6 September 1978

[8] See ECJ, Joined Cases C-293/12 and C-594/12, 8 April 2014 where the Court has held that the retention of traffic data "without any differentiation, limitation or exception" constitutes "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" (§§57 jo. 65).

The Working Party stresses it is the responsibility of the Member States' governments to comply with all their national and international obligations, including the International Covenant on Civil and Political Rights Failing to do so not only infringes upon the fundamental rights of their citizens, but also damages the trust of society in the rule of law.

For surveillance programmes run by third countries, the situation is more complex. Where data is collected, either directly from a source within the EU or after a transfer to the said third country (or another third country for that matter), EU law may still be applicable to the disclosures made under the surveillance programmes. In fact, the national security exemption referred to above only applies to the national security of an EU Member State, and not to the national security of a third country. Of course, situations may occur where the national security interest of a third country coincides with that of a Member State and where joint surveillance operations may be warranted. Also here, the public authorities involved in the surveillance need to be able to demonstrate why and how the national security interests coincide and thus exclude the application of EU law.

All conditions for international transfers of personal data set out in directive 95/46/EC need to be respected: this means above all that the recipient ensures an adequate level of protection and that transfers need to be in line with the original purpose for which the data were collected. Transfers must also comply with the need to have the appropriate legal basis for a fair and lawful processing.

None of the instruments available that can be used as an alternative basis to transfer personal data to countries that have not been found adequate (Safe Harbor, Standard Contractual Clauses and BCRs) allow for third country public authorities for the purpose of indiscriminate, massive surveillance to gain access to personal data transferred on the basis of these instruments. In fact, the exceptions included in these instruments are limited in scope and should be interpreted restrictively (i.e. to be used in specific cases and for specific investigations). Since the adequacy instruments are primarily intended to offer protection to personal data originating in the EU, they should never be implemented to the detriment of the level of protection guaranteed by EU rules and instruments governing transfers. The Working Party furthermore stresses that under the data protection directive the current assessment of the level of data protection in third countries in general does not cover the processing of data for law enforcement or surveillance purposes.

Also companies need to be aware that they may be acting in breach of European law if intelligence services of third countries gain access to the data of European citizens stored on their servers or comply with an order to hand over personal data on a large scale. In that regard, companies may find themselves in a difficult position in deciding whether they comply with the order to supply personal data on a large scale or not: in either case they are likely to be in breach of European or third country law. Enforcement action against these companies in particular should not be excluded in situations where data controllers have willingly and knowingly cooperated with intelligence services to give them access to their data. Companies do need to be as transparent as possible and ensure that data subjects are aware that once their personal data are transferred to non-adequate third countries on the basis of the instruments available for such transfers, they might be subject to surveillance or access

rights by third country public authorities, as far as such exceptions are provided for by the instruments mentioned above. The main focus is however to find an effective solution at the political level. An international agreement providing safeguards could ensure that intelligence services respect fundamental rights.

In order to ensure that intelligence services indeed do respect the limits imposed on surveillance programmes, meaningful oversight mechanisms need to be implemented in the laws of all Member States. This should include fully independent checks on data processing operations by an independent body as well as effective enforcement powers. Next to effective and robust parliamentary scrutiny, this could be done by a data protection authority or another suitable independent body, depending on the oversight arrangements adopted by the Member State. If the oversight were to be carried out by another body, the Working Party encourages regular contacts between this body and the national data protection authority to ensure a coherent and consistent application of the data protection principles.

It should be stressed that oversight mechanisms do not only need to exist on paper, but also have to be applied consistently. The Snowden revelations have shown that even though on paper many checks and balances are in place, including judicial review of intended data collection schemes, the effectiveness of the way the safeguards have been implemented remains doubtful. If safeguards against unwarranted access are not applicable to all surveillance programmes nor apply to all individuals, they do not add up to what the Working Party would consider to be meaningful oversight.

4. Supervision of intelligence services

While other entities have conducted expert analysis over the past year of the oversight arrangements for the security and intelligence services of third countries, fewer expert analyses have emerged about the national intelligence services in each EU Member State. To get a clearer picture of the various arrangements in Europe for supervision over the national intelligence services, the Working Party has issued a questionnaire to all data protection authorities (including two non-EU observers), to find out about their national supervision practice in this regard.[9]

There are two issues worthy of analysis in particular:

1. The existence of comprehensive oversight in the legal framework for national security and intelligence services;

2. The role (or absence of role) of the national data protection supervisory authority in that framework.

The Working Party herewith also responds to the request of Vice President Reding of the European Commission to analyse what the role of data protection authorities could be.[10]

[9] The answers to the questionnaire were provided by 27 EU national data protection authorities, the sub-national data protection authority of Saxony (Germany) and the non-EU data protection authorities from Switzerland and Serbia.
[10] Letter from Vice President Reding to the Chair of the Article 29 Working Party, 30 August 2013.

4.1. Overview of the applicable national oversight mechanisms

The surveillance activities discussed in this Opinion and the appended Working Document are mainly carried out by the intelligence services in the light of their task to protect national security. A wide diversity of oversight models exists, depending on the national legal traditions and structures dedicated to national security arrangements. In 26 of 27 Member States that provided information in response to the questionnaire[11], intelligence services exist and operate on the basis of laws specifying their competences, structure, and responsibilities. In one Member State there are no intelligence services and the security function of the State is carried out by a national police force.[12]

Most respondents report the existence of between one and three security and intelligence authorities at national level. In general there is a division of tasks between internal national security threats and external (foreign) national security threats, which leads as well to different responsibilities, civilian (Ministry of Interior or Justice) and military (Ministry of Defence). In three States, the different structures are integrated so as to form a system of protection that directly reports to the Head of the Government (eg Prime Minister).

The processing of personal data is based on a law at Member State's level and the supervision is based either in the general data protection law (further referred to as 'GDPL') or one or more special laws regulating the processing of personal data by one or more intelligence services.

4.2. The role of the national data protection supervisory authority

It becomes clear from assessing the relevant national legislation that the GDPL in many countries does not apply to the activities of intelligence services and the data protection authority has a limited or in some cases non-existent supervisory role. Often, a specific data protection regime is provided for in law, but it does not necessarily include dedicated oversight from the data protection authority.

In the two other non-EU countries who kindly contributed to the questionnaire[13] processing of personal data by the intelligence services is regulated by the GDPL. They are subject to oversight by the national data protection authority based on provisions of the GDPL.

The GDPL, when applicable, generally provides for a number of exemptions (derogations to one or more principles) for the processing of personal data by intelligence services. These exemptions routinely refer to the basic duties of data controllers and the data subject rights.[14] The limitations may concern restriction to the right to be informed and the right of access by the data subject, which is in general to be exercised through the data protection authority.

---

[11] Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom.

[12] Ireland.

[13] Serbia (one civil service, two military services), Switzerland (one civilian, one military)

[14] E.g. Belgium, Bulgaria, Cyprus, Germany, Hungary, Greece. For some Member States information on exemptions could not be established.

As to supervision of the data processing, in four Member States only it seems that the national general data protections laws (or law establishing general data protection supervisory bodies) provide for in principle the same supervisory powers over the intelligence services as over any other data controller. [15] In thirteen Member States the data protection authority supervision competence includes the national security and intelligence services within scope, but in some cases special rules or procedures apply to the supervision of intelligence or intelligence services, including the possibility to impose sanctions.[16] In nine Member States the data protection authority has no supervisory powers over the intelligence services acting as data controllers.[17]

Only in Sweden and Slovenia is full supervision by the data protection authority over compliance with the applicable data protection obligations in place. Where some other national data protection authorities have powers over the intelligence services, they check compliance with the applicable GDPL and deal with complaints and the exercise of the right of access by the individual concerned. They also have the power to investigate cases either on their own initiative or at the request of a third party and make in situ inspections. Some limitations to these powers may be in place in certain Member States, for example imposing compliance with special security rules when investigation cases to take account of State secrecy requirements.

4.3. The role of other independent oversight mechanisms

Twenty Member States declared that the law provides for parliamentary oversight and/or control over the activities of intelligence services alongside the competences of the data protection authorities for the data processing[18], and specific internal systems of scrutiny.[19] However, different understandings of parliamentary control seem to be in place in the Member States, few of which may be considered to entail having an actual body responsible for the oversight of data protection (including assessing a data subject's rights and compliance with the provisions of both GDPL and specific legislation).[20]

Existing oversight schemes are extremely diverse, comprising as follows:

- A parliamentary committee which may have the broad task of supervising intelligence and security authorities in general, or a particular intelligence services.

- The parliamentary oversight and / or control is in place alongside other (non-data protection authority) independent supervisory bodies. Existing formats of parliamentary control take the form of a parliamentary ombudsman, parliamentary delegation or a parliamentary commission.

[15] Bulgaria, Hungary, Slovenia, Sweden.
[16] Austria, Belgium, Cyprus, Estonia, Finland, France, Germany, Ireland, Italy, Latvia, Luxembourg, Poland, Sweden.
[17] Czech Republic, Denmark, Malta, Netherlands, Portugal, Romania, Slovakia, Spain, United Kingdom
[18] For example, in Finland the Parliamentary Ombudsman is responsible alongside the data protection authority; but his competencies are based on the dedicated law for the security and intelligence services.
[19] The twenty Member States referred to: Austria, Bulgaria, Cyprus, Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Luxembourg, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, United Kingdom.
[20] The opinion does not analyse information on managerial (ministerial) and general political control provided by several contributing states.

- A parliamentary committee is the only supervisory authority outside the executive power structure. The tasks of the parliament here are formulated either in rather a general way, or so that access to open cases is not provided for.

- The oversight is vested in a special authority exclusively. However, the competence can be created by the data protection legislation but there is also a reported incidence of this authority being regulated by soft-law until recently.

- Specialised judicial control is in place alongside the general parliamentary oversight.

- A mixed executive and parliamentary control is in place alongside the general data protection authority, where the chair of the dedicated Commission is a judge and other members are from different political parties in Parliament past and present. Procedures exist for consultation with the data protection authority.

- Inspiration for improving elements of oversight can also be gained from those systems, where a special body was created specially dedicated to data protection oversight of the intelligence services: the Data Supervising Commission, composed of three public prosecutors, nominated by the General Public Prosecutor which supervises the intelligence services alongside with the parliamentary Supervising Council.

- While cases can be brought to the data protection authority to test whether national security is involved, once this involvement is established it must refer the case to two independent Commissioners with independent judicial oversight of national intelligence services and the role of the Secretary of State in granting warrants for conducting covert surveillance. Supporting these is a dedicated Tribunal for data subject redress.

- Dedicated law provides for the co-operation between the special oversight body and the general data protection authority: an independent Legal Protection Commissioner must give authorisation if the intelligence or intelligence services wish to conduct certain operations (e.g. undercover investigations, video surveillance of specific persons). The Legal Protection Commission is further obliged to lodge a complaint with the data protection authority if he is of the opinion that rights under the GDPL have been infringed.

The data protection authority has the power to supervise intelligence services with some limitations, but a special parliamentary body is responsible for oversight on the interception of communication and dealing with complaints. Members of the respective committee are appointed by the Parliamentary Control Committee. The chairperson must have the qualification to hold judicial office.

5. Recommendations

A. More transparency

1. More transparency is needed on how the programmes work and what the supervisors do and decide

The Working Party considers it important that Member States are transparent to the greatest extent possible about their involvement in intelligence data collection and sharing programmes, preferably in public, but if necessary at least with their national parliaments and the competent supervisory authorities. Data protection authorities are recommended to share their expertise at national level in order to restore the balance between national security interests and the fundamental right of respect for the private life of individuals.

Some form of general reporting on surveillance activities should be in place, also in line with the transparency obligation that lies on Member States following the ECtHR.[21] Every interference with fundamental rights has to be foreseeable and therefore these programmes have to be based in clear, specific and accessible legislation. The national data protection authorities are invited to bring this position to the attention of their respective governments.

2. More transparency by data controllers

Companies do need to be as transparent as possible and ensure that data subjects are aware that once their personal data are transferred to non-adequate third countries on the basis of the instruments available for such transfers, they might be subject to surveillance or access rights by third country public authorities, as far as such exceptions are provided for by these instruments. The Working Party is aware that controllers might be ordered to refrain from informing the data subject of the order it has received from a public authority. It welcomes recent efforts to provide the data subject with better and more information about the requests it receives and encourages the companies to continue to improve the information policies.

3. Maximising public awareness

Data subjects need to be aware of the consequences the use of online and offline electronic communication services may have as well as how they can better protect themselves. This is a shared responsibility of data protection authorities, other public authorities, companies as well as civil society. To this end, the Working Party intends to organise a conference in the second half of 2014 bringing together all stakeholders to discuss a possible approach.

[21] Also see European Court of Human Rights, Case no. 48135/06 – *Youth Initiative for Human Rights v Serbia* (25 June 2013), p.6

B. More meaningful oversight

1. Maintain a coherent legal system for the intelligence services, including rules on data protection

The Snowden revelations have made clear the intelligence services in the European Union Member States process large amounts of personal data on a daily basis. These data are also shared with other services in- and outside the EU. The Working Party considers it is important that the Member States have a coherent legal framework for the intelligence services including rules on data processing in compliance with the data protection principles as laid down in European and international law. The rights of the data subject need to be guaranteed to the maximal possible extent, while preserving the public interest at stake.

The Working Party furthermore recommends the national legal framework to contain clear rules on the cooperation and exchange of personal data with law enforcement authorities for preventing, combating and prosecuting crimes, including on the transfer of such data to authorities in other EU Member States and in third countries.

2. Ensure effective oversight on the intelligence services

In the national legal framework on the intelligence services, specific attention should be paid to the oversight mechanisms in place. Appropriate, independent and effective oversight is of the highest importance in a democratic society. The Working Party therefore considers the following good practices from the various oversight mechanisms currently in place in the Member States should be part of the oversight mechanisms in all Member States. The national data protection authorities are urged to bring these elements into the national debate on intelligence services oversight:

- Strong internal checks for compliance with the national legal framework in order to ensure accountability and transparency;

- Effective parliamentary scrutiny in line with national parliamentary traditions. National data protection authorities should encourage parliaments already having supervisory powers over the intelligence services to actively carry out these tasks;

- Effective, robust and independent external oversight, performed either by a dedicated body with the involvement of the data protection authorities or by the data protection authority itself, having power to access data and other relevant documentation on a regular basis and on its own initiative (ex officio), as well as an obligation to inspect following complaints. Prior approval of the intelligence services to be supervised must not be required;

C. Effective application of current law

1. Enforce the existing obligations of EU Member States and of Contracting Parties to the ECHR to protect the rights of respect for private life and data protection

All Member States are Parties to the European Convention of Human Rights. Thus, they have to comply with the conditions Article 7 and 8 ECHR set for their own surveillance

programmes. Their obligations do not end there. Article 1 ECHR also obliges the Parties to secure everyone within their jurisdiction the rights and freedoms provided in the Convention. In both scenarios, EU Member States, as well as any Party to the ECHR, can be brought before the ECtHR for a violation of European legal subjects' right to respect for private life.

2. Controllers subject to EU jurisdiction shall comply with applicable EU data protection legislation

Data controllers established in the EU or making use of equipment in a Member State must respect their obligations under EU law, even where the law of other countries where they operate contradicts EU law. In this regard, data protection authorities cannot ignore the fact that data transfers can occur in contravention of EU law. The Working Party therefore recalls that data protection authorities may suspend, according to the terms set by EU and national data protection provisions, data flows foreseen in the transfer instruments where there is a substantial likelihood that the data protection principles are being violated and that continuing transfers would create an imminent risk of grave harm to the data subject. National data protection authorities should decide according to their national competence if sanctions are in order in a specific situation.

D. Improve the protection on European level

1. Adoption of the data protection reform package

In order to offer strong data protection in Europe, the finalisation of the negotiations on the data protection reform package is of the utmost importance. Not only does the new General Data Protection Regulation and the Police and Justice Data Protection Directive aim for better data protection for individuals. Also, they are designed to clarify their scope of application and give more enforcement powers to data protection authorities. Especially the option to impose (financial) penalties – as a final resort – should ensure more leverage towards data controllers. The Working Party welcomes the proposal of the European Parliament to provide for mandatory information to individuals when access to data has been given to a public authority in the last twelve months. Being transparent about these practices will greatly enhance trust. The Working Party therefore urges the Council and the European Parliament to stick to their agreed timetable[22] and ensure both instruments can be adopted in the course of 2014.

2. Clarify the scope of the national security exemption

There is currently no common understanding of what is meant by national security. No clear definition has been adopted by the European legislator, nor is the case law of the European courts conclusive. However, the exemption must not be extended to the processing of personal data for purposes for which they cannot legally be used.

Another part of the question that needs to be answered is to what extent an exemption focused on national security continues to reflect reality, now it appears the work of the intelligence

[22] http://euobserver.com/justice/122853

services is more than ever before intertwined with the work of law enforcement authorities and pursues several different purposes. Data is shared on a continuous and global basis, leaving aside the question which nation's security is to benefit from the analysis of these data. The Working Party therefore calls upon the Council, the Commission and the Parliament to come to an agreement in order to define the principle of national security and be conclusive as to what should be regarded as the exclusive domain of the Member States. When defining the principle of national security, due account shall be given to the reflections of the Working Party, including the ones made in this Opinion. The EU institutions are also urged to clarify in the data protection reform package that the protection of the national security of third countries alone cannot exclude the applicability of EU law.

E. International protection for EU residents

1. Insist on adequate safeguards for intelligence data sharing

Third countries' public authorities in general, and intelligence services in particular, must not have direct access to private sector data processed in the EU. If they require access to such data in a specific case based on a reasonable suspicion, where applicable they need to make a request under international agreements, providing adequate data protection safeguards. As far as the sharing of intelligence information is concerned, Member States have to ensure that the national laws provide for a specific legal basis for such transfers as well as adequate safeguards for the protection of personal data. In the view of the Working Party, secret cooperation agreements between Member States and/or third countries do not meet the standard of the ECtHR for a clear and accessible legal basis.

2. Negotiate international agreements to grant adequate data protection safeguards

The idea of a so-called Umbrella agreement, currently negotiated between the US and the EU, is a step into a right direction. However, such an agreement is likely to have two shortcomings: it will exempt cases concerning national security, at least from an EU perspective, since it is negotiated as an agreement based on EU law only. Its structure suggests that it would only apply to data transferred between public authorities in the US and the EU, not to data collected by private entities. This is also what becomes clear from the report of the EU-US High Level Contact Group (HLCG) on information sharing and privacy and personal data protection[23], which forms the basis for the negotiations on the Umbrella agreement. The Working Party stresses that under the Umbrella agreement, the purpose for the processing of the transferred data should be the same both in the EU and the US. It would not be acceptable if data originating from EU law enforcement could subsequently be used by US intelligence for national security purposes, if such is not also possible in the EU.

Since the Umbrella Agreement will fall short in offering full protection to all citizens, what is needed is an international agreement providing adequate protection against indiscriminate surveillance. Also the current conflict of jurisdictions affecting part of the disclosed surveillance activities, could be mitigated if such an agreement sets clear limits to

[23] Council Document 15851/09, 23 November 2009

surveillance. However, this agreement would be directly linked to the national security exemption and thus fall outside the scope of EU law. Therefore, it is up to the Member States to start negotiations in a coordinated manner. Due account should be given to the clear identification of which of the surveillance activities described would indeed be covered by national security, and which are rather more related to law enforcement and foreign policy purposes, areas which would fall under Union law. This would trigger the possibility for EU institutions to participate more closely in case steps are taken in this direction.

This new agreement must not be a secret one. It must be published and should include obligations on the contracting parties on the necessary oversight of surveillance programmes, on transparency, on equal treatment of at least citizens of all Parties to the Agreement, on redress mechanisms and other data protection rights. Also, the involved Parties should be encouraged to ensure their parliaments are informed about the use and value of the concluded agreement on a regular basis.

3. Develop a global instrument protecting privacy and personal data

The Working Party supports the development of a global instrument providing for enforceable, high level privacy and data protection principles as agreed upon by the International Conference of Data Protection and Privacy Commissioners in their Madrid Declaration.[24] In this regard, the adoption of an additional protocol to Article 17 of the UN International Covenant on Civil and Political Rights could be considered. In such an international instrument, it must be ensured that the safeguards offered are applicable to all individuals concerned. It is also necessary to come to a general interpretation of the meaning of 'data processing', because there are large differences in the understanding worldwide.

The Working Party supports the initiative taken by the German government and the call from the International Conference of Data Protection and Privacy Commissioners.[25,26] Furthermore, the Working Party continues to support the accession of third countries to the Council of Europe's Convention 108.

[24] International Standards on the Protection of Personal Data and Privacy, adopted by the 31st International Conference of Data Protection and Privacy Commissioners in Madrid.
[25] http://www.bundesregierung.de/Content/EN/Artikel/2013/07/2013-07-19-bkin-nsa-sommerpk.html.
[26] Resolution on anchoring data protection and the protection of privacy in international law, adopted during the 35th International Conference of Data Protection and Privacy Commissioners in Warsaw.

IN THE COURT OF JUSTICE OF THE EUROPEAN UNION
CASE C-698/15

ON A REFERENCE FROM
THE COURT OF APPEAL OF ENGLAND & WALES (CIVIL DIVISION)

Neutral citation: [2015] EWCA Civ 1185

B E T W E E N:

SECRETARY OF STATE FOR THE HOME DEPARTMENT

Appellant

v.

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

Respondents

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

Interveners

WRITTEN OBSERVATIONS OF NGO INTERVENERS

ANNEX 5

Annex 5 to Written Observations of NGO Interveners

Member State Decisions on Data Retention Before and After *Digital Rights Ireland*

Member State	Decision	Date
Period Before *Digital Rights Ireland* Judgment		
Lithuania	Lithuania's Constitutional Court declares Lithuanian data retention laws (Law on Telecommunications 2000 and 2002; Law on Operational Activities 2002; and Code of Criminal Procedure) are incompatible with the Constitution of Lithuania in Ruling in Case No. 34 / 2000-28 / 01[1]	19 September 2002
Bulgaria	Bulgaria's Supreme Administrative Court declares several sections of the Bulgarian data retention law (Act on Electronic Communications) incompatible with the principles of legal certainty in judgement U-I-65/13-19 of 3 July 2014[2]	11 December 2008
Romania	The Romanian Constitutional Court declares the first Romanian data retention laws (Law No.298/2008 regarding the retention of data and the modification of Law No.506/2004 regarding the personal data processing) to be unconstitutional in Decision No.1258[3]	8 October 2009
Germany	The German Constitutional Court declares sections of the Telecommunications Act and the Code of Criminal Procedure void as unconstitutional in judgment 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 of 2 March 2010[4]	2 March 2010
Cyprus	The Supreme Court of Cyprus rules the Cypriot data retention law (Law 183[I]/2007 (Retention of Telecommunication Data for Purposes of Investigation of Serious Criminal Offences)) in violation of constitutional rights protections.[5]	1 February 2011
Czech Republic	The Czech Constitutional Court declares the Czech data retention law (Electronic Communications Act 127/2005) unconstitutional[6]. A revised data retention law was passed in November 2012[7], amending the 2005	31 March 2011

[1] http://www.lrkt.lt/lt/teismo-aktai/paieska/135/ta309/content.
[2] http://www.aip-bg.org/documents/data_retention_campaign_11122008eng.htm.
[3] http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf.
[4] https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2010/03/rs20100302_1bvr025608en.html;jsessionid=6712BF2C43AAC24F176E1A35C3ABE4EF.2_cid383.
[5] https://edri.org/edrigramnumber9-3data-retention-un-lawful-cyprus/ and http://www.supremecourt.gov.cy/Judicial/SC.nsf/All/5B67A764B86AA78EC225782F004F6D28/$file/65-09.pdf.

	Electronic Communications Act.	
Period After *Digital Rights Ireland* Judgment		
Slovakia	The Slovak Constitutional Court rules that the Slovak data retention law (provisions of the Act on Electronic Communications (Act No.351/2011 Coll.), the Penal Code (Act No.301/2005 Coll.) and the Police Force Act (Act No. 171/1993 Coll.)) are incompatible with the Constitution of Slovakia.[8]	29 April 2014
Austria	The Constitutional Court of Austria declares the data retention provisions in the Austrian Telecommunications Act, the Police Authorisation Act and the Criminal Procedure Act to be unconstitutional.[9]	27 June 2014
Slovenia	The Constitutional Court of Slovenia rules that the Slovenian data retention law (provisions of the Act on Electronic Communications) are incompatible with the constitution of Slovenia, in its judgment U-I-65/13-19. The court orders all retained data erased.[10]	3 July 2014
Romania	The Romanian constitutional court rules that the second Romanian data retention law (no. 82/2012) is unconstitutional[11]	8 July 2014
United Kingdom	UK Government passes Data Retention and Investigatory Powers Act 2014[12]	17 July 2014
Poland	The Polish Constitutional Tribunal rules on data retention and other surveillance powers, requiring greater controls on access to data.[13]	30 July 2014
Finland	Finnish Information Society Code 2015 enters into force, modifying previous data retention provisions, removing reference to the Data Retention Directive, shortening the retention periods and removing some classes of electronic data from scope.[14]	1 January 2015
Luxembourg	The Luxembourg Ministry of Justice filed proposal n° 6763 modifying the Luxembourg Criminal Procedure Code and the Act of 30 May 2005 laying down specific provisions for the protection of persons with regard to the processing of personal data in the electronic communications sector, as amended[15]	7 January 2015

[6] https://edri.org/czech-decision-data-retention/.
[7] http://www.loc.gov/law/foreign-news/article/czech-republic-newly-amended-data-retention-law/.
[8] https://edri.org/slovakia-mass-surveillance-of-citizens-is-unconstitutional/ and http://www.eisionline.org/images/Data_retention_rozhodnutie_PL_US_10_2014.pdf.
[9] http://fra.europa.eu/en/caselaw-reference/austria-constitutional-court-g472012-ua.
[10] https://www.ip-rs.si/index.php?id=272&tx_ttnews[tt_news]=1256&cHash=2885f4a56e6ff9d8abc6f94da098f461 and https://edri.org/slovenia-data-retention-unconstitutional/.
[11] http://www.ccr.ro/noutati/COMUNICAT-DE-PRES-99 and https://edri.org/romania-aftermath-of-second-ccr-data-retention-ruling/ .
[12] http://www.legislation.gov.uk/ukpga/2014/27/contents/enacted/data.htm.
[13] http://trybunal.gov.pl/sprawy-w-trybunale/art/2013-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani-4/
[14] http://lexia.fi/2014/12/22/finnish-information-society-code-enters-into-force-2015/ ; http://www.finlex.fi/en/laki/kaannokset/2014/en20140917.pdf.

Netherlands	The court in *Privacy First Foundation et al. v. the State of the Netherlands*, case number C-09/480009/KG ZA 14/1575, rules the Dutch data retention law (the 2009 Data Retention Act) incompatible with EU Charter rights[16]. All Internet Service Providers immediately ceases data retention as a consequence.	11 March 2015
Bulgaria	The Bulgarian Constitutional Court rules that the Bulgarian data retention law (the Electronic Communications Act) as unconstitutional[17]	12 March 2015
Sweden	The Stockholm Administrative Court of Appeal refers the case of *Tele2 Sverige AB v Post- och Telestyrelsen* to the CJEU (Case C-203/15)	4 May 2015
Belgium	The Belgian Constitutional Court rules against the mass collection of communications metadata as unconstitutional and requires repeal of the law.[18]	12 June 2015
Hungary	Hungarian Constitutional Court declines to rule on the merits of national data retention legislation due to procedural issues (see *Társaság a Szabadságjogokért & Privacy International, 'Suggestions for privacy-related questions to be included in the list of issues on Hungary*, Human Rights Committee, 115th Session, October-November 2015', 7 August 2015, pp. 5-6[19]). The proceedings remain ongoing.	No new law/decision
Ireland	*Digital Rights Ireland* proceedings remain ongoing domestically, to enforce the CJEU judgment in relation to the Communications ((Retention of Data) Act 2011[20]	No new law/decision

[15] http://www.lexology.com/library/detail.aspx?g=252b375d-39f5-4379-9095-a772e8eb2f03 and https://www.stibbe.com/en/news/2015/april/benelux-ict-law-newsletter-51-a-new-luxembourg-bill-on-data-retention .

[16] http://pilpnjcm.nl/the-hague-judge-puts-a-stop-to-dutch-data-retention-act/ and http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2015:2498.

[17] http://sofiaglobe.com/2015/03/12/bulgarias-constitutional-court-scraps-data-retention-provisions/ and http://constcourt.bg/caseframe/caseid/477.

[18] https://edri.org/belgian-constitutional-court-rules-against-dataretention/ ; http://www.const-court.be/public/f/2015/2015-084f.pdf

[19] http://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/HUN/INT_CCPR_ICS_HUN_21421_E.pdf).

[20] https://www.digitalrights.ie/dri/wp-content/uploads/2015/12/Ireland_UPR-Stakeholder-Submission-DRI-and-Privacy-International_FINAL.pdf

IN THE COURT OF JUSTICE OF THE EUROPEAN UNION
CASE C-698/15

ON A REFERENCE FROM
THE COURT OF APPEAL OF ENGLAND & WALES (CIVIL DIVISION)

Neutral citation: [2015] EWCA Civ 1185

B E T W E E N:

SECRETARY OF STATE FOR THE HOME DEPARTMENT

Appellant

v.

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

Respondents

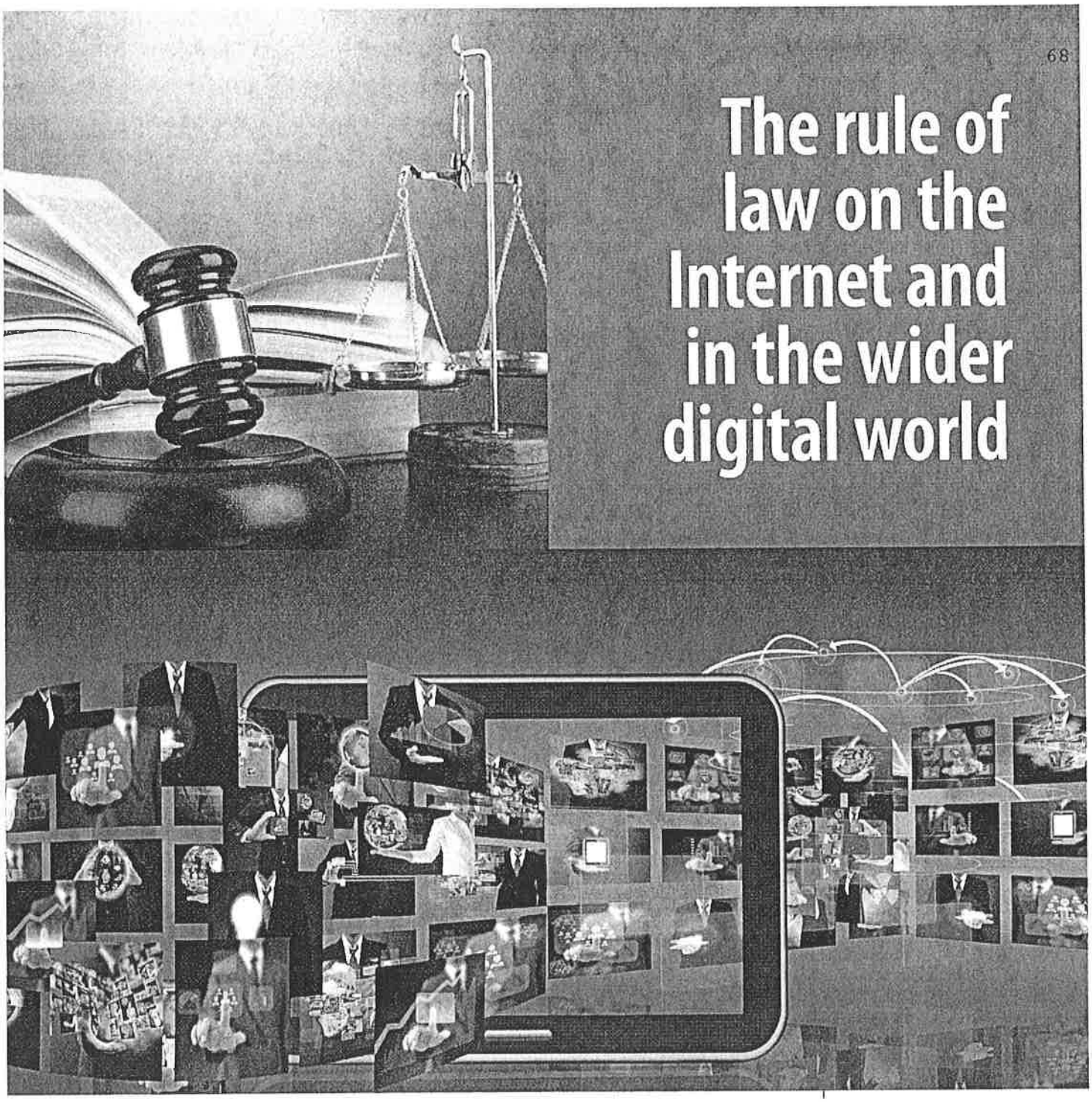
(1) OPEN RIGHTS GROUP;
(2) PRIVACY INTERNATIONAL;
(3) THE LAW SOCIETY OF ENGLAND AND WALES

Interveners

WRITTEN OBSERVATIONS OF NGO INTERVENERS

ANNEX 6

The rule of law on the Internet and in the wider digital world



Issue paper

COMMISSIONER FOR HUMAN RIGHTS
COMMISSAIRE AUX DROITS DE L'HOMME
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Four issues stand out. First, state actions aiming to counter cybercrime, threats to cybersecurity and threats to national security are increasingly intertwined; the boundaries between such activities are blurred, and the institutions and agencies dealing with them work more closely together. Second, states are now co-ordinating their actions in all these regards. Third, the work of national security and intelligence agencies increasingly depends on monitoring the activities of individuals and groups in the digital environment. Fourth, instead of *ex post facto* law enforcement, the emphasis is now on intelligence and prevention, with law-enforcement agencies using techniques – and technologies – previously reserved for secret services.

The nature of the digital environment

Dangerous data

In an age of "Big Data" (when data on our actions are shared and/or exploited in aggregate form) and the "Internet of Things" (when more and more physical objects – things – are communicating over the Internet), it is becoming difficult to ensure true anonymisation: the more data are available, the easier it becomes to identify a person. Moreover, the mining of Big Data, in ever more sophisticated ways, leads to the creation of profiles. Although these profiles are used to spot rare phenomena (e.g. to find a terrorist in a large set of data, such as airlines' passenger name records), they are unreliable and can unwittingly lead to discrimination on grounds of race, gender, religion or nationality. These profiles are constituted in such complex ways that the decisions based on them can be effectively unchallengeable: even those implementing the decisions do not fully comprehend the underlying reasoning.

The digital environment can by its very nature erode privacy and other fundamental rights, and undermine accountable decision making. There is enormous potential for undermining the rule of law – by weakening or destroying privacy rights, restricting freedom of communication or freedom of association – and for arbitrary interference.

Global and private, but not in the sky

Because of the open nature of the Internet (which is its greatest strength), any end point on the network can communicate with virtually any other end point, following whatever route is calculated as being most efficient, the data flowing through all sorts of switches, routers and cables: the Internet's physical infrastructure. The electronic communications system is transnational, indeed global, by its very nature; and its infrastructure is physical and located in real places, in spite of talk of a Cloud. At the moment, many of these physical components are in the USA and many of them are managed and controlled by private entities, not by governmental ones.

The main infrastructure for the Internet consists of high-capacity fibre-optic cables running under the world's oceans and seas, and associated land-based cables and routers. The most important cables for Europe are those that run from continental Europe to the UK, and from there under the Atlantic to the USA. Given the dominance of the Internet and of the Cloud by US companies, these cables carry

helpful later in a criminal investigation. This practice was imposed in the EU by the Data Retention Directive.[260] As noted in a Council of Europe publication:[261]

> [Compulsory suspicionless, untargeted retention of communication records] "just in case" the data might be useful in some future police or secret service enquiry ... ought to be viewed as mass surveillance of citizens without due cause: a fundamental departure from a basic principle of the rule of law.

It is also fundamentally contrary to the most basic data-protection principles of purpose limitation, data minimisation and data-retention limitation.

This issue is seriously aggravated by the fact that even metadata (i.e. recording what links and communications were made in the digital environment, when, by whom, from what location, etc.) can be highly sensitive and revealing, often exposing, for instance, a person's race, gender, religious beliefs, sexual orientation or political and social affiliations.[262]

What is more, extensive research has failed to show any significant positive effect on clear-up rates for crime, and especially not for terrorism-related crime, as a result of compulsory data retention.[263]

Civil society has strongly and convincingly argued for the replacement of suspicionless data retention by data preservation (also referred to as quick-freeze of data), making it possible for law-enforcement agencies to obtain an order requiring e-communications companies and the like to retain the communications data of people when there are factual indications that it may be helpful to the prevention, investigation or prosecution of crimes, with urgent procedures allowing for the imposition of such a measure without delay in appropriate cases, subject to *ex post facto* authorisation.[264]

Not surprisingly, laws introducing compulsory suspicionless data retention have been held to be unconstitutional in several EU member states, including Germany,

---

260. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L.105, p. 54ff. As the title shows, technically this amends the e-Privacy Directive (Directive 2002/58/EC).

261. Korff and Brown, "Social media and human rights", chapter 6 in *Human rights and a changing media landscape* (Council of Europe 2011), p. 184.

262. See the expert witness statement of Prof. Edward Felten in the case of *ACLU vs. the NSA et al.*, at https://www.documentcloud.org/documents/781486-declaration-felten.html. The Article 29 Working Party opinion on surveillance, noted below, also refers to the Felten statement and usefully adds further references to judgments of the European courts stressing that metadata are equally protected under European human rights law as is content: Article 29 WP Opinion 04/2014 (see n. 269), pp. 4-5.

263. *Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten*, Max Planck Institute for Comparative and International Criminal Law, 2nd enlarged report, prepared for the German Federal Ministry of Justice, July 2011, at www.bmj.de/SharedDocs/Downloads/DE/pdfs/20120127_MPI_Gutachten_VDS_Langfassung.pdf?__blob=publicationFile.

264. See the Shadow evaluation report on the Data Retention Directive (2006/24/EC), produced by EDRi in April 2011, available at www.edri.org/files/shadow_drd_report_110417.pdf.

with the Constitutional Court of Romania holding the very principle to be incompatible with fundamental rights.[265]

In April 2014, the Court of Justice of the EU similarly held that the Data Retention Directive violated basic principles of the EU Charter of Fundamental Rights and was invalid *ab initio*.[266] The CJEU criticised in particular the untargeted nature of the retention measures:

> 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....
> 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.[267]

Such untargeted compulsory data retention may therefore no longer be applied under EU law, or under national laws implementing EU law. Since most national data-retention laws explicitly do exactly that, they will all have to be fundamentally reviewed and replaced with targeted surveillance measures.

Two points are worth noting after this important ruling. First, the CJEU described the legislation as a "particularly serious interference with those fundamental rights in the legal order of the EU". Despite this and despite the court's indication in 2007[268] that

---

265. Eleni Kosta, "The way to Luxembourg: national court decisions on the compatibility of the Data Retention Directive with the rights to privacy and data protection", *Scripted*, Vol. 10 No. 3 (October 2013), p. 339ff, at http://script-ed.org/wp-content/uploads/2013/10/kosta.pdf. The Romanian Constitutional Court decision can be found at www.legi-internet.ro/fileadmin/editor_folder/pdf/Decizie_curtea_constitutionala_pastrarea_datelor_de_trafic.pdf and an unofficial translation at www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf (sources taken from Kosta).

266. Judgment of the Court of Justice of the European Union in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, 8 April 2014, available at: http://curia.europa.eu/juris/documents.jsf?num=C-293/12. This follows the opinion of the Advocate-General, who had concluded that the Directive "as a whole" was invalid and in violation of the Charter: http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=lst&docid=145562&occ=first&dir=&cid=218559.

267. Judgment in Joined Cases C-293/12 and C-594/12 (cited in n. 267), paras. 58-59. The court also criticised the lack of clarity over what constitutes "serious crime".

268. Opinion on the Promusicae/Telefónica de España case from Advocate General Kokott, who pointed out that "there is reason to doubt, whether storing of personal data of all users – quasi on stock – is compatible with fundamental rights, in particular as this is done without any concrete suspicion", *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, case C-275/06, 29 January 2008. See Juliane Kokott, "Data retention – a critical side note by the Advocate General", available at www.libertysecurity.org/article1602.html.

IN THE COURT OF JUSTICE OF THE EUROPEAN UNION
CASE C-698/15

ON A REFERENCE FROM
THE COURT OF APPEAL OF ENGLAND & WALES (CIVIL DIVISION)

Neutral citation: [2015] EWCA Civ 1185

B E T W E E N:

SECRETARY OF STATE FOR THE HOME DEPARTMENT

Appellant

v.

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

Respondents

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

Interveners

WRITTEN OBSERVATIONS OF NGO INTERVENERS

ANNEX 7

United Nations A/69/397

General Assembly

Distr.: General
23 September 2014

Original: English

Sixty-ninth session
Agenda item 68 (a)
Promotion and protection of human rights: implementation of human right instruments

Promotion and protection of human rights and fundamental freedoms while countering terrorism*

Note by the Secretary-General

The Secretary-General has the honour to transmit to the General Assembly the report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson, submitted in accordance with General Assembly resolution 68/178 and Human Rights Council resolution 15/15.

* Late submission.

14-61490 (E) 021014

authorities for communications data in 2013 alone.[42] Courts have for some time recognized that the release of metadata to a public authority constitutes an interference with the right to privacy, and the Court of Justice of the European Union recently held that the retention of metadata relating to a person's private life and communications is, in itself, an interference with the right,[43] (with the grant of access to retained metadata for the purpose of analysis constituting a further and distinct interference).[44] In reaching this conclusion, the Court of Justice of the European Union emphasized that communications metadata may allow "very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained".[45]

55. Applying the approach adopted by the Court of Justice of the European Union, it follows that the collection and retention of communications data constitute an interference with the right to privacy, whether or not the data are subsequently accessed or analysed by a public authority. Neither the capture of communications data under mandatory data retention legislation, nor its subsequent disclosure to (and analysis by) State authorities, requires a prior suspicion directed at any particular individual or organization. The Special Rapporteur therefore shares the reservations expressed by the High Commissioner as to the necessity and proportionality of mandatory data retention laws (see A/HRC/27/37, para. 26).

9. Purpose specification

56. Many States lack "purpose specification" provisions restricting information gathered for one purpose from being used for other unrelated governmental objectives. As a result, data that were ostensibly collected for national security purposes may be shared between intelligence agencies, law enforcement agencies and other State entities, including tax authorities, local councils and licensing bodies.[46] National security and law enforcement agencies are typically excluded from provisions of data protection legislation that limit the sharing of personal data. As a result, it may be difficult for individuals to foresee when and by which State agency they might be subjected to surveillance. This "purpose creep" risks violating article 17 of the Covenant, not only because relevant laws lack foreseeability, but also because surveillance measures that may be necessary and proportionate for one legitimate aim may not be so for the purposes of another (ibid., para. 27). The Special Rapporteur therefore endorses the recommendation of his predecessor that States must be obliged to provide a legal basis for the reuse of personal information, in accordance with human rights principles (see A/HRC/13/37, paras. 50 and 66). This is particularly important where information is shared across borders or between States.

[42] See www.intelligencecommissioners.com/.

[43] Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, Judgment of 8 April 2014, para. 34.

[44] Ibid., para. 35.

[45] Ibid., paras. 26, 27 and 37.

[46] For an analysis of the ways in which such purpose creep has occurred in the United Kingdom, see www.whatdotheyknow.com/request/127491/response/315758/attach/html/2/Summay%20of%20Counsels%20advice.pdf.html.