IN THE EUROPEAN COURT OF HUMAN RIGHTS **App No 58170/13**

BETWEEN:

BIG BROTHER WATCH & ORS - v - THE UNITED KINGDOM

WRITTEN OBSERVATIONS OF EUROPEAN NETWORK OF NATIONAL HUMAN RIGHTS INSTITUTIONS

INTRODUCTION

1. On 15 December 2015 the European Court of Human Rights ('the ECtHR') granted liberty to the European Network of National Human Rights Institutions ('ENNHRI') to intervene in this Application in the form of written submissions in accordance with Article 36(2) of the European Convention on Human Rights ('the ECHR') and Rule 44(3) of the Rules of Court.

2. ENNHRI is a registered association representing National Human Rights Institutions ('NHRIs') within the Council of Europe region. ENNHRI membership currently comprises thirty nine NHRIs from thirty five countries across Europe of whom thirty six are accredited with "A" or "B" status under the United Nations ('UN') "Paris Principles"[1]. As NHRIs, ENNHRI members are bodies or institutions separate from both government and civil society organisations with a broad constitutional or legal mandate to promote and protect human rights.

3. Many NHRIs have, as part of their statutory functions, the ability to appear as amicus curiae in human rights cases before their national courts, or indeed before international and regional courts or tribunals, in cases concerning constitutional and international human rights convention provisions. In this capacity NHRIs may regularly appear before the ECtHR as a neutral party providing expertise on human rights matters which the parties may not put before the Court.

4. In these submissions ENNHRI addresses the significance of substantive international human rights standards relevant to:

    a. The issue of exhaustion of domestic judicial remedies, and whether the international legal framework supports the contention that domestic remedies do not have to be followed if they are not capable of providing an effective remedy; and

    b. The protection of privacy as enshrined in international standards relevant to the issues of "in accordance with the law" and "necessary in a democratic society" within the meaning of Article 8(2) ECHR.

5. These submissions do not address the facts or merits of the case.

6. It is established that, in interpreting ECHR provisions and the scope of the States' obligations in specific cases, the ECtHR will look "*for any consensus and common values emerging from the practices of*

[1] These principles were adopted by the UN General Assembly in Resolution 48/134 of 20 December 1993, and set out objective criteria against which NHRIs are tested for their independence, pluralism, impartiality and accountability.

European States and specialised international instruments… as well as giving heed to the evolution of norms and principles in international law."[2]

ISSUE 1: Exhaustion of domestic remedies

7. International law principles are of assistance when the ECtHR approaches the question of exhaustion of domestic remedies. Indeed, the Court's Practical Guide on Admissibility Criteria (Jan 2014) at §75 provides:

> 75. *According to the "generally recognised rules of international law", there may be special circumstances dispensing the applicant from the obligation to avail him or herself of the domestic remedies available.*[3]

8. The requirement to exhaust domestic remedies is common to the rights of individual petition under all major human rights treaties, including the International Covenant on Civil and Political Rights ('ICCPR') and the American Convention on Human Rights ('ACHR'):

   a. Article 5(2)(b) of the Optional Protocol to the ICCPR states in relevant part:

   > *2. The Committee shall not consider any communication from an individual unless it has ascertained that: … (b) The individual has exhausted all available domestic remedies. This shall not be the rule where the application of the remedies is unreasonably prolonged.*

   b. Article 46 ACHR provides in relevant part:

   > *1. Admission by the Commission of a petition or communication lodged in accordance with Articles 44 or 45 shall be subject to the following requirements:*
   >
   > *a. that the remedies under domestic law have been pursued and exhausted in accordance with generally recognized principles of international law; ...*
   >
   > *2. The provisions of paragraphs 1.a and 1.b of this article shall not be applicable when:*
   >
   > *a. the domestic legislation of the state concerned does not afford due process of law for the protection of the right or rights that have allegedly been violated;*
   >
   > *b. the party alleging violation of his rights has been denied access to the remedies under domestic law or has been prevented from exhausting them; or*
   >
   > *c. there has been unwarranted delay in rendering a final judgment under the aforementioned remedies.*

[2] Opuz v Turkey, 33401/02, Eur. Ct. H.R., para. 164 (2009).

[3] See also the ECtHR's Practical Guide on Admissibility Criteria, §60: "*As the text of Article 35 itself indicates, this requirement [of exhaustion of domestic remedies] is based on the generally recognised rules of international law. The obligation to exhaust domestic remedies forms part of customary international law, recognised as such in the case-law of the International Court of Justice (for example, see the case of Interhandel (Switzerland v The United States), judgment of 21 March 1959). It is also to be found in other international human-rights treaties: the International Covenant on Civil and Political Rights (Article 41(1)(c)) and the Optional Protocol thereto (Articles 2 and 5(2)(b)); the American Convention on Human Rights (Article 46); and the African Charter on Human and Peoples' Rights (Articles 50 and 56(5))*".

9. As each of these provisions recognises, the rule derives from the general principles of international law. These include principles from the diplomatic protection sphere.[4] Article 15 of the International Law Commission ('ILC') Draft Articles on Diplomatic Protection (2006) sought to codify the established exceptions to the rule of exhaustion, and form a useful background to the consideration of the specific application of the rule in the human rights field. Article 15 and its associated commentary state in relevant part (emphasis added):

> ***Article 15:***
>
> *Local remedies do not need to be exhausted where: (a) There are no reasonably available local remedies to provide effective redress, or the local remedies provide no reasonable possibility of such redress; ...*
>
> ***Commentary:***
>
> *… In this form the test* [in Article 15(a)] *is supported by judicial decisions which have held that local remedies need not be exhausted where the local court has no jurisdiction over the dispute in question; the national legislation justifying the acts of which the alien complains will not be reviewed by local courts; ... the local courts do not have the competence to grant an appropriate and adequate remedy to the alien;* ..(emphasis added)

10. In support of the pertinent underlined assertion, the ILC cites a number of authorities from a range of jurisdictions, including inter-state arbitration,[5] the Inter-American Court of Human Rights ('IACtHR'),[6] and the ECtHR.[7]

11. Turning to the specific application of the rule in the international human rights sphere, the ACHR provisions contain the most detailed description in any major human rights treaty of what type of domestic remedies must be exhausted, much of which is reflected and built on in the case law of the ICCPR's Human Rights Committee ('HRC') and the IACtHR.

12. Particularly relevant are the following points:

    a. A remedy which does not offer *"a reasonable prospect of redress"* need not be exhausted: see the Human Rights Committee (HRC) decision in *Patiño v Panama*.[8]

---

[4] See, for example, the decision of the ICJ in the *Interhandel Case (Switzerland v United States),* Preliminary Objections, Judgment, ICJ GL No 34, [1959] ICJ Rep 6, at p. 27: *"The rule that local remedies must be exhausted before international proceedings may be instituted is a well-established rule of customary international law."*

[5] *Claim of Finnish Shipowners against Great Britain in respect of the Use of Certain Finnish Vessels During the War,* 1934, UNRIAA, vol. III, p. 1479 at pp. 1496-1497.

[6] *Velásquez Rodríguez Case*, IACtHR, (Ser. C) No. 4 (1988), where it was held in the context of a disappearance case, that *"A remedy must also be effective - that is, capable of producing the result for which it was designed. Procedural requirements can make the remedy of habeas corpus ineffective: if it is powerless to compel the authorities;*." (§66, emphasis added).

[7] *Yağci and Sargin v Turkey*, Judgment of 8 June 1995, *European Court of Human Rights, Reports and Decisions*, No. 319, p. 3 at p. 17, para. 42; *Hornsby v Greece*, Judgment of 19 March 1997, *European Court of Human Rights, Reports and Decisions*, 1997-11, No. 33, p. 495 at p. 509, para. 37.

[8] Communication No. 437/1990, U.N. Doc. CCPR/C/52/D/437/1990 (1994), §5.2. See also, *Thompson v Panama*, Communication No. 438/1990, U.N. Doc. CCPR/C/52/D/438/1990 (1994), §5.2, which refers to a "*reasonable prospect of success"*. c.f. the ECtHR's Practical Guide on Admissibility Criteria (Jan 2014) at §§76, 81: *"The remedy must be capable of providing redress in respect of the applicant's complaints and of offering reasonable prospects of success"* …

b. Where a remedy could involve a finding in principle in the individual's favour, but would not have binding effect, it is not an effective remedy which needs to be exhausted: see the HRC decision in *C v Australia*.[9]

c. Where primary legislation effectively ousts substantive judicial review and limits the role of the domestic court to a formal determination that cannot result in a substantive remedy, there is no available remedy which needs to be exhausted: see again the HRC decision in *C v Australia.*[10]

d. In order for domestic proceedings to be an available and effective remedy, "*procedural guarantees for 'a fair and public hearing by a competent, independent and impartial tribunal' must be scrupulously observed"*: see the decision of the HRC in *Gilboa v Uruguay*.[11] This principle is similarly reflected in the language of the ACHR and the case law of the IACtHR:

i. A remedy will not need to be exhausted where the domestic legislation does not afford *"due process of law"*: see Article 46(2)(a) ACHR:

ii. "*Due process of law*" is to be determined with reference to the fair trial guarantees otherwise provided for in the relevant treaty: see the Advisory Opinion of the IACtHR in *Exceptions to the Exhaustion of Domestic Remedies*.**[12]** The IACtHR explained that a remedy which did not comply with the fair trial guarantees of Article 8 ACHR was not a remedy which needed to be exhausted under Article 46.

13. In summary, the international legal framework, including the ICCPR, ACHR and case law supports the contention that domestic remedies do not have to be followed if they are not capable of providing an effective remedy.

ISSUE 2: Substantive Article 8(2) issues

14. The issues arising on the Application include whether the United Kingdom's conduct is:

a. In accordance with the law (has a basis in domestic law, is compatible with the rule of law, is accessible and foreseeable);

b. Necessary in a democratic society in pursuit of a legitimate aim (proportionality).

International and EU law analysis

15. The rights to privacy and to the protection of personal data providing for the protection of communication against interferences or attacks which are contrary to the rule of law are firmly rooted in international and EU law.

"*where a suggested remedy did not in fact offer reasonable prospects of success, for example in the light of settled domestic case-law, the fact that the applicant did not use it is no bar to admissibility.*"

[9] Communication No. 900/1999, U.N. Doc CCPR/C/76/D/900/1999 (2002), §7.3.

[10] Ibid., §7.4.

[11] Communication No. 147/1983, U.N. Doc. CCPR/C/OP/2 at 176 (1990), §7.2.

[12] *Exceptions to the Exhaustion of Domestic Remedies (Arts. 46(1), 46(2)(a) and 46 (2)(b) of the American Convention on Human Rights),* Advisory Opinion OC-11/90, August 10, 1990, IACtHR (Ser. A) No. 11 (1990), at §§19-31.

16. Most relevant, Article 17 of the ICCPR provides that *"(1) No one shall be subjected to arbitrary or unlawful interference with his privacy ... or correspondence … (2) Everyone has the right to the protection of the law against such interference or attacks."*

17. These provisions are mirrored in several other international and regional human rights instruments, namely by Article 16 of the Convention on the Rights of the Child ('CRC'), Article 14 of the Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families ('ICRMW'), Article 22 of the Convention on the Rights of Persons with Disabilities ('CRPD'), Article 11 of the American Convention on Human Rights, Article 21 of the Arab Charter on Human Rights and Article 21 of the non-binding ASEAN Human Rights Declaration.

18. Moreover, the rights to privacy and family life and to the protection of personal data, are explicitly guaranteed in Articles 7 and 8 respectively of the EU Charter of Fundamental Rights (see Annex A), which have generated abundant case law from the Court of Justice of the European Union ('CJEU').[13]

Scope

19. International instruments adopted more recently explicitly include "*other communications"* (Article 14 ICRMW) and *"other types of communication"* (Article 22 CRPD) under the right to privacy, thus responding to the new electronic and digital modes of exchanging information which have emerged in recent decades beyond traditional written correspondence. In relation to Article 17 ICCPR these new modes of communication have been addressed by the HRC in its General Comment No. 16. [14]

20. Metadata (or 'communications data') may fall under the scope of privacy protection as affirmed by reports of the Office of the UN High Commissioner for Human Rights ('OHCHR') and two Special Procedures mandated by the UN Human Rights Council ('HRC').[15] Subsequently, their views have been endorsed by the UN General Assembly in December 2014. [16]

Requirements under Article 17 ICCPR according to the HRC

21. The HRC states in General Comment No. 16 (Article 17, 1988): *"competent public authorities should only be able to call for such information relating to an individual's private life the knowledge of which is essential in the interests of society as understood under the Covenant"* [17] and elaborates further: *"Even with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such*

[13] Schecke & Eifert v Land Hessen, Joined Cases C-92/09 & C-93/09 [2010] ECR I-11063; Digital Rights Ireland & Seitlinger, Joined Cases C-293/12 & C-594/12 (ECLI:EU:C:2014:238); Google, Case C-131/12 (ECLI:EU:C:2014:317); Schrems v Data Protection Commissioner, Case C‑362/14 (ECLI:EU:C:2015:650).

[14] CCPR General Comment No. 16. Article 17 (Right to privacy). U.N. Doc. CCPR/GEC/6624 (1988).

[15] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. U.N. Doc. A/HRC/23/40 (2013), §15; The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights. U.N. Doc. A/HRC/27/37 (2014), §19; Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. U.N. Doc. A/69/397 (2014), §53.

[16] General Assembly Resolution 69/166, The right to privacy in the digital age. U.N. Doc. A/RES/69/166 (2014).

[17] CCPR General Comment No. 16. Article 17 (Right to privacy). U.N. Doc. CCPR/GEC/6624 (1988), §7.

authorized interference must be made only by the authority designated under the law, and on a case-by-case basis. …" [18]

22. Case law has reiterated that compliance with Article 17 requires any interference to be:[19]
    a. Provided for by law;
    b. In accordance with the provisions, aims and objectives of the ICCPR; and
    c. Reasonable in the particular circumstances of the case.

23. The last requirement – reasonableness – "*implies that any interference with privacy must be proportionate to the end sought, and must be necessary in the circumstances of any given case*."[20]

24. In the light of these requirements the HRC has issued Concluding Observations on surveillance practices of State Parties to the ICCPR that challenge a) the absence of specific legislation, b) the lack of clarity of existing legislation, c) the lack of effective oversight, d) the unavailability of redress mechanisms, or e) the failure to systematically inform persons who were wrongfully monitored and thereby ensure their access to adequate remedies.

25. Examples of such Concluding Observations are the ones in response to State reports by Jamaica in 1997,[21] Poland in 1999,[22] Hong Kong in 2006,[23] as well as the Republic of Korea in 2006, [24] Sweden in 2009,[25] and Bulgaria in 2011.[26]

26. In the past two years, the HRC affirmed and, in part, detailed its previously issued recommendations when reviewing the State Party reports by three members of the "Five Eyes" alliance, namely the United States, Canada and the United Kingdom, in 2014 and 2015.

27. In 2014, the Committee made detailed recommendations to the United States to take measures to ensure that its surveillance activities conform to Article 17 ICCPR including that any interference complies with the principles of legality, proportionality and necessity regardless of the nationality or location of the individuals affected and to provide for judicial involvement in the authorisation of surveillance (see Annex B). [27]

---

[18] Ibid. §8.

[19] *Van Hulst v Netherlands,* Communication No. 903/1999, U.N. Doc. CCPR/C/82/D/903/1999 (2004), §7.3. See also, *Toonen v Australia*, Communication No. 488/1992, U.N. Doc CCPR/C/50/D/488/1992 (1994), §8.3.

[20] *Toonen, ibid; Van Hulst, ibid,* §7.6.

[21] Consideration of reports submitted by State Parties under Article 40 of the Covenant. Concluding Observations of the Human Rights Committee - Jamaica. U.N. Doc. CCPR/C/79/Add.83 (1997), §20.

[22] Consideration of reports submitted by State Parties under Article 40 of the Covenant. Concluding Observations of the Human Rights Committee - Poland, U.N. Doc. CCPR/C/79/Add.110 (1999), §22.

[23] Consideration of reports submitted by States parties under article 40 of the Covenant. Concluding Observations of the Human Rights Committee - Hong Kong Special Administrative Region (HKSAR). U.N. Doc. CCPR/C/HKG/CO/2 (2006), §12.

[24] Consideration of reports submitted by States parties under article 40 of the Covenant. Concluding observations of the Human Rights Committee - Republic of Korea. U.N. Doc. CCPR/C/KOR/CO/3, (2006), §9.

[25] Consideration of reports submitted by States parties under article 40 of the Covenant. Concluding observations of the Human Rights Committee - Sweden. U.N. Doc. CCPR/C/SWE/CO/6 (2009), §18.

[26] Consideration of reports submitted by States parties under article 40 of the Covenant. Concluding observations of the Human Rights Committee - Bulgaria. CCPR/C/BGR/CO/3 (2011), § 22.

[27] Concluding observations on the fourth periodic report of the United States of America. U.N. Doc. CCPR/C/USA/CO/4 (2014), §22.

28. In 2015, the Committee recommended to Canada, in light of proposed amendments of the Canadian Security Intelligence Act *"potentially resulting in mass surveillance and targeting activities that are protected under the Covenant without sufficient and clear legal safeguards",* that it should:

> *"(d) establish oversight mechanisms over security and intelligence agencies that are effective and adequate, and provide them with appropriate powers as well as sufficient resources to carry out their mandate;*
>
> *(e) provide for judicial involvement in the authorization of surveillance measures …"*[28]

29. Most recently, in 2015, the HRC reviewed the State Party report of the United Kingdom of Great Britain and Northern Ireland. It expressed concern that the Regulation of Investigatory Powers Act 2000 provides for untargeted warrants for the interception of communications sent or received outside the United Kingdom without affording the same safeguards as apply to internal communications and the lack of safeguards in regard to receipt of private communications from foreign security agencies and the sharing of personal communications data with such agencies. It made a number of detailed recommendations including providing for judicial involvement in the authorisation of such measures in all cases and that legal provisions authorising such interference must be sufficiently precise, publicly accessible and provide effective safeguards against abuse (see Annex C). [29]

30. To summarise, the HRC has responded to the development of electronic and digital communication and its interception and surveillance by public authorities. To ensure conformity with Article 17 ICCPR the Committee considers necessary:

    a. Precise legislation avoiding terminology which could be open to wide interpretation and limiting the purpose of surveillance, its targets and duration;
    b. Judicial involvement in authorisation of surveillance;
    c. Robust systems of independent monitoring with the necessary guarantees of impartiality and effectiveness bolstered by appropriate powers and sufficient resources; and
    d. Access of affected persons to effective remedies in cases of abuse, among others by information thereof.

Other sources affirming the views of the HRC

31. In 2009 the then UN Special Rapporteur on human rights and counter-terrorism, Martin Scheinin,[30] prepared a report concerning the right to privacy, articulating concerns that the right was being eroded by counter-terrorism surveillance.[31] The Special Rapporteur took the view that Article 17 ICCPR should also be interpreted as containing *"elements of a permissible limitations test".* He drew comparison with permissible limitations to the right of freedom of movement under Article 12 ICCPR as explained by the HRC in General Comment No. 27 (Freedom of Movement, 1999)[32], which he described as codifying the

[28] Concluding observations on the sixth periodic report of Canada. U.N. Doc. CCPR/C/CAN/CO/6 (2015), §10.

[29] Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland. U.N. Doc. CCPR/C/GBR/CO/7 (2015), §24.

[30] Professor of International Law and Human Rights at the EUI, Florence; leader of the www.SURVEILLE.eui.eu project.

[31] *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, U.N. Doc. A/HRC/13/37 (2009).

[32] ICCPR General Comment No. 27: Article 12 (Freedom of Movement), U.N. Doc. CCPR/C/21/Rev.1/Add.9 (1999).

position of the Human Rights Committee on permissible limitations to the rights provided under the Covenant. The permissible limitations test, as expressed in the General Comment includes the following elements:

a. *Any restrictions must be provided by the law (paras. 11–12 [of General Comment No. 27]);*
b. *The essence of a human right is not subject to restrictions (para. 13);*
c. *Restrictions must be necessary in a democratic society (para. 11);*
d. *Any discretion exercised when implementing the restrictions must not be unfettered (para. 13);*
e. *For a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims; it must be necessary for reaching the legitimate aim (para. 14);*
f. *Restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve the desired result; and they must be proportionate to the interest to be protected (paras. 14–15);*
g. *Any restrictions must be consistent with the other rights guaranteed in the Covenant (para. 18).*[33]

32. Special Rapporteur Scheinin's view on the applicability of the permissible limitations test to Article 17 ICCPR was echoed in 2013 by the then Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, who analysed the implications of States' surveillance of communications for the exercise of the human rights to privacy and to freedom of opinion and expression.[34]

33. Special Rapporteur La Rue found that *"legislation has not kept pace with the changes in technology"*.[35] He recommended that legislation must stipulate that State surveillance of communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority, and individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State.[36]

34. On 12 June 2013, shortly after the publication of La Rue's report, the Global Principles on National Security and the Right to Information were launched. The Principles "*were drafted by 22 organizations and academic centres … in consultation with more than 500 experts from more than 70 countries at 14 meetings held around the world, facilitated by the Open Society Justice Initiative, and in consultation with the four special rapporteurs on freedom of expression and/or media freedom and the special rapporteur on counter-terrorism and human rights"*.[37]

35. The Principles (known as the Tshwane Principles after the place of their adoption) have since been

[33] U.N. Doc. A/HRC/13/37 (2009), §§16-17.

[34] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. U.N. Doc. A/HRC/23/40 (2013), §§28-29.

[35] Ibid., §§38 and 50.

[36] Ibid., §§81-83.

[37] Tshwane Principles, https://www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles, p5.

endorsed by the Parliamentary Assembly of the Council of Europe.[38] Principle 10 sets out categories of information to which a high presumption in favour of disclosure applies. Principle 10 (E) sets out the position with regard to surveillance and includes that the legal framework, procedures to be followed, entities authorised to conduct surveillance, and information about the use of surveillance powers should be available to the public. In addition the public should be fully informed of any illegal surveillance. (See Annex D for further details).[39]

36. In the wake of the Snowden revelations, the UN General Assembly adopted the Resolution "The right to privacy in the digital age" without vote on 18 December 2013.[40] In the resolution, the General Assembly welcomes the report of Special Rapporteur Frank La Rue, and *"[a]ffirms that the same rights that people have offline must also be protected online, including the right to privacy".* Consequently, the General Assembly calls upon all States (emphasis added):

> *"(a) To respect and protect the right to privacy, including in the context of digital communication;*
>
> *(b) To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law;*
>
> *(c) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;*
>
> *d) To establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data …"*[41] (emphasis added)

37. Moreover, the General Assembly requested the OHCHR 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".*[42] This report , published on 30 June 2014[43], notes that *"[u]nlike certain other provisions of the Covenant [the ICCPR], article 17 does not include an explicit limitations clause"* but states, referring to the Siracusa Principles on the Limitation and Derogation Provisions in the ICCPR, HRC General Comments Nos. 16, 27, 29, 34, and 31 and other authoritative sources, that:

> *"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*

[38] Recommendation 2024 (2013) (http://www.assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=20194&lang=en), §1.3; Resolution 1954 (2013) (http://www.assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=20190&lang=en), §§7-9.

[39] Tshwane Principles, pp. 25-26. Note the presumption in favour of disclosure does not apply in respect of information that relates solely to surveillance of the activities of foreign governments except in relation to violations of human rights and international humanitarian law.

[40] General Assembly Resolution 68/167. The right to privacy in the digital age. U.N. Doc. A/RES/68/167 (2013).

[41] Ibid., §§3-4.

[42] Ibid., §5.

[43] The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights. U.N. Doc. A/HRC/27/37 (2014).

option available. 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."[44]

38. On the basis of this finding, the OHCHR concludes:

> *"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."*[45] (emphasis added)

39. The OHCHR recommends that "*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.*"[46] (emphasis added)

40. Drawing on the report of the OHCHR and the 2014 report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism,[47] the UN General Assembly adopted another Resolution on "The right to privacy in the digital age" on 18 December 2014.[48] This resolution mainly reaffirms the resolution adopted in December 2013 but adds an important element to the protection of privacy when calling on the States:

> *"To provide individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access to an effective remedy, consistent with international human rights obligations …"*[49]

CONCLUSION

41. ENNHRI submits that the clear implication from the international materials set out above is that in order for any restriction on privacy rights to be justified as "in accordance with the law" and "necessary in a democratic society" in the surveillance or security context, the interference must be exceptional and be justified on a case-by-case basis, including – as a matter of principle – by prior judicial authorisation and subject to independent monitoring.

ENNHRI

5 February 2016

[44] Ibid., §§22-23.

[45] Ibid., §25.

[46] Ibid., §50.

[47] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. U.N. Doc. A/69/397 (2014).

[48] General Assembly Resolution 69/166. The right to privacy in the digital age. U.N. Doc. A/RES/69/166 (2014).

[49] Ibid., §4(e).

IN THE EUROPEAN COURT OF HUMAN RIGHTS **App No 58170/13**

BETWEEN:

BIG BROTHER WATCH & ORS - v - THE UNITED KINGDOM

WRITTEN OBSERVATIONS OF EUROPEAN NETWORK OF NATIONAL HUMAN RIGHTS INSTITUTIONS

ANNEXES

Annex A: Charter of Fundamental Rights of the European Union 2012/C 326/02, Articles 7 and 8:

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

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.

Annex B: Human Rights Committee - Concluding observations on the fourth periodic report of the United States of America. U.N. Doc. CCPR/C/USA/CO/4 (2014). §22:

"…The State party should:

(a) Take all necessary measures to ensure that its surveillance activities, both within and outside the United States, conform to its obligations under the Covenant, including article 17; in particular, measures should be taken 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 the individuals whose communications are under direct surveillance;

(b) Ensure that any interference with the right to privacy, family, home or correspondence is authorized by laws that: (i) are publicly accessible; (ii) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (iii) are sufficiently precise and specify in detail the precise circumstances in which any such interference may be permitted, the procedures for authorization, the categories of persons who may be placed under surveillance, the limit on the duration of surveillance; procedures for the use and storage of data collected; and (iv) provide for effective safeguards against abuse;

(c) Reform the current oversight system of surveillance activities to ensure its effectiveness, including by providing for judicial involvement in the authorization or monitoring of surveillance measures, and considering the establishment of strong and independent oversight mandates with a view to preventing abuses;

(d) Refrain from imposing mandatory retention of data by third parties;

(e) Ensure that affected persons have access to effective remedies in cases of abuse."

Annex C: Human Rights Committee - Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland. U.N. Doc. CCPR/C/GBR/CO/7 (2015). §24:

"..The Committee is concerned (a) that the Regulation of Investigatory Powers Act 2000, which makes a distinction between 'internal' and 'external' communications, provides for untargeted warrants for the interception of external private communications and communications data that are sent or received outside the United Kingdom without affording the same safeguards as apply to the interception of internal communications; and (b) about the lack of sufficient safeguards in regard to the obtaining of private communications from foreign security agencies and the sharing of personal communications data with such agencies. …

The State party should:

(a) Review the regime regulating the interception of personal communications and the retention of communications data, also taking into account the recommendations made by the Intelligence and Security Committee of Parliament and the Independent Reviewer of Terrorism Legislation, with a view to ensuring that such activities, both within and outside the State party, conform with its obligations under the Covenant, including article 17. In particular, measures should be taken 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 the individuals whose communications are under direct surveillance;

(b) Ensure that any interference with the right to privacy, with the family, with the home or with correspondence is authorized by laws that (i) are publicly accessible; (ii) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (iii) are sufficiently precise and specify in detail the precise circumstances in which any such interference may be permitted, the procedures for authorization, the categories of persons who may be placed under surveillance, the limit on the duration of surveillance, and procedures for the use and storage of data collected; and (iv) provide for effective safeguards against abuse;

(c) Ensure that robust oversight systems over surveillance, interception and intelligence-sharing of personal communications activities are in place, including by providing for judicial involvement in the authorization of such measures in all cases, and by considering the establishment of strong and independent oversight mandates with a view to preventing abuses; …

(e) Ensure that persons affected have access to effective remedies in cases of abuse."

Annex D: The Global Principles on National Security and the Right to Information ('The Tshwane Principles'). Finalized in Tshwane, South Africa and issued on 12 June 2013.

"Principle 10: Categories of Information with a High Presumption or Overriding Interest in Favour of Disclosure

…E. Surveillance

(1) The overall legal framework concerning surveillance of all kinds, as well as the procedures to be followed for authorizing surveillance, selecting targets of surveillance, and using, sharing, storing, and destroying intercepted material, should be accessible to the public.

Note: This information includes: (a) the laws governing all forms of surveillance, both covert and overt, including indirect surveillance such as profiling and data-mining, and the types of surveillance measures that may be used; (b) the permissible objectives of surveillance; (c) the threshold of suspicion required to initiate or continue surveillance; (d) limitations on the duration of surveillance measures; (e) procedures for authorizing and reviewing the use of such measures; (f) the types of personal data that may be collected and/or processed for national security purposes; and (g) the criteria that apply to the use, retention, deletion, and transfer of these data.

(2) The public should also have access to information about entities authorized to conduct surveillance, and statistics about the use of such surveillance.

Note: This information includes the identity of each government entity granted specific authorization to conduct particular surveillance each year; the number of surveillance authorizations granted each year to each such entity; the best information available concerning the number of individuals and the number of communications subject to surveillance each year; and whether any surveillance was conducted without specific authorization and if so, by which government entity.

The right of the public to be informed does not necessarily extend to the fact, or operational details, of surveillance conducted pursuant to law and consistent with human rights obligations. Such information may be withheld from the public and those subject to surveillance at least until the period of surveillance has been concluded.

(3) In addition, the public should be fully informed of the fact of any illegal surveillance. Information about such surveillance should be disclosed to the maximum extent without violating the privacy rights of those who were subject to surveillance.

(4) These Principles address the right of the public to access information and are without prejudice to the additional substantive and procedural rights of individuals who have been, or believe that they may have been, subject to surveillance.

Note: It is good practice for public authorities to be required to notify persons who have been subjected to covert surveillance (providing, at a minimum, information on the type of measure that was used, the dates, and the body responsible for authorizing the surveillance measure) insofar as this can be done without jeopardizing on-going operations or sources and methods.

(5) The high presumptions in favour of disclosure recognized by this Principle do not apply in respect of information that relates solely to surveillance of the activities of foreign governments.

Note: Information obtained through covert surveillance, including of the activities of foreign governments, should be subject to disclosure in the circumstances identified in Principle 10A."