IN THE EUROPEAN COURT OF HUMAN RIGHTS **Application no 58243/00**

(1) LIBERTY
(2) BRITISH-IRISH RIGHTS WATCH
(3) THE IRISH COUNCIL FOR CIVIL LIBERTIES

Applicants

v.

UNITED KINGDOM

Respondent Government

APPLICANTS' OBSERVATIONS ON *WEBER* DECISION AND NECESSITY

Introduction

1. The Section Registrar's letter of 29 August 2007 indicated that the Chamber President has requested observations on two points:

   1) In the light of the Court's inadmissibility decision in *Weber and Saravia v. Germany* 54934/00, dec. 29.6.06, is the English law regarding the safeguards which apply to the interception of external communications sufficiently detailed and accessible? In particular, can any real distinction be made between the British and German systems?

   2) In the event the system for interception of communications is "in accordance with the law", each party is requested succinctly to explain its position on the question whether the interference is "necessary in a democratic society".

2. On point (1), the Applicants submit that the *Weber* decision highlights the deficiencies in the English system. The G10 Act set out on its face detailed provisions regulating the way in which individual communications were to be selected from the pool of material derived from "strategic interception"; disclosure of selected material among the various agencies of the German State and the use that each could properly make of the material; and the retention or destruction of the material. The authorities' discretion was further

regulated and constrained by the public rulings of the BVerfG on the compatibility of the provisions with the *Grundgesetz*. It is not surprising that the Court found that the provisions of the modified G10 Act contained sufficient safeguards to satisfy the predictability and accessibility criteria.

3. The contrast with interception of external communications under IOCA could not be greater. Under the law in force at the time the interception took place, no provision was made on the face of the statute for any part of the processes following the initial interception, other than the duty on the Secretary of State to make unspecified "arrangements". The arrangements themselves were unpublished. There was no legal material in the public domain indicating how the authorities' powers to select, disclose, use or retain particular communications were regulated. The authorities' conduct was not "in accordance with the law" because unsupported by any predictable legal basis satisfying the accessibility principle.

4. On point (2), the Applicants submit:

   a. If the Court considers that their observations about the adequacy of the safeguards contained in the "arrangements" made by the Secretary of State more properly belong to the question whether the interference is necessary and proportionate than to the question whether it is "in accordance with the law", the Court is invited to conclude that the arrangements did not provide adequate safeguards, and on that basis the interference cannot be regarded as "necessary in a democratic society".

   b. In any event, the interference cannot be regarded as necessary and proportionate for the further reasons summarised below.

5. The Applicants make the following further observations in support of those submissions.

"In accordance with the law": the English system in the light of the *Weber* decision

The Applicants' case: recapitulation

6. The Applicants' detailed submissions on the principles applicable to the "in accordance with the law" criterion in the context of interception and subsequent processing of communications can be found at:

- paras. 19 to 22 of the original Annex to the application;
- paras. 10 to 16 of their Reply dated 15 July 2003 to the Government's Further Observations of 23 May 2003; and
- paras. 12 to 15 of their Reply dated 30 June 2005 to the Government's Supplementary Observations dated 14 February 2005.

7. The principles relied on by the Applicants remain firmly established in the Court's case law: see the summary at paras. 92 to 95 of the *Weber* decision. Para. 95 contains a useful reminder that the law must set out sufficient minimum safeguards in relation to a multiplicity of matters, including in particular:

- "the procedure to be followed for examining, using and storing the data obtained;
- the precautions to be taken when communicating the data to other parties; and
- the circumstances in which recordings may or must be erased or the tapes destroyed".

The Court reiterated that these post-interception steps are equally significant interferences with Article 8(1) as the interception itself: see para. 79.

8. The Court referred to its *Weber* decision (among others) when giving judgment in *AEIH and Ekimdzhien v. Bulgaria* (no. 62540/00, 28 June 2007), finding that the relevant Bulgarian legislation failed to meet the "in accordance with the law" criterion. At paragraph 75 of that judgment, the Court pointed out [emphasis added]:

> "In view of the risk of abuse intrinsic to any system of secret surveillance, such measures must be based on a law that is **particularly precise. It is essential to have clear, detailed rules** on the subject, especially as the technology available for use is continually becoming more sophisticated..."

9. The Applicants develop their case as to why the system under IOCA fails to meet the "in accordance with the law" standard at:

- Paras. 15 and 16 of the original Annex to the application
- Paras. 15 to 32 of their Reply, submitted in March 2003, to the Government's Observations of 28 November 2002;
- Paras. 7, 8, 16 and 17 of their Reply dated 15 July 2003 to the Government's Further Observations of 23 May 2003; and
- Paras. 17 to 19 (and see also paras. 20, 21 and 26) of their Reply dated 30 June 2005 to the Government's Supplementary Observations dated 14 February 2005 (which dealt with issues arising in the parallel domestic proceedings on the RIPA regime, which replaced IOCA on 2 October 2000).

10. The central point is that in the case of external interception, the warrantry procedure under IOCA authorises interception of a vast mass of communications – similar to the "strategic interception" which *Weber* concerned. By contrast with *internal* interception, the real decision to pay attention to particular individuals' communications for the purposes of crime prevention, national security, etc., arises not at the stage of seeking and issuing a warrant, but in the post-interception processes of filtering and selection of communications from the mass of intercept product. Yet nothing on the face of the statute, or in any other published material capable of amounting to "law", provides any indication of the necessary minimum safeguards, the essential provisions indicating how the decision-making process is regulated or constrained. Nor was there any such published provision in relation to the other important post-interception processes of actual use, onward disclosure/sharing, and retention/destruction of intercept product.

11. All that appeared on the face of the statute was the opaque requirement for the Secretary of State to make "arrangements". But the arrangements were wholly unpublished, and their scope and content unknown to those whose communications might be intercepted under the external regime. Hence it was simply impossible for members of the public to know with any reasonable certainty (as the Court put it in *Malone*) which elements of the

process are the subject of legal rules and which are simply left to operational discretion (see the Applicants' Reply of 20 June 2005 to the Government's supplementary observations).

12. During the course of the present proceedings, the Government offered in evidence a description of certain practices and procedures, apparently forming part of the "arrangements" operated by the agencies in question, which it claimed demonstrated the existence of necessary safeguards and constraints on the various post-interception processes. Having disclosed those matters, it is not open to the Government to argue that, at the time the interception complained of took place, there were overriding reasons of national security preventing publication of at least some material describing to the public the essence of the safeguards in existence (see paras. 7 and 8 of the Applicants' Reply of 15 July 2003 to the Government's Further Observations).

Comparison with *Weber*

13. The Applicants previously drew the attention of the Court to the German domestic proceedings on the constitutionality of the G10 Act. German and English versions of the BVerfG judgment of 14 July 1999 were submitted as an appendix to Mr. Campbell's First Witness Statement in March 2003. The BVerfG ruled that Article 10 of the *Grundgesetz* (which covers similar ground to ECHR Article 8) was contravened by a number of aspects of the G10 strategic surveillance regime that resemble certain features of the IOCA external interception system. The Applicants are grateful to the Court for supplying the *Weber* decision, in which the Court examined those aspects of the G10 law that had been ruled compatible with the *Grundgesetz* and those modified by the BVerfG (and subsequently by the legislature in 2001) in the light of the BVerfG's findings of incompatibility or partial incompatibility.

14. The G10 Act as examined by the Court in *Weber* contained the following express provisions about the treatment of material derived from strategic interception as applied to non-German telephone connections:

a. Federal Intelligence Service only authorised to carry out monitoring of communications with the aid of search terms which served, and were suitable for, the investigation of the dangers described in the monitoring order -- s. 3(2), first sentence (dec. para. 32)

b. Search terms to be listed in the monitoring order -- s. 3(2), fourth sentence (dec. para. 32)

c. Execution of monitoring process (ie. including the use of search terms) to be recorded in minutes by technical means – s. 3(2), fifth sentence (dec. para. 32)

d. Personal data obtained through interception could only serve prevention, investigation and prosecution of listed offences, if the data subject was subject to individual monitoring or if there were "factual indications" implicating a person in a listed offence -- section 3(3), first sentence (dec. para. 33)

e. Duty of Federal Intelligence Service to report to Federal Government under FIS Act s. 12 subject to requirement that the personal data contained in the report be identified and limited to use for the purposes which had justified their collection – s. 3(3), second sentence, as modified in order to provide sufficient safeguards in relation to the use of the material (Dec. para. 33)

f. Data to be transmitted to Office for Protection of the Constitution of the Federation and the *Länder*, and other specified bodies, for the s.3(3) purposes and so far as necessary for the recipients to carry out their duties, and only so far as serving the protection of an important legal interest and where there is a sufficient factual basis for suspicion that offences planned or committed – s. 3(5) first sentence, as modified to ensure proportionality (dec. paras. 36, 39-42, 44 – and note reciprocal duty on recipient authority to verify necessity of transmission: see below)

g. Decision to transmit data to such a body to be taken by staff member qualified to hold judicial office; decision to transmit, destroy or delete the data to be recorded in minutes – s. 3(5) second sentence, as modified to ensure effective supervision of the transmission of data (dec. paras. 36, 43, 44)

h. Where data no longer necessary to achieve the s. 3(1) purposes and not to be transmitted to other authorities under s. 3(5), they must be destroyed and deleted from files by a staff member qualified to hold judicial office. Destruction not to take

place until 6 months after subject notified that monitoring has taken place – s. 3(6) first sentence as modified to ensure effective judicial review (dec. paras. 46, 49)

i. Destruction and deletion must be recorded in minutes – s. 3(6) second sentence (dec. para. 46)

j. Six-monthly verification of whether conditions for destruction or deletion were met – s. 3(6) third sentence (dec. para. 46)

k. Recipient authorities to verify whether transmitted data needed to achieve the s. 3(3) aims – s. 3(7) first sentence (dec. para 47)

l. Recipient authorities to destroy data transmitted to them unnecessarily, unless separation of necessary from unnecessary data impossible or requiring excessive effort, and even then use of unnecessary data prohibited. Destruction not to take place until 6 months after subject notified that monitoring has taken place – s. 3(7) second and third sentences, as modified to ensure effective judicial review (dec. paras. 47, 49)

m. Personal data about a person involved in the monitored communications to be destroyed if no longer necessary for the purposes listed in the Act and no longer of significance for judicial examination of legality of measure; destruction to be supervised by a person qualified to hold judicial office, and not to take place until 6 months after subject notified that monitoring has taken place – s. 7(4), first sentence, as modified to ensure effective judicial review (dec. paras. 48, 49).

n. Destruction to be recorded in the minutes – s. 7(4) second sentence (dec. para. 48)

o. Six-monthly examination of whether personal data to be destroyed – s. 7(4) third sentence (dec. para. 48)

p. Access prohibited to data retained only for the purpose of judicial examination – s. 7(4) fifth sentence (dec. para. 48)

q. Recipient authorities to mark transmitted data as having been obtained through strategic interception – modification to s. 3(7) (dec. para. 50)

r. Federal Intelligence Service or recipient authority to notify persons monitored of the restriction on secrecy of their communications as soon as notification could occur without compromising the aim of the restriction and the use of the data obtained, unless data destroyed within 3 months of receipt by FIS or recipient authorities *and*

data had not been used before destruction – s. 3(8), first and second sentences, as modified to ensure adequate safeguards (dec. paras. 51-54)

s. Monitoring measures under supervision of independent body, the G10 Commission; supervision by Commission covers (notwithstanding the original wording of the statute) the whole process of obtaining and using the data, including measures taken under s. 3(3), (5), (6) and (8), not only the making of monitoring orders by the competent Minister – s. 9(2) as modified to ensure the legislation was read and applied as providing for broad supervision by the Commission

t. Judicial review excluded where measures ordered and executed to prevent an armed attack on German territory; but person concerned must be notified of measures as soon as measures discontinued provided notification not jeopardising purpose, whereupon the person could have recourse to the courts – s. 9(6), subject to s. 9(5) (dec. paras 59-61).

15. Thus the German legislation examined by the Court -- *a fortiori* following its modification by the BVerfG and subsequently the legislature -- contained comprehensive and explicit provisions establishing a clear and precise legal framework for each stage of the process of strategic interception. For each step, from initial authorisation of strategic monitoring, through the method of selection (ie. search terms and their proper scope), disclosure/sharing and use by the State authorities, decisions about retention or destruction/deletion of data and notification of the individual, to supervision by the Commission and review by the courts, the law clearly defined the purposes for which the authorities could act, the scope of their decision-making functions, and the specific safeguards in place to ensure the proportionality of each interference with rights and the effectiveness of supervision and review.

16. There is a sharp contrast with the "arrangements" under IOCA as described in the UK Government's evidence in the present case.

17. First, the practices so described cover a narrower range of aspects of the process, and are considerably vaguer, than the provisions considered in *Weber*. So even if those practices

had been a form capable of amounting to "law", they would fall far short of the regulatory measures and safeguards necessary to meet the predictability criterion in relation to clandestine interception. It is relevant that the BVerfG regarded the provisions it examined, as variously modified, as the *minimum* necessary safeguards to ensure the compatibility of the G10 Act with Article 10 of the *Grundgesetz*. It is impossible to see how the UK "arrangements", falling short of even the minima reflected in the German legislation, and involving (among other things) no possibility of scrutiny of the process by the ordinary courts, can satisfy the requirements of ECHR Article 8(2).

18. Second, the (then) unpublished material relied on by the Government plainly cannot in any event amount to "law". Even if the Court were persuaded that the range of matters described in the Government's evidence provided a set of constraints and safeguards in principle capable of satisfying the predictability criterion, their secret character is fatal to their accessibility. As the German system indicates, the proper place for the provisions that delimit and regulate the authorities' powers is in promulgated legislation.

Is the interference "necessary in a democratic society"

19. As the Court reiterated in *Weber*, even if measures involving clandestine surveillance are in accordance with the law, the adequacy of the safeguards or guarantees against abuse of individuals' rights may feature in the assessment of whether the system under which the measures are imposed meets the "necessary in a democratic society" criterion: see decision para. 106. If, contrary to the Applicants' case, the Court considers that the law sufficiently describes the constraints and safeguards applicable under the IOCA regime, the Applicants nevertheless invite the Court to conclude that the substantive content of those constraints and safeguards is insufficient, in all the circumstances, to satisfy the requirement of proportionality. The Applicants rely *mutatis mutandis* on the submissions they have made on the adequacy of the IOCA system in the context of the "in accordance with the law" issue: see the references at paragraph 9 above.

20. The Applicants also remind the Court that the Government apparently seeks to rely on the perfunctory ruling of the IPT on 21 April 2005 dismissing the Applicants' domestic

complaints about external interception under RIPA after 2 October 2000 so far as not determined by the IPT's reasoned (but erroneous) ruling on the "in accordance with the law" issue dated 9 December 2004: see paras 1 to 3 and 29 to 31 of the Applicants' Reply dated 30 June 2005 to the Government's Supplementary Observations.

21. The Applicants noted in that Reply that the Government submitted to the IPT "closed" evidence to which the Applicants had no access: see para. 5.c. That inevitably presents this court with considerable difficulty in attaching weight to any conclusions supposedly reached by the IPT: see para. 33.

22. There is a comparable problem as regards the proportionality of the measures complained of in the present case. The Government seeks to rely, among other things, on the "safeguards" provided by the Commissioner and former Interception of Communications Tribunal established under IOCA. But, as the Applicants have observed, each of these bodies operated within the "ring of secrecy". There was no prospect of any judicial proceedings observing the ordinary rules of fairness, independence, impartiality and publicity. In particular, the nature of the statutory procedure means that the Applicants have been denied the opportunity to make any informed representations in relation to their complaints; and/or have not been entitled to query or respond to any adverse references to them. As the Court knows, the former Tribunal purported to dismiss the Applicants' complaint in a single, opaque paragraph in its letter of 16 December 1999 (submitted with the original application).

23. That contrasts with the German system in which a person aggrieved by measures imposed under the G10 Act has, in almost every case, recourse to judicial review in the courts. Under the G10 Act as modified following the BVerfG judgment of July 1999, effective judicial review was facilitated by the duty, in most cases, to notify the subject that measures have been imposed. Under the IOCA system, no such notice could be given: on the contrary, the Government adopted (and still adopts under RIPA) a "neither confirm nor deny" approach. That seriously hampers the effectiveness of even the limited "safeguards" provided under IOCA. In the *AEIH and Ekimdzhien v. Bulgaria* case

(above, paragraph 8), the Court similarly attached weight to the fact that those subject to monitoring under the Bulgarian legislation were prevented from knowing -- even after the event -- that they had been the subject of secret monitoring, by contrast with the position under the G10 Act: see judgment, paras. 90 and 91.

24. The Applicants also observe that, whatever "closed" material the former Tribunal might have considered in the present case before summarily dismissing the Applicants' complaints in December 1999, the Government has placed no material before the Court enabling it to conclude that interception and subsequent processing of these Applicants' communications served any legitimate aim, or was necessary or proportionate to such aim as it may have been intended to pursue.

25. As the Court has repeatedly pointed out in its case-law, assessment of whether a respondent Government has established that an interference is "necessary in a democratic society" is not undertaken in the abstract but entails an examination of the specific facts of each case: "all the circumstances of the case", as the Court put it in its *Klass and others* judgment (Series A no. 28) at para. 50. The Applicants respectfully submit that where the Government declines to share with the Court any material capable of elucidating the specific facts and circumstances, the Court should be very slow to accede to Government submissions that the necessity test is satisfied. Moreover the inability of the Court (and the Applicants) to examine the factual basis for rejecting their complaints denies the Applicants any practical and effective means of ensuring that their Convention rights are safeguarded.

Concluding remarks

26. The Court now has the advantage of successive rounds of submissions from the parties on the issues raised by the Applicants' complaints. The case self-evidently raises serious and important points of Convention principle. Whatever the Court's ultimate view of the balance of argument, the Applicants respectfully suggest that they are at minimum entitled to have their complaints declared admissible and to receive the judgment of the Court on the merits.

27. The Applicants invite the Court to find that the Government have failed to establish that the interference with Article 8(1) rights in this case was permitted under the "in accordance with the law" or "necessary in a democratic society" limbs of Article 8(2), and to give judgment in the Applicants' favour.

28. The Applicants renew their suggestion that the Court would be assisted by a hearing in this case, for the reasons given previously (see paras. 11 and 12 of the Applicants Additional Observations dated 27 March 2006) and because of the additional issues raised by the comparison between the IOCA system and the system considered by the Court in the *Weber* case. The Court will recall that the German system features in the comparative analysis contained in the expert evidence submitted by both parties.

Richard Clayton QC

Gordon Nardell

Alex Gask, Solicitor, Liberty Legal Department
on behalf of the Applicants
Date: 12 October 2007