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

BETWEEN:

BIG BROTHER WATCH & ORS

Applicants

-v-

UNITED KINGDOM

Respondent

APPLICANTS' REQUEST FOR A REFERENCE TO THE GRAND CHAMBER

I. INTRODUCTION

1. The complaints brought in this application concern three different aspects of the UK's surveillance regime, primarily under the Regulation of Investigatory Powers Act 2000 ("**RIPA**"):

   1.1 The bulk interception of communications under s.8(4);

   1.2 Intelligence sharing with foreign governments; and

   1.3 The obtaining of communications data from communications service providers ("**CSPs**") under Chapter II of RIPA.

2. The Chamber (First Section), in its judgment of 13 September 2018 ("**the Judgment**"), held that:

   2.1 The bulk interception regime violated Article 8 and Article 10 ECHR due to insufficient oversight and inadequate safeguards. However, the decision of a State to operate a bulk interception regime did not of itself violate the Convention;

   2.2 The regime for sharing intelligence with foreign governments, as amended and updated following the filing of the Application, did not violate Article 8 or Article 10 ECHR;

2.3 The regime for obtaining communications data from CSPs violated Article 8 ECHR as it was not in accordance with the law.

3. Big Brother Watch, Open Rights Group, English PEN and Dr Constanze Kurz (together, "**the Applicants**") request that the case be referred to the Grand Chamber pursuant to Article 43 of the Convention, and Rule 73 of the Court's Procedural Rules (1 August 2018), on the basis that the case concerns (a) a serious question affecting the interpretation or application of the Convention and/or (b) a serious issue of general importance which warrants consideration by the Grand Chamber. In the following submission, the Applicants address only the aspects of the case before the Court which concern Article 8 ECHR, on which they made submissions in the Court below.

4. The Applicants have also seen, and commend, the application of the 10 Human Rights Organisations for a referral in Application No. 24960/15.

II. THE THRESHOLD FOR REFERRAL TO THE GRAND CHAMBER

5. Article 43 ECHR provides:

> *1. Within a period of three months from the date of the judgment of the Chamber, any party to the case may, in exceptional cases, request that the case be referred to the Grand Chamber.*
>
> *2. A panel of five judges of the Grand Chamber shall accept the request if the case raises a serious question affecting the interpretation or application of the Convention or the Protocols thereto, or a serious issue of general importance.*[1]
>
> *3. If the panel accepts the request, the Grand Chamber shall decide the case by means of a judgment.*

6. Rule 73 of the Rules of Court (1 August 2018) provides:

> *1. In accordance with Article 43 of the Convention, any party to a case may exceptionally, within a period of three months from the date of delivery of the judgment of a Chamber, file in writing at the Registry a request that the case be referred to the Grand Chamber. The party shall specify in its request the serious question affecting the interpretation or application of the Convention or the Protocols thereto, or the serious issue of general importance, which in its view warrants consideration by the Grand Chamber.*
>
> *2. A panel of five judges of the Grand Chamber constituted in accordance with Rule 24 § 5 shall examine the request solely on the basis of the existing case file. It shall accept the request only if it considers that the case does raise such a question or issue. Reasons need not be given for a refusal of the request.*
>
> *3. If the panel accepts the request, the Grand Chamber shall decide the case by means of a judgment.*

[1] Emphasis added save where otherwise indicated.

7. Given the breadth of the impact of the Chamber's decision in this application, it is clear that it raises issues of general public importance. Indeed, in a similar context, the Court of Justice of the European Union ("**CJEU**") has emphasised that what is at stake is the compatibility of "*automatic processing*", on a "*generalised basis*", of "*all means of electronic communication* […of] *practically the entire European population* […]"[2], and that, in the context of government-mandated retention of communications data by telecommunications operators, this activity "*taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, 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*" (Joined Cases C-203/15 Tele 2 Sverige AB and C-698/15 Watson and Others (ECLI:EU:C:2016:970) ("***Watson***") at §§98-99).

8. There is, moreover, recent precedent for the Grand Chamber to accept requests for referrals in relation to covert surveillance measures (López Ribalda and Others v Spain, App. no. 1874/13, 9 January 2018; Zakharov v Russia, App. no. 47143/06 (2016) 63 EHRR 17), which reflects the importance and the currently pressing nature of this issue to the maintenance of an open democratic society, across the Contracting Parties to the Convention.

9. For the following five reasons, the present case raises a serious question affecting the interpretation or application of the ECHR; further or alternatively a serious issue of general importance.

10. First, the legal issues addressed by the Chamber, on any view, fall into either or both of these categories. The Chamber dealt, in particular, with the following:

    10.1 **In relation to the s.8(4) bulk interception regime:** this was the first consideration of the United Kingdom's bulk interception regime since the Court's judgment in Liberty v United Kingdom (2009) 48 EHRR 1, App. no. 58243/00, 1 July 2008. The Judgment analysed the minimum requirements that must be set out in law in order to avoid abuses of power by state authorities. The Chamber held that the "*six minimum requirements*" set out in Weber and Saravia v Germany (2008) 46

[2] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger (ECLI:EU:C:2014:238) at §§55-56.

EHRR SE5 ("**Weber**") applied (see Judgment, §315). Importantly, the Court rejected the Applicants' arguments (addressed further below) that the six minimum requirements should be "*updated*" in light of a technological "*sea change*" which had occurred since the latter cases were decided, by including requirements for (i) objective evidence of reasonable suspicion of serious crime or of conduct amounting to a specific threat to national security in relation to the persons for whom data was being sought, (ii) prior independent judicial authorisation of interception warrants, and (iii) subsequent notification to the surveillance subject. Notwithstanding the Fourth Section's recognition of the need for "*simultaneous development of legal safeguards securing respect for citizens' Convention rights*" alongside technological change[3], the First Section rejected the need to update the Weber requirements. It nevertheless held that there had been a violation of Article 8 on the basis of (i) the lack of oversight of the entire selection process, including the selection of bearers for interception, the selectors and search criteria for filtering intercepted communications, and the selection of material for examination by an analyst (§§346-347); and (ii) the absence of any real safeguards applicable to the retention and selection of related communications data for examination and use (§§316-320).

10.2 **In relation to the intelligence sharing regime:** whether there was a basis in law for the requesting of intelligence from foreign intelligence agencies, and whether that law was sufficiently accessible and pursued several legitimate aims. The Court found that these requirements were satisfied, in light of recent disclosures concerning the legal regime which had been made after the Application was filed (§427). There was thus no breach of Article 8 ECHR (§§447-449).

10.3 **In relation to the Chapter II regime:** whether the acquisition of communications data from CSPs was lawful. The Chamber found a violation of Article 8 on the basis that the Chapter II regime permitted access to retained data for the purpose of combating crime (rather than combating only "*serious crime*") and, save for where access is sought for the purpose of determining a journalist's source, was not subject to prior review by a court or independent administrative body (§§467-468).

[3] Application no. 37138/14 Szabó and Vissy v Hungary, Fourth Section, 12 January 2016 at §§68 and 70.

11. Second, the Chamber itself emphasised the significance of the case in acknowledging that:

11.1 There is a "*risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it*" (§308, emphasis added);

11.2 This case was the first time the Court has been asked to consider the ECHR compliance of an intelligence sharing regime (§416);

11.3 "*States could use intelligence sharing to circumvent stronger domestic surveillance procedures and/or any legal limits which their agencies might be subject to as regards domestic intelligence operations*" (§423);

11.4 The Court has only twice before been called to consider the ECHR compliance of a regime for the acquisition by a public authority of communications data from a CSP: in *Malone v the United Kingdom*, 2 August 1984, Series A no.82 and in *Ben Faiza v France*, App. no. 31446/12, 8 February 2018 (§460); and

11.5 As was rightly emphasised by the Partly Concurring and Partly Dissenting Opinion of Judges Koskelo and Turković, in relation to bulk interception, "[i]*t is obvious that such an activity – an untargeted surveillance of external communications with a view to discovering and exploring a wide range of threats – by its very nature takes on a potentially vast scope, and involves enormous risks of abuse. The safeguards against those risks, and the standards which under the Convention should apply in this regard, therefore raise questions of the highest importance*" (at §3).

12. Third, the issues raised are highly topical. They have been the subject of, among other things:

12.1 In the UK, a number of important recent decisions of the Investigatory Powers Tribunal;[4]

[4] See, e.g. (i) Belhadj and Others v Security Service, Secret Intelligence Service, Government Communications Headquarters, the Secretary of State for the Home Department, and the Secretary of State for the Foreign and Commonwealth Office, IPT/13/132-9/H and IPT/14/86/CH, 29 April 2015; (ii) News Group and Others v The Commissioner of Police of the Metropolis IPT/14/176/H, 17 December 2015; and (iii) Privacy International v. Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters,

12.2 A number of recent prominent and well-informed parliamentary, governmental and non-governmental reports in the UK and at European level;[5] and

12.3 Several recent judgments of this Court and the CJEU.[6] The Applicants note, in particular, Centrum för rättvisa v Sweden, App. no. 35252/08 (albeit which concerned a different legal regime), in which a referral request has also been made, consideration of which the Grand Chamber Panel has adjourned.

13. Fourth, the large number of third parties[7] who raised their concerns as to the systemic impact of the regimes in issue further attests to the serious nature of the questions and issues raised in this case.

14. Fifth, given the UK's role as a telecommunications hub, the issues raised in the Application extend outside the UK itself and affect all European citizens, as illustrated by Dr Kurz's interest as the Fourth Applicant.

15. For all these reasons, the Applicants submit that this is an exceptional case within the meaning of Article 43 and that the two grounds in Rule 73 are satisfied, and that accordingly a referral to the Grand Chamber is justified.

III. BULK INTERCEPTION

16. The Chamber found a violation of Article 8 in relation to the s.8(4) regime on the limited basis (safeguarding and oversight) identified above. It accepted, however, that a bulk

Security Service and Secret Intelligence Service (IPT/15/110/CH; EU OJ C 22, 22.1.2018, p. 29–30), 8 September 2017.

[5] See, e.g. (i) Intelligence and Security Committee of Parliament: July 2013 Statement on GCHQ's alleged interception of communications under the US PRISM programme; (ii) Privacy and security: a modern and transparent legal framework; (iii) "*A Question of Trust*": Report of the Investigatory Powers Review by the Independent Reviewer of Terrorism Legislation ("**the Anderson Report**"); (iv) A Democratic Licence to Operate: Report of the Independent Surveillance Review ("ISR"); (v) Report of the Bulk Powers Review; (vi) Attacks in London and Manchester March-June 2017: Independent Assessment of MI5 and Police Internal Reviews; (vii) Annual Report of the Interception of Communications Commissioner for 2016; and (viii) the 2015 Report of the European Commission for Democracy through Law ("**the Venice Commission**") on the Democratic Oversight of Signals Intelligence Agencies.

[6] Ben Faiza v France, App. no. 31446/12, 8 February 2018; Tele 2 and Watson and others, above.

[7] Namely (i) the European Network of National Human Rights Institutions; (ii) Article 19; (iii) Access Now; (iv) The Helsinki Foundation for Human Rights; (v) The International Commission of Jurists; (vi) Open Society Justice Initiative; (vii) European Digital Rights and other organisations active in the field of human rights in the information society; (viii) The Law Society of England and Wales; (ix) The Electronic Privacy Information Center; (x) Bureau Brandeis; (xi) Center for Democracy and Technology; (xii) Pen American Center; (xiii) Human Rights Watch; (xiv) The National Union of Journalists; (xv) The International Federation of Journalists; and (xvi) The Media Lawyers' Association.

interception regime could, in principle, be permissible as falling within the wide margin of appreciation afforded to national authorities in choosing how best to protect national security (§314). The Applicants do not accept that this is correct, for at least the following reasons, and submit that it is imperative and timely that the Grand Chamber examine this issue.

17. First, the cases relied on by the Chamber - Weber (supra) and Liberty v UK, are, as the Chamber noted, more than ten years old, and address materially different situations.[8] While the Chamber recognised that changes in technology could pose greater threats to states, it failed to acknowledge the corollary to this: namely, that changes in technology also pose a greater threat to the Article 8 rights of individuals, who now face far greater risks of arbitrary interference with their rights than was previously the case.[9] The Court failed, for instance, to consider the cumulative effect of combining data from many warrants and bearers, as well as the building of mass data repositories, and the increasing automation – and therefore wide-scale interrogation - of those databases. It was not therefore sufficient to simply invoke a "*wide*" margin of appreciation without further analysis. Indeed, it is difficult to see why this application is not comparable to the database of DNA samples considered by the Grand Chamber – and held to be disproportionate though of "*inestimable value*" – in S and Marper v United Kingdom (2009) 48 EHRR 50.

18. Second, it is common ground that interception of data constitutes an interference with Article 8 and that such interference will only be justified if it is "*necessary in a democratic society*".

19. It is necessary to consider proportionality at each of the stages in the process of interception, which are broadly (though there is some overlap and this is not a strictly linear process) as follows: (i) interception (the signal is obtained from tapping a source, such as a fibre optic cable, and all the data is copied to GCHQ's computers); (ii) extraction (the intercepted signals are converted into a digital stream so that the data can be reconstructed, and data is processed to structure and organise "packets" into units of communication) (iii) filtering (data is included or excluded at this stage); (iv) storage (the data, whether targeted or bulk, is retained in a database); (v) analysis

[8] See e.g. Applicants' Consolidated Observations, §§9, 21, 24.
[9] See e.g. Applicants' Application, 30 September 2013, §1; Applicants' Consolidated Observations, §4.

(querying, examining, or data-mining); and (vi) dissemination (use of the resulting information to provide or contribute to intelligence).

20. The UK's purported justifications for bulk interception do not hold water. The discovery of new targets through bulk interception is disproportionate in circumstances where those targets are highly likely to be discovered through the alternative use of appropriate discriminators following extraction, i.e. at stage (iii) above. As the Chamber noted, "[t]*he intelligence services should not be permitted to obtain via a bulk warrant what they could obtain via a targeted warrant*" (§343).

21. The Applicants submit that a bulk interception regime of this nature cannot, therefore, be proportionate: the bulk collection and storage of data and communications of a substantial segment of the European population, the majority of whom are of no interest to the intelligence agencies, is plainly disproportionate.

22. The Chamber relied heavily on the view of the Government's Independent Reviewer of Terrorism Legislation that "*bulk interception was an essential capability*" and on his conclusion that "*no alternative or combination of alternatives would be sufficient to substitute for the bulk interception power*" (§§176 and 384).[10] It concluded that "[i]*t is clear that bulk interception is a valuable means to achieve the legitimate aims pursued, particularly given the current threat level from both global terrorism and serious crime*" (§386). But utility is not the test integral to Article 8 ECHR, as the Grand Chamber recognised in Marper (at §§92 and 135). The Chamber erred in its uncritical adoption of the position of the Government's Independent Reviewer and its focus on a partial selection of materials supportive of that position to the exclusion of the concerns expressed by many international bodies as to mass surveillance.

[10] This reliance was particularly unusual – and regrettable – given that the Government's Independent Reviewer's Terms of Reference did not include analysis of the necessity or proportionality of such interception: the Reviewer did not claim to pronounce on the necessity of bulk powers, and in fact explicitly declined to do so. See footnote 245 to his Report of the Bulk Powers Review (August 2016): *"The legal significance of the familiar terms "necessity" and "proportionality" is not altogether straightforward…I have accordingly (in keeping with my terms of reference) avoided pronouncing on whether the powers under review are "necessary", a word which in its everyday meaning could be taken to encompass assessments of proportionality or overall desirability which are excluded from my remit."*

IV. SAFEGUARDS

A. The need for new safeguards

23. Even assuming that a bulk interception regime of this nature could in principle be permissible, given the new and extended threats to Article 8 rights posed by such bulk interception, the Chamber was wrong to confine itself to the application of the existing "*6 minimum requirements*" identified as necessary safeguards for less extensive and intrusive forms of interception in Weber (supra) as constituting adequate protections for private life and correspondence in this new context. The Weber criteria were formulated prior to the information and communications revolution of the past decade (which introduced, among other things, the smart phone and commonplace mobile connectivity) and are no longer sufficient to ensure that a communications surveillance regime is compatible with Article 8 ECHR. As such, they should be updated as set out at §8.1 above, to reflect "*the important role played by the internet […] in modern society*"[11], which has become "*both ubiquitous and increasingly intimate*"[12]. The Applicants note and adopt the arguments of Judges Koskelo and Turković in this regard, in particular as set out at §§12-15 of their judgment.[13]

24. The Court declined to add the additional requirements on the basis that (i) "*requiring objective evidence of reasonable suspicion in relation to the persons for whom data is being sought and the subsequent notification of the surveillance subject would be inconsistent with the Court's acknowledgment that the operation of a bulk interception regime in principle falls within a State's margin of appreciation. Bulk interception is by definition untargeted, and to require "reasonable suspicion" would render the operation of such a scheme impossible. Similarly, the requirement of "subsequent notification" assumes the existence of clearly defined surveillance targets, which*

---

[11] Case C 131/12, Google Spain SL (ECLI:EU:C:2014:317) at §80.

[12] "*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, §1.

[13] Judges Koskelo and Turković noted, in particular, that (a) the line of caselaw relied on by the Chamber was "*no longer an adequate basis for assessing the standards*" governing this area; (b) there was an "*obvious*" need for "*real safeguards through independent control and review*" in circumstances where the threats on account of which surveillance of communications is considered necessary have changed, and where "*the notion of terrorism...may...be used quite loosely and opportunistically in a desire to legitimise interferences with such rights and freedoms*"; and (c) the Convention standards must be considered in the light of increasing evidence among States of a "*degradation of democratic standards and the rule of law*" (§14).

is simply not the case in a bulk interception regime" (§317); and (ii) while judicial authorisation was an "*important safeguard against arbitrariness*" and "*desirable*", it was not a "*necessary requirement*" (§318); "*by itself it can neither be necessary or sufficient to ensure compliance with Article 8*" (§320).

25. The Chamber's error regarding the permissibility, or proportionality, of such a regime thus fed into its conclusions regarding objective evidence of suspicion and subsequent notification of the subject. The Applicants do not accept that to require objective evidence of reasonable suspicion in relation to the persons for whom data is being sought and the subsequent notification of the surveillance subject would render an interception regime of the necessary scale impossible. They note and adopt, in particular, the submission of the 10 Human Rights Organisations in relation to the ability of other jurisdictions to make provision for notification after the event, apparently without jeopardising their intelligence operations; and to the case of Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria, App. No. 62540/00.

B. Bulk interception and the application of the *Weber* criteria

26. In addition, the Chamber erred in finding that certain of the *Weber* criteria were satisfied. In particular:

26.1 **In relation to the third *Weber* criterion (limits on duration):** The Applicants argued that, in practice, a s.8(4) warrant may continue indefinitely under a system of rolling warrant renewals.[14] The Chamber, relying on Kennedy v UK (2011) 52 EHRR 4 at §162, saw "*no evidence to substantiate the applicants' claim that once issued, section 8(4) warrants could continue indefinitely regardless of whether they continued to be necessary and proportionate*" (§360). But Kennedy concerned the use of *targeted* telephone tapping. The Chamber failed to grapple with the Applicants' submission that there was no real durational check on the power because "*bulk interception warrants under s. 8(4)...will always be renewed as they are not based on any particular individuals and specific threat, but rather on general threats to national security etc., and there is no limit to the number of times a warrant may be renewed*."[15]

[14] Applicants' Consolidated Observations, 29 September 2017, §122.
[15] Applicants' Consolidated Observations, §122, emphasis added.

26.2 **In relation to the fourth *Weber* criterion (examination, usage and storage of data):** The Applicants contended that the breadth of a certificate accompanying a s.8(4) warrant meant that it placed no effective constraint on the scope of filtering and analysis of data.[16] In particular, there was no requirement that the selectors used to filter intercepted communications be identified in the certificate (§277). The Chamber did not properly engage with this submission but focussed instead on the separate issue of the subjection of the search criteria and selectors used to independent oversight (§340). Nor did the Chamber adequately deal with the fact that it is at the filtering stage that data mining and complex processing may take place, involving the structuring of data, creation of session histories, etc.

26.3 **In relation to the sixth Weber criterion (erasure and destruction of data):** The Applicants argued that there were no effective or binding safeguards against disproportionate retention of intercepted data.[17] The Chamber's conclusion that the provisions on the erasure and destruction of intercept material were sufficiently clear (§374) ignored the question of whether the provisions in question in fact constituted an effective safeguard. This was despite the Chamber having accepted that the purported upper limit of two years for retention of data had not been complied with in at least one case (the Liberty proceedings before the IPT) (§§372-373). The Court also accepted the automatic discarding / destruction of intercepted material which was not caught in the filtering process without question (§§329, 341, 370, 370-374). That this does in fact take place is not, however, clear from the query databases. Moreover, it does not address the issue of the retention of "insights" generated from the intercepted data; such derived data can be as intrusive, or more so, than the communications data originally intercepted.

V. INTELLIGENCE SHARING

27. As noted above, this is the first case in which the Court has been asked to consider the compliance of an intelligence sharing regime with the Convention. The Applicants argued that there was no basis in law for the intelligence sharing carried out by the intelligence services and no regime which satisfied the "*quality of law*" requirements (§398). The Chamber considered three categories of material: (i) material which the NSA

[16] Applicants' Consolidated Observations, §113 and 123.2.
[17] Applicants' Consolidated Observations, §127.

had provided to the UK intelligence services unsolicited, which on its face derived from intercept; (ii) communications which the UK intelligence services had either asked the NSA to intercept, or to make available to them as intercept; and (iii) material obtained by the NSA other than by the interception of communications.

28. The Chamber declined to consider the first category on the basis that the Government had, at the hearing, advised that it was "*implausible and rare*" for intercept material to be obtained unsolicited (§417). This is concerning. First, that such material is obtained "*rarely*" is very different from it "*never*" being obtained; if it is obtained at all, such receipt cannot be "*implausible*" and it should have been analysed by the Chamber. Second, this raises a question as to the meaning of "*solicited*" and "*unsolicited*" material which was not examined by the Chamber. The Applicants' understanding is that, consistently with the known symbiosis between NSA and GCHQ systems, much intelligence sharing is automatic and is not based on express requests. An example of this is the DISHFIRE database of millions of SMS messages, which is jointly operated by the NSA and GCHQ.

VI. CONCLUSION

29. For all the above reasons, the Applicants respectfully request that the case be referred to the Grand Chamber.

12 December 2018

HELEN MOUNTFIELD QC
Matrix Chambers

RAVI MEHTA
FLORA ROBERTSON
Blackstone Chambers

DANIEL CAREY
Solicitors to the Applicants
Deighton Pierce Glynn Solicitors
Unit 10C
Whitefriars
Bristol BS1 2NT
Tel: 0117 332 3598
Fax: 0117 370 1036
www.dpglaw.co.uk