IN THE INVESTIGATORY POWERS TRIBUNAL **Case No. IPT/15/110/CH**

BETWEEN:

PRIVACY INTERNATIONAL

Claimant

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS
(2) SECRETARY OF STATE FOR THE HOME DEPARTMENT
(3) GOVERNMENT COMMUNICATIONS HEADQUARTERS
(4) SECURITY SERVICE
(5) SECRET INTELLIGENCE SERVICE

Respondents

SKELETON ARGUMENT
ON BEHALF OF THE RESPONDENTS
On sharing of BPD/BCD
for hearing on 8-10 March 2017

The issue

1. In its October 2016 judgment, and subsequent order of 31 October 2016, the Tribunal held that the BPD and BCD regimes were lawful under Article 8 ECHR from the dates of their respective avowal, and unlawful prior to those dates. However, the Tribunal wished to give "*further consideration...to the provisions for safeguards and limitations in the event of transfer by the SIAs to other bodies, such as their foreign partners and UK Law Enforcement Agencies*." The remaining issue therefore concerns transfer of BPD and BCD by the SIAs to non-SIA third parties, in particular *"UK law enforcement agencies, commercial companies or foreign liaison partners"* (Claimant's skeleton, §3(b)).

The law

2. As the Tribunal held at §37 of its judgment in *Liberty/Privacy*, in order for an interference to be "*in accordance with the law*":

> "*i) there must not be an unfettered discretion for executive action. There must be controls on the arbitrariness of that action.*
>
> *ii) the nature of the rules must be clear and the ambit of them must be in the public domain so far as possible, an "adequate indication" given (Malone v*

UK [1985] 7 EHRR 14 at paragraph 67), so that the existence of interference with privacy may in general terms be foreseeable..."

See also *Bykov v. Russia*[1], at §78, quoted at §37 of *Liberty/Privacy*.

3. As the Tribunal also noted in *Liberty/Privacy*, in the field of national security much less is required to be put into the public domain and therefore the degree of foreseeability must be reduced, because otherwise the whole purpose of the steps taken to protect national security would be put at risk (see §§38-40 and §137). See also in that respect, *Malone v UK*[2] (at §§67-68m), *Leander v Sweden*[3] at §51 and *Esbester v UK*[4], quoted at §§38-39 of *Liberty/Privacy*. Thus, as held by the Tribunal in the *British Irish Rights Watch* case[5] (a decision which was expressly affirmed in the *Liberty/Privacy* judgment at §87): "*foreseeability is only expected to a degree that is reasonable in the circumstances, and the circumstances here are those of national security...*" (§38)

4. Thus, the national security context is highly relevant to any assessment of what is reasonable in terms of the clarity and precision of the law in question and the extent to which the safeguards against abuse must be accessible to the public (see §§119-120 of the *Liberty/Privacy* judgment).

5. As to the procedures and safeguards which are applied, two points are to be noted.

   5.1. It is not necessary for the detailed procedures and conditions which are observed to be incorporated in rules of substantive law. That was made clear at §68 of *Malone* and §78 of *Bykov*; and was reiterated by the Tribunal at §§118-122 of *Liberty/Privacy*. Hence the reliance on the Code in *Kennedy v United Kingdom*[6] at §156 and its anticipated approval in *Liberty v United Kingdom*[7] at §68 (see §118 of *Liberty/Privacy* and also *Silver v United Kingdom*[8]).

   5.2. It is permissible for the Tribunal to consider rules, requirements or arrangements which are "below the waterline" i.e. which are not publicly accessible. In *Liberty/Privacy* the Tribunal concluded that it is "*not necessary that the precise details of all of the safeguards should be published, or contained in legislation, delegated or otherwise*" (§122), in order to satisfy the "in accordance with the law" requirement; and that the Tribunal could permissibly consider the "*below the waterline*" rules, requirements or arrangements when assessing the ECHR compatibility of the regime (see §§50, 55, 118, 120 and 139 of *Liberty/Privacy*). At §129 of *Liberty/Privacy* the Tribunal stated:

[1] Appl. no. 4378/02, 21 January 2009.
[2] (1984) 7 EHRR 14.
[3] [1987] 9 EHRR 433.
[4] [1994] 18 EHRR CD 72.
[5] IPT decision of 9 December 2004.
[6] [2011] 52 EHRR 4.
[7] [2009] 48 EHRR.
[8] [1983] 5 EHRR 347.

"*Particularly in the field of national security, undisclosed administrative arrangements, which by definition can be changed by the Executive without reference to Parliament, can be taken into account, provided that what is disclosed indicates the scope of the discretion and the manner of its exercise...This is particularly so where:*

i. The Code...itself refers to a number of arrangements not contained in the Code...

ii. There is a system of oversight, which the ECHR has approved, which ensures that such arrangements are kept under constant review."

5.3. Those conclusions were reached in the context of the s.8(4) RIPA interception regime. They are equally applicable to the s.94 and BPD regimes to which published Handling Arrangements and *"below the waterline"* arrangements apply and where there is similar oversight by the Intelligence Services Commissioner and the Interception of Communications Commissioner.

6. In the context of interception, the ECtHR has developed a set of minimum safeguards in order to avoid abuses of power. These are referred to as 'the *Weber* requirements'. At §95 of *Weber*[9], the ECtHR stated:

> "*In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: (1) the nature of the offences which may give rise to an interception order; (2) a definition of the categories of people liable to have their telephones tapped; (3) a limit on the duration of telephone tapping; (4) the procedure to be followed for examining, using and storing the data obtained; (5) the precautions to be taken when communicating the data to other parties; and (6) the circumstances in which recordings may or must be erased or the tapes destroyed.*" (numbered items added for convenience, see §33 of *Liberty/Privacy*)

(And see also *Valenzuela Contreras v Spain*[10] at §59)

7. However it is important to recognise what underpins the *Weber* requirements, as highlighted at §119 of the *Liberty/Privacy* judgment. In particular, §106 of *Weber* states as follows:

> "*The Court reiterates that when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life,* ***it has consistently recognised that the national***

[9] (2008) 46 EHRR SE5.
[10] (1999) 28 EHRR.

authorities enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security *(see, inter alia, Klass and Others, cited above, p. 23, § 49; Leander, cited above, p. 25, § 59; and Malone, cited above, pp. 36-37, § 81).* ***Nevertheless, in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse*** *(see Klass and Others, cited above, pp. 23-24, §§ 49-50; Leander, cited above, p. 25, § 60; Camenzind v. Switzerland, judgment of 16 December 1997, Reports 1997-VIII, pp. 2893-94, § 45; and Lambert, cited above, p. 2240, § 31).* ***This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law*** *(see Klass and Others, cited above, pp. 23-24, § 50).*" (emphasis added)

8. The Tribunal in *Liberty/Privacy* placed considerable reliance on oversight mechanisms in reaching their conclusion that the intelligence sharing regime and the s.8(4) RIPA regime were Article 8 compliant. In particular:

   8.1. The role of the Commissioner and "*his clearly independent and fully implemented powers of oversight and supervision*" have been long recognised by the ECtHR, as is evident from *Kennedy* at §§57-74, 166, 168-169 (see *Liberty/Privacy* at §§91-92). This is a very important general safeguard against abuse. In *Liberty/Privacy* the Tribunal relied, in particular, on his duty to keep under review the adequacy of the arrangements required by statute and by the Code, together with his duty to make a report to the Prime Minister if at any time it appeared to him that the arrangements were inadequate.

   8.2. The advantages of the Tribunal as an oversight mechanism were emphasised at §§45-46 of *Liberty/Privacy*, including the "*very distinct advantages*" over both the Commissioner and the ISC for the reasons given at §46 of the judgment.

   8.3. In addition the ISC was described as "*robustly independent and now fortified by the provisions of the JSA*" (see §121 of *Liberty/Privacy*) and therefore constituted another important plank in the oversight arrangements.

   8.4. Consequently there is a need to look at all the circumstances of the case and the central question under Art. 8(2) is whether there are: "*...adequate arrangements in place to ensure compliance with the statutory framework and the Convention and to give the individual adequate protection against arbitrary interference, which are*

sufficiently accessible, bearing in mind the requirements of national security and that they are subject to oversight." (see §125 of the *Liberty/Privacy* judgment)

Sharing of BPD/BCD with foreign partners and LEAs

9. There are considerable limits on the Respondents' ability to address in OPEN the matters which are relevant to the restrictions which might be placed in relation to sharing of BPD or BCD with LEAs and foreign partners if it were to occur. CLOSED evidence has been filed, of which some has been disclosed into OPEN. See:

   9.1. GCHQ's OPEN statement of 9 February 2017

   9.2. Security Service's OPEN Statement of 10 February 2017; and

   9.3. SIS's Amended OPEN Statement of 3 March 2017.

10. The SIAs can neither confirm nor deny whether they have agreed to share or in fact have shared or do share BPD or BCD with either foreign liaison or LEA: see GCHQ's statement of 9.2.17, §7; SyS's statement of 10.2.17, §§8-10; SIS's statement of 8.2.17, §§9 and 11. The matters set out at §52 of the Claimant's skeleton argument in reliance on alleged "Snowden documents" are also neither confirmed nor denied.

11. The Respondents do, however, assert that it would be lawful to share with foreign partners and LEAs, and set out in the Annex to this skeleton the safeguards and policies which would apply were they to do so.

12. In summary, in relation to **BPD**:

   12.1. Any sharing of BPD must be authorised in advance by a senior individual within the sharing Agency: see Joint SIA BPD Policy of February 2015 (Annex, §28)

   12.2. The relevant necessity and proportionality tests for onward disclosure under the SSA or ISA would have to be met: Joint SIA, BPD Policy of February 2015 (Annex, §28) Cross-SIA OPEN BPD Handling Arrangements, §§5.2, 6.1 (Annex, §29), as would the statutory safeguards under the SSA, ISA, CTA, HRA, DPA and OSA (Annex, §§3-27).

   12.3. Guidance on the meaning of "necessity" and "proportionality" is given: Cross-SIA OPEN BPD Handling Arrangements, §§6.2, 6.3(Annex, §29)

   12.4. Any data shared with other organisations would be shared on the basis that it must not be shared beyond the recipient organisation unless explicitly agreed in advance, or approved through the Action-on process. Action-on is a process which is used by each of the SIAs. (Annex, §31); see Joint SIA BPD Policy (Annex, §28).

12.5. Before disclosing BPD, as part of the consideration of proportionality, staff must *"consider whether other, less intrusive methods can be used to achieve the desired outcome"* Cross-SIA OPEN BPD Handling Arrangements, §5.2, and also §6.3 (Annex A, §29).

12.6. Sensitive BPDs, or fields within a BPD containing sensitive data, must be protected if it is not judged to be necessary or proportionate to share them: Joint SIA BPD Policy (Annex, §28)

12.7. Before disclosing any BPD, staff must take reasonable steps to ensure the intended recipient *"has and will maintain satisfactory arrangements for safeguarding the confidentiality of the data"* and also ensuring that it is "securely handled" or have received satisfactory assurances from the intended recipient with respect to such arrangements Cross-SIA OPEN BPD Handling Arrangements, §6.4 (Annex, §29).

12.8. Detailed policies exist which govern consideration of whether or not to share BPD; obtaining adequate assurances from potential recipients of BPD; and monitoring compliance with those assurances. These would include:

12.8.1. Carrying out due diligence, including into:

12.8.1.1. The nature and extent of any handling arrangements for BPD within the recipient partner organisation, in particular in relation to access, examination, storage and onward disclosure of BPD/information derived from BPD;

12.8.1.2. The law of the particular jurisdiction of the recipient;

12.8.1.3. Existing knowledge of the partner's capabilities, intent and practice, and history of compliance;

12.8.1.4. The necessity of sharing, including to meet the relevant statutory purpose of the sharing Agency;

12.8.1.5. The recipient's storage systems;

12.8.2. Obtaining assurances to ensure that the partner complies with equivalent standards as would apply to the Agency's own staff and procedures;

12.8.3. Refusing to share BPD in the absence of satisfactory due diligence or assurances;

12.8.4. Monitoring those assurances, including both by the Action-on process but also by conducting regular meetings, visits and discussions with any partners who might be in receipt of BPDs.

(See Annex, §§50-63)

The precise nature of the policies in place varies across the agencies (See Annex, §§37-40, 45-46 and 50-63). However, those policies and practices do not exist in isolation; the policy/practice of one agency would be taken into account by others e.g. by the Security Service who in addition to applying their own policy would *"[t]ake into account the approach taken by any other SIAs who may have shared bulk data and have regard to any protocols/understandings that the other agencies may have used/followed"* (Annex, §46(a)), and by GCHQ (Annex, §39(d)).

12.9. Disclosure of the whole or a subset of a BPD is subject to internal authorisation procedures in addition to those which apply to an item of data. An application must be made to a senior manager designated for the purpose. This must describe the BPD intended to be disclosed, set out the operational and legal justification for the proposed disclosure, and whether any caveats or restrictions should be applied to the proposed disclosure. This is so the senior manager can then consider the relevant factor with operational, legal and policy advice taken as appropriate. See Cross-SIA OPEN BPD Handling Arrangements, §6.7 (Annex, §29).

12.10. In difficult cases, the relevant Intelligence Service may seek guidance or a decision from the Secretary of State: Cross-SIA OPEN BPD Handling Arrangements, §6.7 (Annex, §29).

12.11. *"Wider legal, political and operational risks would also have to be considered, as appropriate"*: Joint SIA BPD Policy (Annex, §28)

12.12. The disclosure of a BPD (as in the case of its acquisition or retention) is subject to scrutiny in each Intelligence Service by an internal Review Panel, whose functions include *"to ensure that...any disclosure is properly justified"*: Cross-SIA OPEN BPD Handling Arrangements, §8.1 (Annex, §30).

13. The Agency-specific Handling Arrangements, and relevant authorisation forms, reflect the requirements of the overarching Cross-SIA OPEN BPD Handling Arrangements. See:

13.1. The GCHQ BPD Handling Arrangements and its Bulk Personal Data Acquisition Retention (BPDAR): Annex, §§35 and 36.

13.2. The Security Service's BPD Guidance of March 2015, its BPD Handling Arrangements of November 2015 and its Form for Sharing: Annex, §§42-44.

13.3. SIS's Bulk Data Acquisition, Exploitation and Retention policy from 2009 onwards and the SIS BPD Handling Arrangements of November 2015: Annex, §§47-49.

14. As for **BCD**:

14.1. Disclosure of an entire BCD or a subset of a BCD outside the Intelligence Service may only be authorised by a Senior Official, equivalent to a member of the Senior Civil Service, or the Secretary of State: see the Cross-SIA BCD Handling Arrangements, §4.4.1 (Annex, §64).

14.2. The relevant necessity and proportionality tests for onward disclosure under the SSA or ISA would have to be met: Cross-SIA BCD Handling Arrangements, §§4.4.1-4.4.2 (Annex, §64) as would the statutory safeguards under the SSA, ISA, CTA, HRA, DPA and OSA (Annex, §§3-27).

14.3. Guidance on the meaning of "*necessity*" and "*proportionality*" is given: Cross-SIA OPEN BCD Handling Arrangements, §§4.4.3-4.4.4 (Annex, §64)

14.4. Any data shared with other organisations would be shared on the basis that it must not be shared beyond the recipient organisation unless explicitly agreed in advance, or approved through the Action-on process. Action-on is a process which is used by each of the SIAs. (Annex, §65).

14.5. Before disclosing BCD, as part of the consideration of proportionality, staff must "*consider whether there is a reasonable alternative that will still meet the proposed objective – i.e. which involves less intrusion.*" Cross-SIA OPEN BCD Handling Arrangements, §4.4.4 (Annex, §64).

14.6. Before disclosing any BCD, staff must take reasonable steps to ensure the intended recipient "*has and will maintain satisfactory arrangements for safeguarding the confidentiality of the data*" and also ensuring that it is "*securely handled*" or have received satisfactory assurances from the intended recipient with respect to such arrangements Cross-SIA OPEN BCD Handling Arrangements, §4.4.5 (Annex, §64).

14.7. Again, as with BPD, there are policy requirements in place requiring:

14.7.1. That recipients accord the material a level of protection equivalent to the SIAs' own safeguards (in the case of GCHQ these are the safeguards applicable by RIPA to all operational data even if it was not obtained under RIPA powers);

14.7.2. Special care must be taken to ensure that the acquisition, analysis, retention and dissemination of any legally privileged or confidential journalistic material is necessary and proportionate. Such data may even be removed.

Again, the policies in place varies across the agencies (See Annex, §§69-72 and75-76). Again, however, the policy/practice of one agency would be taken into account into account by another in addition to applying their own policy (Annex, §76(a)).

15. Again, the Agency-specific Handling Arrangements reflect the requirements of the overarching Cross-SIA OPEN BCD Handling Arrangements. See:

    15.1. The GCHQ BCD Handling Arrangements of November 2015: Annex, §68;

    15.2. The Security Service's BCD Handling Arrangements of November 2015: Annex, §74.

16. In light of the above, the Claimant's submission that *"there are no published arrangements governing the safeguards to be applied when considering sharing of data with foreign intelligence services or other UK law enforcement agencies"* (Claimant's skeleton, §64) is wrong. Furthermore, the Respondents submit that the published arrangements set out above, and in detail in Annex A, satisfy the requirement in *Weber* at §106 that "*there exist adequate and effective guarantees against abuse*" and in *Liberty/Privacy* at §125 that there are "*...adequate arrangements in place to ensure compliance with the statutory framework and the Convention and to give the individual adequate protection against arbitrary interference, which are sufficiently accessible, bearing in mind the requirements of national security and that they are subject to oversight.*"

17. The Claimant also asserts that there is no Commissioner oversight over sharing of BCD/BPD (Claimant's skeleton, §65). The Intelligence Services Commissioner and Interception of Communications Commissioner have oversight and access to all GCHQ, Security Service and SIS material in relation to BPD/BCD governance (as applicable), including that relating to sharing, were it to occur. The Tribunal has upheld the adequacy of the Commissioners' oversight throughout (at least) the post-avowal period.[11] See also:

    17.1. BPD: The Intelligence Services Commissioner Additional Review Functions (Bulk Personal Datasets) Direction 2015, pursuant to which the Prime Minister, pursuant to his power under s.59(a) of RIPA, directed the Intelligence Services Commissioner to *"continue to keep under review the acquisition, use, retention and* ***disclosure*** *by the* [SIAs] *of bulk personal datasets, as well as the adequacy of safeguards against misuse."* and to *"assure himself that the acquisition, use, retention* ***and disclosure*** *of bulk personal datasets does not occur except in accordance with"* the relevant sections of the SSA 1989 and ISA 1994 and to *"seek to assure himself of the adequacy of the [SIAs'] handling arrangements and their compliance therewith."* (emphasis added) (see Annex, §33).

[11] Since 2010 in the case of BPD and since July 2016 in the case of BPD (October 2016 judgment, §§80-82).

17.2. BCD: the Interception of Communications Commissioner has oversight over all aspects of disclosure of BCD (see Annex, §33).

18. The Claimants' submissions in this regard are simply unsustainable. There plainly is Commissioner oversight over sharing/disclosure of BPD/BCD. It is a further very important general safeguard against abuse.

Industry partners

19. GCHQ shares BPD/BCD with industry partners for the purpose of developing its systems. Its safeguards are explained at §41 of the Annex. The Security Service and SIS neither confirm nor deny whether they share bulk data with industry partners. Were they to do so, the policies which apply to disclosure of BPD/BCD generally would apply.

EU law

20. The Claimant repeats (at skeleton §§66-67) its submission that BCD may not be transferred out of the EU, and that in relation to some of the data that may be held in BPDs, the safeguards identified in *Watson* must be adopted. The Respondents have already responded to those submissions at Section E of their skeleton argument on EU law and proportionality, and do not repeat their position.

JAMES EADIE QC

ANDREW O'CONNOR QC

ROBERT PALMER

RICHARD O'BRIEN

3 March 2017