

ALKOTMÁNYBÍRÓSÁG	
Ügyszám:	III/537-7/2015
Érkezett:	2015 APR 08.
Példány:	1 (FAX) Kezelőiroda:
Melléklet:	db K/

9 98 OPEN RIGHTS GROUP

Free Word Centre
60 Farringdon Road
London, EC1R 3GA
United Kingdom

**PRIVACY
INTERNATIONAL**

62 Britton Street
London, EC1M 5UY
United Kingdom

Alkotmánybíróság
1535 Budapest
Pf. 773.
Hungary

8 April 2015

By mail and fax - 0036 1 212 1170

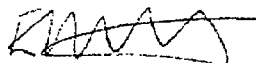
Dear Judge [REDACTED]

Case number: III./537/2015

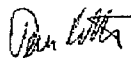
Thank you for your letter of 23 March 2015.

Further to our letter of 19 March 2015 we enclose an amicus curiae brief on behalf of Open Rights Group and Privacy International.

Yours sincerely,



Elizabeth Knight
Legal Director, Open Rights Group



Tomaso Falchetta
Legal Officer, Privacy International

IN THE HUNGARIAN CONSTITUTIONAL COURTCase ref: III/537/2015BETWEEN:

DALMA DOJCSAK

Claimant

v.

TELENOR MAGYARORSZÁG ZRT

Defendant(1) OPEN RIGHTS GROUP;
(2) PRIVACY INTERNATIONALCo-Interveners

AMICUS CURIAE SUBMISSIONS OF THE
CO-INTERVENERS

I. Introduction

1. These are the submissions of the co-interveners, acting as *amicus curiae* in order to bring relevant matters to the attention of the Hungarian Constitutional Court in this referral pursuant to Article 25 (1) of Act 151 of 2011 on the Constitutional Court.
2. The claim concerns extensive powers of data retention contained in Article 159A of Act 100 of 2003 on Electronic communications ("The Electronic Communications Act") and raises the fundamental question of their compatibility with the Charter of Fundamental Rights of the European Union ("CFR") and the European Convention of Human Rights ("ECHR"). These issues are of particular significance in light of "the important role played by the internet [...] in modern society" (Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (13 May 2014) (ECLI:EU:C:2014:317) ("Google Spain") at §80). The internet has become "both ubiquitous and increasingly intimate"¹. In 2011, the European Commission noted that "[t]he volume of

¹ "The right to privacy in the digital age", Report of the Office of the United Nations High Commissioner for Human Rights, 20 June 2014, A/HRC/27/37 available at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

both telecommunications traffic and requests for access to traffic data is increasing", with "over 2 million data requests [...] submitted each year"².

3. On 8 April 2014, by a judgment in Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger* (ECLI:EU:C:2014:238) ("*DRI*"), the Grand Chamber of the Court of Justice of the European Union ("CJEU") concluded that the Data Retention Directive ("*DRD*")³ involved a disproportionate interference with individual rights to privacy and data protection, as guaranteed by Articles 7 CFR and 8 ECHR (privacy) and Article 8 CFR (data protection). As a consequence it annulled the DRD, *ab initio*.
4. The Open Rights Group ("*ORG*") and Privacy International ("*PI*") (together "*the co-interveners*"), are leading non-governmental organisations which are active in the fields of privacy, in particular freedom of expression, privacy, innovation, consumer rights and creativity on the Internet. They support the claim. They respectfully submit that the relevant provisions are contrary to EU law and in particular, in breach of the Data Protection Directive 1995/46 ("*DPD*")⁴ and the Directive on privacy and electronic communications 2002/58/EC ("*PECD*")⁵ which provide for directly effective rights⁶ to erasure, anonymised data, non-identification of callers and prohibit the retention of location data. They also breach the rights of affected individuals under the CFR.
5. By this *amicus curiae* brief, the co-interveners draw the Court's attention to:
 - 5.1. The substantial and carefully calibrated EU rules in the field of data retention and data protection more generally;

² "Evaluation report on the Data Retention Directive (Directive 2006/24/EC)" COM(2011) 224 final, Brussels, 18.4.2011, available at <http://www.statewatch.org/news/2011/apr/eu-com-data-retention-report-225-11.pdf>.

³ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).

⁴ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Official Journal L.281, 23.11.1995 at pp.31-50).

⁵ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Official Journal L.201, 31.07.2002 at pp.37-47).

⁶ See e.g. Joined Cases C-468/10 and C-469/10, (*ASNEF*) *v* *Administración del Estado*, [2011] ECR I-12181 ("*ASNEF*") (ECLI:EU:C:2011:777) at §§50-55.

- 5.2. The importance of the retention of 'communications data' or 'metadata' as well as the content of private communications;
- 5.3. The seriousness of data retention as an interference with the relevant CFR and ECHR rights; and
- 5.4. The need for effective remedies in national legal systems to address breaches of EU law, including in litigation between private parties.

II. The importance of the EU legal framework

6. Data protection, including in the digital sector is subject to EU legislation that Member States are required to implement and to do so in a way that complies with fundamental rights as protected by the CFR and the ECHR. Domestic legislation governing data protection in the digital sector falls within the scope of and must comply with EU law.

The EU framework

7. The DPD and the PECD both regulate the extent to and manner in which personal data can be processed. The DPD, which establishes the core requirements of the regime, is intended to: "*ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data*" (*Google Spain* at [66]).
8. The starting point in relation to such data is the PECD, which provides for EU-wide harmonisation of the level of protection to be afforded by national laws to the processing of personal data in the electronic communications and telecommunications sectors.⁷ Its provisions complement and particularise those provided in the DPD: Article 1 PECD. Crucially, the DPD and PECD were adopted because the Council of Ministers considered that "*the establishment and functioning of the internal market [were] liable to be seriously affected by differences in national rules applicable to the processing of personal data*", such that it was necessary to fully harmonise those rules, including those relating to retention and

⁷ It amended and replaced Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, which also provided for a prohibition on retention and a right to erasure/anonymisation.

storage of data, and to ensure a high level of protection for fundamental rights, most importantly, the right to privacy: see Recital 7 DPD, ASNEF (above) §§27-30; Case C-101/01 *Lindqvist* [2003] ECR I-12971 (ECLI:EU:C:2003:596), §§79 and 96.

9. The PECD provides a directly effective individual right to confidentiality, erasure and anonymity in respect of one's 'communications' or 'traffic data.'⁸ Indeed, it obliges Member States to:
 - 9.1. ensure the confidentiality of such data through the adoption of national legislation to prohibit 'storage' or 'other kinds of interception or surveillance' without the user's consent, save where legally authorised in accordance with Article 15(1); Article 5(1)-(3) PECD (see recital (3) of the DRD);
 - 9.2. require electronic communications providers to erase traffic data relating to subscribers and users or make it anonymous when it is no longer needed for the purpose of the transmission of the communication, save where it is necessary to retain the data for billing purposes and/or where legally authorised under Article 15(1); Article 6 PECD (recital (3) DRD);
 - 9.3. require service providers to offer the possibility of non-identification for callers (Article 8 PECD); and
 - 9.4. prohibit the processing (including retention), of location data unless that data is made anonymous or is processed with the user's consent and even then the user must "*continue to have the possibility, using simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication*": Article 9 PECD (recital (3) DRD).
10. There was good reason for adopting those rights on an EU-wide basis. Data is not a 'national phenomenon': it travels across borders and ensures free commerce and free communication. It was for that reason that harmonisation of rules relating to its

⁸ 'Traffic data' is defined in Article 2(b) PECD as data processed for the purpose of the conveyance of a communication on an electronic communications network or for the purposes of billing. 'Electronic communications network' is defined in Directive 2002/21 as a common regulatory framework for electronic communications, networks and services: see Article 2 PECD.

processing was considered so important for the internal market. In the context of what is being considered in this case, a Hungarian resident may receive a call from a German resident, which will then form part of the Hungarian resident's data, that may (must) be retained. Or a Hungarian resident may search a German internet site or travel to France and send a SMS message. Again that data will be retained as 'his' data. However, the data relating to these communications are cross-border data; they give rise to rights not only for persons in Hungary but also for those outside Hungary. One person's data is also likely to be that of another. A German resident needs to be sure that when contacting a Hungarian resident, his data rights will be fully protected. This Court is obliged therefore to consider the legality of the relevant provisions on the basis of their inter-state effects; this is not a purely domestic matter.

11. Further, as the CJEU made clear in *DRI*, the DPD and PECD essentially concern three inter-related but distinct aspects of a retention regime: (a) the *retention* of data (including on a mass scale); (b) the *access* regime for such data; and (c) the *storage* and potential *transfer* of such data, including outside the EU. Whilst as explained below, the 'retention' on its own gives rise to very serious issues irrespective of the risk of access/disclosure, it is nevertheless necessary for the Court to consider retention in the light of the existing access/storage regimes.

Derogations from the data protection principles

12. By Article 15 of the PECD, Member States can exceptionally restrict the rights set out in Articles 5, 6, 8(1)-(4) and 9 when "*necessary, appropriate and proportionate [...] to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection 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 Party⁹, set up under Article 29 of the DPD as an independent European advisory body on data protection and privacy, stated in its Opinion 5/2002¹⁰ (at p.3) that the:

"...retention of traffic data for purposes of law enforcement should meet strict conditions under Article 15 (1): i.e. in each case only for a limited period and where necessary, appropriate and proportionate in a democratic society. Where

⁹ Article 29 of the DPD provided for the establishment of this Working Group.

¹⁰ Concerning the precursor to the DRD (Draft Council Framework Decision, Doc 8958/04), and available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp64_en.pdf.

traffic data are to be retained in specific cases, there must therefore be a demonstrable need, the period of retention must be as short as possible and the practice must be clearly regulated by law, in a way that provides sufficient safeguards against unlawful access and any other abuse. Systematic retention of all kinds of traffic data for a period of one year or more would be clearly disproportionate and therefore unacceptable in any case." (emphasis added)

13. That statement reflects the settled case-law of the CJEU that the protection of the fundamental right to privacy requires that derogations and limitations in relation to the protection of personal data can be adopted and applied only in so far as is strictly necessary: Case C-473/12, *Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert*, (7 November 2013) (ECLI:EU:C:2013:715), §39, citing Case C-73/07 *Satakunnan Markkinapörssi and Satamedia* [2008] ECR I-9831 (ECLI:EU:C:2008:727), §56, and Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063 (ECLI:EU:C:2010:662), §§77 and 86.
14. Derogations from data protection rights under Article 13 of the DPD or Article 15 of the PECD can only be invoked by a Member State where it can establish that such exceptions are strictly necessary: see Case C-275/06 *Promusicae* [2008] ECR I-271 (ECLI:EU:C:2008:54) and *IPI* (cited above). Further, when invoked, any derogation must comply with the general principles of Union law, including those mentioned in Article 6(1) and (3) of the Treaty on European Union (TEU), which refer to respect for fundamental rights and freedoms laid down in the CFR and the ECHR. As the Court stated at paragraph 70 in *Promusicae*:
- "...Member States must, when transposing the directives mentioned above, take care to rely on an interpretation of the directives which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order. Further, when implementing the measures transposing those directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality (see, to that effect, Lindqvist, paragraph 87, and Case C-305/05 *Ordre des barreaux francophones et germanophone and Others* [2007] ECR I-0000, paragraph 28)." (emphasis added)
15. Accordingly, following the adoption of the PECD, there was necessarily disagreement between Member States as to whether the requirements of Article 13 DPD and 15 PECD could be met, that is, whether retention of communications data could be justified under

those exceptional provisions. Accordingly, Member States adopted a further Directive, the DRD, as a means of requiring Member States to oblige communications providers to retain data and provide state access to it. The DRD did not purport to comply with the strict requirements of Article 15 of the PECD and indeed was specifically adopted to derogate from Articles 5, 6 and 9 of the PECD: (Article 3 DRD). Further it amended the PECD so as to disapply the strict exception requirements of Article 15 in relation to that data: Article 15(1a) PECD (Article 11 DRD). As AG Cruz Villalón stated in his opinion of 12 December 2013 in *DRI* it “derogate[d] from the derogating rules which are laid down in Article 15(1) of [the PECD]” (§39).

The CFR

16. Article 51 of the CFR states that it is binding on States when they are “implementing EU law”. This formulation is to be interpreted broadly and, in effect, means whenever a Member State is acting “within the material scope of EU law”¹¹. The “scope” of EU law must also be understood widely¹², and “some of the points to be determined are whether that legislation is intended to implement a provision of EU law; the nature of that legislation and whether it pursues objectives other than those covered by EU law, even if it is capable of indirectly affecting EU law; and also whether there are specific rules of EU law on the matter or capable of affecting it”¹³. The legislation at issue clearly falls within the scope of EU law in light of the DPD/PECD and the purpose of the Hungarian Act – to implement the DRD.
17. The CFR provides for two rights which are affected by legislation such as that under examination:

“Article 7

Respect for private and family life

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

Article 8

Protection of personal data

¹¹ See the Explanations Relating to the Charter of Fundamental Rights (2007/C 303/02) OJ 2007 C303/17 (“the Explanations”), p.32.

¹² Case C-617/10 *Åklagaren v Hans Åkerberg Fransson* (26 Feb 2013) (ECLI:EU:C:2013:105), at §§25- 26.

¹³ Case C-206/13 *Cruciano Siragusa v Regione Sicilia – Soprintendenza Beni Culturali e Ambientali di Palermo* (ECLI:EU:C:2014:126) at §25.

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority."

18. As the Explanations¹⁴ set out (at p.20), Article 7 CFR corresponds to Article 8 ECHR, and Article 8 CFR corresponds closely to the rights protected under the DPD.

Proportionality

19. The co-interveners note that the claimant's submissions on the constitutionality of Article 159/A of the Electronic Communications Act, and the reasons given by the first instance judge for requesting the opinion of this Court on the lawfulness of that Article, emphasise the requirement for any interference with the fundamental rights protected by the Hungarian Fundamental Law to comply with the requirements of proportionality laid down in Article I(3) of the Hungarian Fundamental Law. The co-interveners emphasise that the requirements of proportionality in EU law and under the ECHR for any interference in fundamental rights and freedoms entail similar considerations. In particular, Article 52(1) CFR provides that "*Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.*" As the Explanation of Article 52(1) CFR states:

The wording [of Article 52(1)] is based on the case-law of the Court of Justice: '... it is well established in the case-law of the Court that restrictions may be imposed on the exercise of fundamental rights, in particular in the context of a common organisation of the market, provided that those restrictions in fact correspond to objectives of general interest pursued by the Community and do not constitute, with regard to the aim pursued, disproportionate and unreasonable interference undermining the very substance of those rights' (judgment of 13 April 2000, Case C-292/97, paragraph 45 of the grounds).

¹⁴ Article 6(1) TEU states that "The rights, freedoms and principles in the Charter shall be interpreted ...with due regard to the explanations referred to in the Charter, that set out the sources of those provisions."

20. For the reasons explained in more detail in Section IV below, the co-interveners agree that for the reasons given by the claimant at §13 of her submissions, and in the judgment of the first instance judge, the provisions of Article 159/A of the Electronic Communications Act do not comply with the requirements of proportionality and submit that for the same reasons that Article is incompatible with both EU law and the ECHR.

III. The importance of metadata/communications data

21. The co-interveners understand that Article 159A of the Electronic Communications Act requires service providers such as the Defendant to retain a wide range of data arising from the use of fixed line and mobile telephones, internet access, internet e-mail and internet telephony by subscribers. It is understood that this includes personal data about the subscriber or user; the supply address and type of equipment used by the subscriber (in the case of fixed line telephony or fixed location internet access); data capable of identifying the parties to any communication including the IMEI and IMSI of the calling party and the receiving party of any communication; the date, start and end time of the communication or use of internet, email or internet telephony; intermediate subscriber/user numbers to which calls are routed through a call forwarding or transfer service; cell site information capable of identifying the geographical location from which a mobile telephone call is made; the date, time and location of any use of pre-paid anonymous services. This data is referred to in these submissions as 'metadata'.
22. In the co-interveners' submission, the range of metadata caught by the legislation is incredibly wide, and potentially affects different persons, locations and a variety of equipment which may be carrying communications. A wide range of European and International institutions have recently emphasised the importance of metadata and the breadth of the uses to which it may be put if intercepted and retained by public authorities and/or telecommunications providers.
23. Advocate General Cruz Villalón noted, in his Opinion in *DRI*, that the collection of metadata includes a wide range of information which enables a detailed picture to be painted of an individual's activities, beliefs and relationships to others (see §74). The CJEU in *DRI* stressed that:
- "[26] [...] the data [...] include data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to identify the

location of mobile communication equipment, data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services. Those data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.

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

24. As the Claimant points out in her submissions (§4), the data which Article 159A of the Electronic Communications Act requires the Defendant and other service providers to retain is precisely of this nature.

25. Both the Advocate General and the CJEU referred to the fact that the mere knowledge that all of one's data is being retained is sufficient to potentially change individuals' behaviour and communication, as this creates "*the vague feeling of surveillance*" (AG at §§52 and 72).¹⁵

26. On 10 April 2014, the Article 29 Working Party published its "*Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes*".¹⁶ The Working Party recognised that metadata can be even more revealing than content data:

"It is also particularly important to note that metadata often yield information more easily than the actual contents of our communications do. 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."

¹⁵ The German Constitutional Court has referred to this as the "*diffusely threatening feeling of being watched*", Judgment of 02 March 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, see <https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html>.

¹⁶ The Opinion is available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf.

27. The Working Party went on to explain that such metadata is 'personal data' for the purposes of EU law because it falls within the definition in Article 2(a) of the DPD, which defines personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly" (at p.5).
28. Similarly, on 30 June 2014 the Office of the UN High Commissioner for Human Rights ("UNHCHR"), published a report in which it stressed that the distinction between the seriousness of interception of metadata and content is "*not persuasive*" and "*any capture of communications data is potentially an interference with privacy [...] whether or not those data are subsequently consulted or used*". In particular, it was emphasised that "[t]he 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 [sic] beyond even that conveyed by accessing the content of a private communication" (at §19).
29. Indeed, like the AG and CJEU in *DRI*, the UNHCHR considered that the mere fact of such capture may have a "*potential chilling effect on rights, including those to free expression and association*"¹⁷. The UNHCHR concluded that "[m]andatory third-party data retention [...] appears neither necessary nor proportionate" (§26, p.9).
30. The UN Special Rapporteur on the promotion and protection of human rights while countering terrorism shared this view. In his fourth annual report¹⁸ he noted that "[t]he communications of literally every Internet user are potentially open for inspection by intelligence and law enforcement agencies in the States concerned. This amounts to a systematic interference with the right to respect for the privacy of communications, and requires a correspondingly compelling justification" (§9, p.4). The Special Rapporteur concluded that "[t]he hard truth is that the use of mass surveillance technology effectively does away with the right to privacy of communications on the Internet altogether" (§12, p.5). In short, "mass surveillance of digital content and communications data presents a serious challenge to an established norm of international law" (§18, p.7).

¹⁷ *Supra* n.1, pp.6-7 at §§19-20. See also "*Surveillance of Emergent Associations: Freedom of Association in a Network Society*", K. J. Strandburg, December 2007 at p.1, available at http://works.bepress.com/katherine_strandburg/11.

¹⁸ Dated 23 September 2014 (A/69/397), this is available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement>.

31. Similarly, on 18 December 2014, the United Nations' General Assembly passed a resolution which emphasised that "*certain types of metadata, when aggregated, can reveal personal information and can give an insight into an individual's behaviour, social relationships, private preferences and identity*" (preamble paragraph 14, p.2).¹⁹

32. In December 2014, the Council of Europe's Commissioner for Human Rights ("the Commissioner") published an Issues paper²⁰ in which he recommended that (p.22):

"6. Suspicionless mass retention of communications data is fundamentally contrary to the rule of law, incompatible with core data-protection principles and ineffective. Member states should not resort to it or impose compulsory retention of data by third parties."

33. In particular, the Commissioner stressed that "[t]his 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" (p.115). The Commissioner expressed concern that "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" (ibid.). He also stressed that metadata can be "unreliable and can unwittingly lead to discrimination on Application 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).

IV. The Requirements of EU law and their application to the legislation in issue

A. Exceptions to the Directives must be narrowly construed;

34. In *DRI*, the CJEU reiterated that provisions governing data processing and retention - liable to infringe fundamental freedoms in particular the right to privacy - "must necessarily be interpreted in the light of fundamental rights" (at §68). In construing Article 15

¹⁹ Resolution A/RES/69/166, available at http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/69/166. See also UN Human Rights Council Resolution A/HRC/RES/28/16, preamble paragraph 15, adopted on 26 March 2015.

²⁰ "The rule of law on the internet and in the wider digital world", <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2654047&SecMode=1&DocId=2216804&Usage=2>

and deciding whether the relevant provisions comply with it, the Court must ensure protection for individual rights under Articles 7 and 8 CFR and Article 8 ECHR: Case C-390/12 *Pfleger and ors* (30 April 2014) (ECLI:EU:C:2014:281) at §36.

35. Further, as noted above, the Court must interpret the exceptions in Article 15 PECD strictly (see also Case C-119/12 *Josef Probst v mr.nexnet GmbH* (22 November 2012) (ECLI:EU:C:2012:748), at §23). In other words, the relevant provisions must go no further than is strictly necessary to achieve the relevant purpose.

B. Substantive requirements applied to the Hungarian legislation:

36. Firstly, for *inter alia* all the reasons set out by the claimant in respect of the incompatibility of the provisions with the rights to privacy and data protection in the Hungarian Fundamental Law, the relevant provisions do not comply with Articles 7 and 8 CFR or Article 8 ECHR, which they must do in order to meet the requirements of Article 15 PECD and EU law generally.

37. Secondly, Article 159/A was inserted into the Electronic Communications Act by Article 13 of Act 174 of 2007 on the amendment of Act 100 of 2003 on Electronic Communications, which was adopted with the objective of transposing into Hungarian law the DRD (see Article 18(2)(c) of Act 174 of 2007). It is notable that the requirements of Article 159/A essentially duplicate those laid down in the DRD as respects (i) the categories of data to be retained, including the requirement to retain data about unsuccessful calls (Article 5 DRD) and (ii) the purposes for which it is to be retained (to enable access by law enforcement agencies and the national security service). The DRD was declared unlawful by the CJEU in *DRI* such that the provisions of Article 159/A necessarily also fall to be declared unlawful (as noted by the Commissioner, considered below).

38. The claimant emphasises the importance of access and the inter-relationship between *retention, access and storage of data*. The co-intervenors also wish to emphasise that, as the CJEU made clear in *DRI*, data interception and retention in itself gives rise to a very serious interference with fundamental rights, irrespective of whether access is subsequently sought or indeed could be subsequently sought. This is because the very fact of retention is likely to affect individuals' sense of freedom and impact directly on

private behaviour. As the AG and CJEU noted in *DRI*, knowledge that all one's data is being retained is likely to alter how individuals behave and communicate and create a sense of being subject to surveillance that potentially has profound implications for individual freedom within the private sphere.²¹ This is so whether or not there is a true or realistic risk that that data will ever be accessed. What matters is the fact of retention; it is this that potentially affects private behaviour and thus interferes with private life.

39. The AG in *DRI* considered the interference that retention involved to be "*particularly serious*": §70 and the CJEU considered it potentially so great that it could in fact have an effect on the use of communications and consequently on freedom of expression: §§27-28.
40. The Council of Europe's Commissioner 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 most 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).
41. The co-intervenors submit that the retention of vast swathes of metadata, including in relation to persons for whom there is no suspicion of criminal behaviour or that they pose a threat to national security, is a serious interference with Articles 7 and 8 CFR and Article 8 ECHR. Indeed, the requirements of Article 159A of the Electronic Communications Act potentially entail "*an interference with the fundamental rights of practically the entire European population*" and certainly the entire Hungarian population given that they relate to any "*communications data*" as defined by the Act.
42. Thirdly, the co-intervenors understand that the Hungarian legal provisions concerned contain no safeguards which might enable persons whose data have been retained to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data, which the CJEU in *DRI* considered to be a mandatory

²¹ See, for instance, ORG's report "*Digital Surveillance - Why the Snoopers' Charter is the wrong approach: A call for targeted and accountable investigatory powers*" available at <https://www.openrightsgroup.org/assets/files/pdfs/reports/digital-surveillance.pdf>. See further the Witness statement of Edward W. Felten (Director of the Center for Information Technology Policy, Princeton University) in *ACLU v James R. Clapper & others* on the sensitive nature of metadata: <https://www.aclu.org/files/pdfs/natsec/clapper/2013.08.26%20ACLU%20PI%20Brief%20-%20Declaration%20-%20Felten.pdf>.

requirement for lawful derogation from the obligation laid down in Article 8(1) CFR (§53-55 of its judgment).

43. Fourthly, the blanket nature of the data retention obligation (which appears to apply to *all* electronic communications providers and to *all* subscribers and service users) is such that it cannot meet the criticisms of the CJEU in *DRI*. The obligation under Article 159/A of the Electronic Communications Act does not lay down the clear and precise rules that the CJEU has said are needed to govern the scope and application of the measure in question and to impose minimum safeguards: §§54-55, 65 *DRI*. In particular, there is nothing in the relevant provisions capable of complying with the need for any data retention obligation:

- a. to be person- or crime- specific. Indeed there is no obligation on the service providers to satisfy themselves that there is any connection (even indirect) between the person whose data is being collected and a situation which is liable to give rise to criminal prosecutions. The blanket nature of the data retention obligation is such that it must necessarily capture the data of persons for whom there is no evidence capable of suggesting their conduct might have a link, even an indirect or remote one, with a serious crime, which the Court explicitly criticised: §58 - 59 *DRI*. This breadth renders the relevant provisions arbitrary - "*it will not be enough that the measures are targeted to find certain needles in a 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*"²².
- b. to exclude persons whose communications are subject to professional secrecy obligations: §58 *ibid*;
- c. to be confined to the minimum period 'strictly necessary': §62 *ibid*. In particular, the retention of "*subscriber data*" (i.e. the data falling within Article 159/A (1)(a) to (c)) is authorised for up to 12 months after "*the termination of the subscriber contract*" (Article 159/A(3)). This could potentially be a very lengthy period - and it is

²² "*The right to privacy in the digital age*", *supra* n.1, §25 at p.9.

entirely unclear why a period longer than 12 months is necessary (as noted by the AG at §149 of his Opinion in *DR1*). Indeed, the co-intervenors understand that in this case the Defendant relied upon the possibility for data to be retained for up to 3 years under the Electronic Communications Act. Moreover, in the case of other traffic data, Article 159/A (3) requires data to be retained systematically for 12 months after the origination of the communication (6 months in the case of unsuccessful calls) which, as the Article 29 Working Party stated in its Opinion 5/2002 (noted above), is "clearly disproportionate and therefore unacceptable".

V. Remedies for breaches of EU law

44. Article 19(1), §2 of the Treaty on European Union ("TEU") is a new provision inserted by the Lisbon Treaty which specifically states that "*Member States shall provide remedies sufficient to ensure effective legal protection in the fields covered by Union law*". This reflects the well-established principles of EU law that, as a facet of the principle of "*sincere cooperation*" between Member States and the EU (Article 4(3) TEU²³):

"detailed procedural rules governing actions for safeguarding an individual's rights under [Union] law must be no less favourable than those governing similar domestic actions (principle of equivalence) and must not render practically impossible or excessively difficult the exercise of rights conferred by [Union] law (principle of effectiveness)"²⁴.

45. Moreover, this requirement for effective remedies must be met by all courts in a Member State²⁵. Although national courts are not under an obligation to raise issues of EU law *ex officio*²⁶, they may do so where their national law allows this²⁷. The CJEU has also held that a party need not have relied upon EU law in order for the national court to do so²⁸.

²³ This provides, *inter alia*, that Member States must "*take any appropriate measure, general or particular, to ensure fulfilment of the obligations arising out of the Treaties or resulting from the acts of the institutions of the Union*" (§2).

²⁴ See the judgment of the Grand Chamber in Case C-432/05 *Unibet (London) Ltd and Unibet (International) Ltd v Justitiekanslern* [2007] ECR I-2271 (ECLI:EU:C:2007:163) at §43.

²⁵ Case 106/77 *Amministrazione delle Finanze dello Stato v Simmenthal SpA* [1978] ECR 629 (ECLI:EU:C:1978:49) at §§16 and 21.

²⁶ Joined Cases C-222/05 to C-225/05 *van der Weerd* [2007] ECR I-4233 (ECLI:EU:C:2007:318) at §§34-38 and 41.

46. Finally, a failure by the highest court of a Member State to correctly apply EU law to a case before it, including by deciding not to send a preliminary reference to the CJEU, may lead to the liability of that State, where loss has been suffered by a party²⁹.
47. In those circumstances, the co-interveners would respectfully submit that when faced with a *clear* case insofar as the requirements of EU law are concerned, such as the one before the Constitutional Court, it is necessary for a Member State's highest court to (a) examine the EU law issues raised by the proceedings (unless national law precludes this) and (b) to provide the affected party with an effective remedy for any breach of EU law.
48. The co-interveners understand that by virtue of Article 24(2)(f) of the Hungarian Fundamental Law, the Constitutional Court is required to examine any legal regulation for conflict with any international treaty and that by Article 24(3)(c) it is empowered to annul any legal regulation which is in conflict with an international treaty. Section 32(1) of Act CLI of 2011 on the Constitutional Court empowers the Court to consider the compatibility of a law with an international treaty of its own motion as well as on request. They further note that Article E(3) of the Fundamental Law allows for EU law to lay down generally binding rules of conduct as a matter of Hungarian law and that Article Q(2) requires Hungarian law to be compatible with international law. It therefore appears that the rules of national law not only do not preclude the national court from considering the compatibility of a regulation with EU law but require the Constitutional Court to do so.
49. This case is clear because:
- 49.1. The Hungarian legislation at issue was specifically introduced in order to give effect to Hungary's obligations under the DRD. It was therefore an act of a Member State implementing EU law;

²⁷ See, e.g. Joined Cases C-87 to C-89/90 *Verholen and Others v Sociale Verzekeringsbank Amsterdam* [1991] ECR I-03757 (ECLI:EU:C:1991:314) at §§13; Lenaerts, Maselis and Gutman, *EU Procedural Law*, OUP, 2015, p.131 at 4-39.

²⁸ See, for instance in the Case C-2/06 *Willy Kempter KG v Hauptzollamt Hamburg-Jonas* [2008] ECR I-411 (ECLI:EU:C:2008:78) at §§44 and 46.

²⁹ Case C-224/01 *Gerhard Köbler v Republik Österreich* [2003] ECR I-10239 (ECLI:EU:C:2003:513) at §36.

49.2. The CJEU has given clear recent guidance as to the requirements for legislation governing data retention, in order for it to be compatible with the fundamental rights engaged. There is no apparent distinguishing feature between the legislation at issue and the DRD to suggest that the CJEU's guidance in *DRI* is not compelling. The finding of the CJEU in *DRI* that the DRD is incompatible with EU law has the consequence that Article 159/A of the Electronic Communications Act is also incompatible with EU law.

VI. Conclusion

50. The co-interveners respectfully submit that this Court should hold that the obligation contained in Article 159/A of the Electronic Communications Act is not only contrary to the Hungarian Fundamental Law but is a violation of EU law for the reasons set out above. In the circumstances, the Court should declare that Article 159/A is invalid and strike it down.
51. In the co-interveners' view, the matters before the Court are *acte clair*, i.e. they should be determined without the Court needing to refer the matter to the CJEU, given that the *DRI* judgment is clear as to the requirements with which legislation governing data retention must comply. In other words "[t]he correct application of [EU] law [is] so obvious as to leave no scope for any reasonable doubt as to the manner in which the question raised is to be resolved" (Case 283/81, *CILFIT Srl v Ministero della Sanità* [1982] ECR 3415 (ECLI:EU:C:1982:335) at §16). Before reaching this conclusion, "the national court [...] must be convinced that the matter is equally obvious to the courts of the other member-States and to the Court of Justice".
52. The relevant provisions do not sufficiently address the serious concerns identified therein and would therefore fall foul of the *DRI* test. As to the other Member States, the co-interveners have initiated research into the response to the *DRI* judgment in other Member States of the Union³⁰ and refer the Court to other existing analysis of the comparative position³¹. It is instructive to note that similar legislation has been struck

³⁰ Available at: <https://www.openrightsgroup.org/blog/2015/status-of-data-retention-in-the-eu-following-the-cjeu-ruling-update-april-2015>

³¹ See, e.g. "Data Retention after the Judgement of the Court of Justice of the European Union", Boehm & Cole, Münster/Luxembourg, 30 June 2014, available at

down by the highest administrative and constitutional courts in Germany, Bulgaria, Romania, Cyprus, the Czech Republic, Slovenia without any need for a reference to the CJEU. Other proceedings are ongoing. In particular, the Austrian decision (27 June 2014) upon return of the preliminary ruling in *DRI* is a recent example of the application of *DRI* to national implementing legislation finding breaches of the CFR and ECHR. A lower Dutch court has also come to a similar conclusion. Other Member States have indicated their intention to enact new legislation revising their data retention regimes. Accordingly, the position is *acte clair* and the relevant provisions should be disapplied.

53. To the extent that the Court retains doubts as to the compatibility of the relevant provisions *with the DRI principles*, however, then it would be appropriate for the matter to be referred to the CJEU to clarify how the *DRI* requirements apply outside the context of the DRD, and within the scope of Article 15 PECD. Indeed, in case of such doubt, the co-interveners submit that the Court would be bound to refer the matter to the CJEU as “*a decision on the question is necessary to enable it to give judgment*” (per Article 267 TFEU) and the Constitutional Court is the last instance in the Hungarian legal system.

8 April 2015

Acting *pro bono*

JESSICA SIMOR QC

Matrix Chambers

ALISON PICKUP

Doughty Street Chambers

RAVI S. MEHTA

Blackstone Chambers

Case ref: III/537/2015

IN THE HUNGARIAN CONSTITUTIONAL COURT
BETWEEN:

DALMA DOJCSAK

Claimant

- and -

TELENOR MAGYARORSZÁG ZRT

Defendant

- and -

(1) OPEN RIGHTS GROUP

(2) PRIVACY INTERNATIONAL

Co-Interveners

AMICUS CURIAE SUBMISSIONS OF
THE CO-INTERVENERS

Elizabeth Knight
Legal Director
Open Rights Group
+44 (0) 20 7096 1079
www.openrightsgroup.org

Tomaso Falchetta
Legal Officer
Privacy International
www.privacyinternational.org

Solicitors to the co-interveners