Neutral Citation Number: [2022] EWHC 770 (QB)

Case No: CO/4253/2018

IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
DIVISIONAL COURT

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 4 April 2022

Before :
PRESIDENT OF THE QUEEN'S BENCH DIVISION
MR JUSTICE JOHNSON

- -

Between :

THE QUEEN
on the application of
PRIVACY INTERNATIONAL **Claimant**

- and -

INVESTIGATORY POWERS TRIBUNAL **Defendant**

-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 **Interested Parties**

- -
- -

Tom de la Mare QC, Ben Jaffey QC and Daniel Cashman (instructed by Bhatt Murphy) for the Claimant
Sir James Eadie QC, Andrew O'Connor QC and Richard O'Brien (instructed by Government Legal Department) for the Interested Parties
Angus McCullough QC and Adam Straw QC (instructed by the Special Advocates' Support Office) as Special Advocates

Hearing dates: 9 February 2022 – 10 February 2022
Further written submissions: 3 March 2022, 11 March 2022, 15 March 2022, 16 March 2022

- -

Approved Judgment

Dame Victoria Sharp P:

1. This is the judgment of the court.

2. This claim concerns the regulation of sharing Bulk Personal Datasets ("BPDs") by MI5, MI6 and GCHQ ("the Agencies") with foreign intelligence agencies.

3. In a judgment dated 23 July 2018 ("the 2018 judgment") the Investigatory Powers Tribunal ("the Tribunal") concluded by a majority that the regulatory regime was compatible with article 8 of the European Convention of Human Rights ("ECHR") in the period from 2015 to 2017. In particular, it concluded that adequate safeguards were in place to comply with article 8. The claimant seeks judicial review of that decision. The issue was described by the Tribunal as "a matter of the greatest importance", in part because BPDs disclosed by the Agencies might be unlawfully used in contexts involving a risk to life (the claimant identified the possibility of rendition operations, or drone strikes).

4. Part of the reasoning of the Tribunal was given "in closed": that reasoning was not published or disclosed to the claimant (save by way of an "open" summary), because the Tribunal considered that to do so would be damaging to the interests of national security.

5. On 8 October 2019 Supperstone J made case management directions for these proceedings. The directions made provision for the appointment of Special Advocates who could examine all of the material that was put before the Tribunal, and the entirety of the Tribunal's reasoning, and then represent the claimant's interests in closed proceedings. The Special Advocates have advanced closed arguments in support of the claimant's claim. So far as was possible, consistent with the interests of national security, extracts from the Special Advocates' closed arguments were disclosed to the claimant. Permission to claim judicial review was granted by Swift J on 22 July 2020.

6. We heard open submissions from Tom de la Mare QC on behalf of the claimant, and Sir James Eadie QC on behalf of the Agencies. These submissions addressed, primarily, the question of whether the Tribunal had correctly identified the safeguards that are required by article 8 for the sharing of BPDs with foreign agencies. We heard closed submissions from Angus McCullough QC as Special Advocate, and Sir James Eadie QC on behalf of the Agencies. These submissions addressed the detail of the closed evidence and the Tribunal's closed judgments, and, in particular, the Tribunal's assessment that the safeguards in place met the required standards.

7. In this judgment we deal with all of the arguments that have been raised, both in open and in closed, so far as it is possible to do so without disclosing material that the Tribunal treated as closed. Some of our reasoning is set out in a separate closed judgment.

8. Mr McCullough QC confirmed, in the course of the closed hearing, that he did not consider that the closed arguments raise any point of legal principle. Nothing in our closed judgment raises any point of legal principle. Rather, our closed judgment addresses the arguments of the Special Advocates as to the application of the legal principles to the facts.

Use of BPDs by the Agencies

9. Prior to March 2015 there was no public acknowledgement ("avowal") of the use of BPDs by the Agencies. On 12 March 2015 the Intelligence and Security Committee of Parliament ("the ISC") published a report, "Privacy and Security: A modern and transparent legal framework." The report avows, for the first time, that the Agencies acquire and use BPDs. These are datasets that contain personal information about a large number of people. The report expresses concerns about the regulation of the acquisition and use of BPDs by the Agencies.

10. In a judgment dated 17 October 2016 ("the 2016 judgment"), the Tribunal sets out the following explanation of BPDs:

> "(1) A Bulk Personal Dataset… is a dataset that contains personal data about individuals, the majority of whom are unlikely to be of intelligence interest, and that is incorporated into an analytical system and used for intelligence purposes. Typically, such datasets are very large, too large to be processed manually.
>
> (2) The [Agencies] obtain and exploit BPD for several purposes:
> - to help identify subjects of interest or unknown people that surface in the course of investigations;
> - to establish links between individuals and groups;
> - or else to improve understanding of targets' behaviour and connections;
> - and to verify information obtained through other sources.
>
> (3) BPD obtained and exploited by the [Agencies] includes a number of broad categories of data. By way of example only these include: biographical and travel (eg passport databases); communications (eg telephone directory); and financial (eg finance related activity of individuals).
>
> (4) While each of these datasets in themselves may be innocuous, intelligence value is added in the interaction between multiple datasets. One consequence of this is that intrusion into privacy can increase.
>
> (5) BPD is operationally essential to the [Agencies] and growing in importance and scale of holdings. Examples of the vital importance of BPD to intelligence operations include… identifying foreign fighters [and] preventing access to firearms."

11. We were shown, in the closed proceedings, examples of records extracted from BPDs. We are satisfied that the above explanation is accurate and sufficiently comprehensive to encapsulate the nature of BPDs in a way that enables assessments to be made as to their capacity to impact on privacy rights.

12. The Tribunal summarises, in its 2016 judgment, the evidence about BPDs that was given by MI5:

> "44) MI5 acknowledges that it holds the following categories of BPD:

- [Law Enforcement Agencies]/Intelligence. These datasets primarily contain operationally focussed information from law enforcement or other intelligence agencies.

- Travel. These datasets contain information which enable the identification of individuals' travel activity.

- Communications. The datasets allow the identification of individuals where the basis of information held is primarily related to communications data, eg a telephone directory.

- Finance. These datasets allow the identification of finance related activity of individuals.

- Population. These datasets provide population data or other information which could be used to help identify individuals, eg passport details.

- Commercial. These datasets provide details of corporations/individuals involved in commercial activities.

45) A number of these datasets will be available to the public at large. Some of these publicly available datasets will be sourced from commercial bodies, and we will pay for them (as another public body or a member of the public could do). MI5 also acquired BPD from Government departments, from [MI6] and GCHQ and from law enforcement bodies.

46) MI5's holding of passport information is key to our ability to be able to investigate travel activity. Holding that data in bulk, and being able to cross-match this to other data and other BPD held, is what enables us to find the connection and 'join the dots.' That would simply not be possible if we did not hold the bulk data in the first place. Using travel data, for example, to try and establish the travel history of a particular individual will necessarily involve holding, and searching across a range of BPD and other data that we hold, and it is through fusing these that we are able to resolve leads and identify particular individuals, with high reliability, at pace and with minimum intrusion.

47) Holding the data in bulk (and holding data relating to persons not of intelligence interest) is an inevitable and necessary prerequisite to being able to use these types of dataset to make the right connections between disparate pieces of information. Without the haystack one cannot find the needle; and the same result cannot be achieved (without fusion/combination) through carrying out a series of individual searches or queries of a particular dataset (or a number of datasets).

48) It is also relevant to note that as BPDs are searched electronically there was inevitably significantly less intrusion into individuals' privacy, as any data which has not produced a 'hit' will not be viewed by the human operator of the system, but only searched electronically."

13. The following facts were agreed between the parties in the proceedings before the Tribunal:

> "(i) GCHQ, MI5 and MI6 collect and hold BPDs, on their respective analytical systems.
>
> (ii) BPDs consist of large amounts of personal data: The majority of individuals whose personal data is contained in a BPD will be of no intelligence interest.
>
> (iii) Multiple BPDs are analysed together to obtain search results.
>
> (iv) BPD may be acquired through overt and covert channels.
>
> (v) BPD can contain sensitive personal data as defined under s2 of the Data Protection Act 1998 and/or information covered by legal professional privilege, journalistic material and financial data.
>
> (vi) GCHQ, MI5 and MI6 share BPDs, and BPDs may be shared with their foreign partners and/or may be disclosed to persons outside the agencies, as described in their Handling Arrangements.
>
> (vii) MI5, GCHQ and MI6 each acquire BPDs from other Government departments. …GCHQ, MI5 and MI6 do not currently hold and have never held a BPD of medical records, although medical data may appear in BPDs.
>
> (viii) There have been instances of non-compliance with BPD safeguards at GCHQ, MI5 and MI6, as disclosed in the various Commissioners' Reports.
>
> (ix) There was no statutory oversight of BPDs by the [Intelligence Services] Commissioner prior to the March 2015 ISC Report.
>
> (x) Prior to the publication of that ISC Report, the holding of BPDs was not publicly acknowledged."

14. It is thus in the public domain that the Agencies use BPDs in the way described. At the time of the hearing before the Tribunal, the Agencies had not stated, in public, whether any of the Agencies had ever shared BPDs with foreign intelligence agencies (agreed fact (vi) only extends to the possibility that this may happen). The true position was revealed to the Tribunal in its closed hearings. The Tribunal considered that this was a legitimate application of the "neither confirm nor deny" ("NCND") policy (see at [61]). The Tribunal's 2016 judgment proceeds on the assumption that sharing has taken place. We do likewise (see paragraphs 66 and 77-80 below).

The legal regime regulating BPDs

15. The Tribunal set out the regime that regulates BPDs in great detail in appendix B to its 2016 judgment. It also set out, as appendix 2 to its 2018 judgment, (and again in great detail – running to 38 pages) the handling arrangements and other guidance in relation to sharing BPDs outside the Agencies. We summarise the principal features.

The Agencies

16. The Agencies may only disclose information where that is necessary for the proper discharge of their functions (here, to protect the interests of national security) – see s2(2)(a) of the Security Service Act 1989 (so far as MI5 is concerned), and ss2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994 (so far as, respectively, MI6 and GCHQ are concerned). These statutory limits apply to the disclosure of information to foreign agencies.

17. The Agencies are each a public authority within the meaning of the Human Rights Act 1998. By s6(1), it is unlawful for the Agencies to act in a way that is incompatible with a Convention right. Article 8 ECHR is a Convention right. Article 8(1) provides that "everyone has the right to respect for his private and family life, his home and his correspondence." By article 8(2) there must be no interference with this right except where that is "in accordance with the law" and is "necessary in a democratic society" for a specified aim (here, the interests of national security).

The Commissioners

18. The offices of the Interception of Communications Commissioner and the Intelligence Services Commissioner ("the Commissioners") were established by ss57 and 59 of the Regulation of Investigatory Powers Act 2000. These provisions provided that (amongst other matters):

    (1) Appointments to those offices must be made by the Prime Minister.

    (2) The Commissioners must hold (or have held) high judicial office.

    (3) The Interception of Communications Commissioner was required to keep under review (among other matters) the exercise and performance by the Agencies of powers and duties conferred or imposed in respect of the acquisition and disclosure of communications data.

    (4) The Commissioners must give the Tribunal such assistance as it requires (including by providing an opinion as to any issue falling to be determined by the Tribunal).

19. By s59A of the 2000 Act, the Intelligence Services Commissioner was additionally required, so far as directed by the Prime Minister, to keep under review the carrying out of any aspect of the functions of (among others) the Agencies. On 11 March 2015 the Prime Minister gave a direction under s59A of the 2000 Act – the Intelligence Services Commissioner Additional Review Functions (Bulk Personal Datasets) Direction 2015. This directed the Intelligence Services Commissioner to:

> "continue to keep under review the acquisition, use, retention and disclosure by the [Agencies] of [BPDs], as well as the adequacy of safeguards against misuse [and to] assure himself that the acquisition, use, retention and disclosure of [BPDs] does not occur except in accordance with [the 1989 and 1994 Acts and to] seek to assure himself of the adequacy of the [Agencies'] handling arrangements and their compliance therewith."

20. The Intelligence Services Commissioner was Sir Mark Waller in the period 2011-2016. The Interception of Communications Commissioner was Sir Stanley Burnton in the period 2015-2017.

The policy, handling arrangements and oversight

21. BPD policy came into force in February 2015. This applies to each of the Agencies and represents the agreed policy for each of the Agencies. The Tribunal explains in its 2016 judgment (at [39]) that the policy sets out "[s]pecific, detailed measures… which are designed to limit access to data to what is necessary and proportionate, to ensure that such access is properly audited, and to ensure that disciplinary measures are in place for misuse." The policy makes the following provision in respect of the sharing of BPDs:

> "**D. Sharing**
> …
> When sharing BPD the supplying Agency must be satisfied that it is necessary and proportionate to share the data with the other Agency/Agencies… A log of data sharing will be maintained by each agency;
>
> The sharing of BPD must be authorised in advance by a senior individual within each Agency, and no action to share may be taken without such authorisation;
> …
> *Were BPD to be shared with overseas liaison the relevant necessity and proportionality tests for onwards disclosure under the SSA or ISA would have to be met….*" [Underlining in original to denote a 'gist']

22. On 4 November 2015 the BPD "handing arrangements" were published. Paragraph 2.6 requires that that any disclosure of BPD has "clear justification, accompanied by detailed and comprehensive safeguards against misuse" and is "subject to rigorous oversight." Disclosure to a third party may only be made if that is necessary to achieve a defined objective (which may include the interests of national security) and is proportionate to that objective. Prior to any such disclosure, staff must take steps to ensure that the recipient "has and will maintain satisfactory arrangements for safeguarding the confidentiality of the data and ensuring that it is securely handled" or have received satisfactory assurances from the intended recipient. Additional safeguards are in place in the case of disclosure of the whole or a subset of a BPD (as opposed to a single item of data). This requires an application to a senior manager for authorisation. Each Agency is required to have an internal review panel to scrutinise the disclosure of BPD (amongst other matters) to ensure that it is properly justified. Each Agency must have an audit team that monitors the use of BPD in order to detect misuse.

23. The Handling Arrangements also deal with oversight. Each Agency must report its BPD operations to the relevant Secretary of State. The use (including disclosure) of BPDs was overseen by the Intelligence Services Commissioner on a regular six-monthly basis (except where oversight fell within the remit of the Interception of Communications Commissioner). Each Agency must ensure that it can demonstrate that proper judgments have been made on the necessity and proportionality of any disclosure of BPDs. Each Agency is required to satisfy the appropriate Commissioner that its policies and procedures provide adequate safeguards against misuse and are strictly complied with. Each Agency must provide the appropriate Commissioner with all such documents and information as may be required by the Commissioner.

24. The system of oversight which was then in place is described by the ISC in its March 2015 Report as follows:

> "157. …the rules governing the use of [BPDs] are not defined in legislation. Instead, the [Agencies] derive the authority to acquire and use [BPDs] from the general powers to obtain and disclose information (in support of their organisation's functions) that are afforded to the heads of each of the [Agencies] under the Intelligence Services Act 1994… and the Security Service Act 1989…
>
> 160. In terms of independent review, the Intelligence Services Commissioner has non-statutory responsibility for overseeing the [Agencies'] holdings of [BPDs]… The Commissioner explained to the Committee that he retrospectively reviews the [Agencies'] holdings of [BPDs] as part of his six-monthly inspection visits. This includes reviewing the intelligence case for holding specific datasets, necessity and proportionality considerations, the possible misuse of data and how that is prevented…
>
> Internal controls
>
> 161. The Agencies have told the Committee that the acquisition and use of [BPDs] is tightly controlled, and that the HRA 'triple test' (ie for a lawful purpose, necessary and proportionate) is considered both at the point of acquisition, and also before any specific searches are conducted against the data (which is when they consider the principal intrusion into an individual's privacy to occur).
>
> 162. Senior staff are responsible for authorising the acquisition of Bulk Personal Datasets. The Director General of MI5 explained:
>
> > …there are datasets that we deliberately choose not to reach for, because we are not satisfied that there is a case to do it, in terms of necessity and proportionality…
>
> The Agencies each have a review panel, chaired by a senior official, which meets every six months to review the [BPDs] currently held by the Agency… Datasets that are found not to have sufficient operational value are deleted.
>
> 163. The Agencies have said that they apply strict policy and process safeguards to control and regulate access to the datasets…. These controls include: i) Training, audit and disciplinary procedures… ii) Heightened safeguards for sensitive categories of information…
>
> We note that while these controls apply inside the Agencies, they do not apply to overseas partners with whom the Agencies may share the datasets…"

The Investigatory Powers Commissioner

25. Part 7 of the Investigatory Powers Act 2016 introduced a new regime for BPDs, and for the oversight of the Agencies. It came into force in September 2017. The office of the Investigatory Powers Commissioner ("IPCO") was established by s227 of the Investigatory Powers Act 2016, with effect from 29 January 2017. By s233 the

Investigatory Powers Commissioner must make an annual report to the Prime Minister (which must then, subject to specified sensitivities, be published by the Prime Minister).

26. IPCO's annual report for 2018 referred to the fact that the Tribunal had called for "a review of existing procedures at GCHQ in relation to sharing of intelligence and of bulk datasets… under the supervision of IPCO." IPCO's annual report for 2019 states:

> "In response, GCHQ conducted a detailed review of the processes and procedures governing decisions to share data in bulk with foreign partners and then implemented measures to bring about improvements. In the future, this area will be covered as part of our regular oversight and inspection arrangements.
>
> The main outcomes of GCHQ's review are as follows:
>
> Sharing of bulk data with foreign intelligence partners is now incorporated into our regular oversight and inspection processes;
> The review has brought new standardisation. Decisions and permissions to share are captured on a Data Sharing Permission (DSP) form and stored electronically in a central location;
> Each DSP records the necessity and proportionality of sharing a type of bulk data with the partner in question and how the partner safeguards operational data, confirms that the relevant [BPD] warrant permits overseas sharing, and also details the accesses covered and equity considerations;
> Each foreign partner has provided written assurance in relation to their handling of shared bulk data;
> A dedicated team is the formal coordination point and record keeper of DSPs for the sharing of bulk data with Five Eyes and other foreign partners; and
> GCHQ has invested in the development of a workflow tool to automate the DSP process by marrying operational data sharing in their systems to the DSPs. This provides a double-check capability that mitigates the risk of sharing without permission. An additional feature is the ability automatically to match warrants to operational purposes, thus reducing the burden on those checking that the appropriate operational purpose/s are present and correct.
>
> We anticipate that the measures taken by GCHQ including the automated workflow tool, when implemented, will improve compliance in this area. They will provide a centralised record of what data is shared with whom, where and why. The decisions about sharing will be accessible by GCHQ staff as required, by our inspectors and, when necessary, by the IPT and will meet the requirements described in the Tribunal's CLOSED [2018 judgment].
>
> <u>Bulk personal data (BPD)</u>
>
> Overall, administration of bulk personal datasets (BPDs) within GCHQ is to a high standard. During this reporting period GCHQ introduced a clear and auditable process when considering the classification of BPD. All decisions and details of the datasets are collated internally and recorded in an auditable manner. We intend to review this material at future BPD inspections."

The Investigatory Powers Tribunal

27. The Tribunal was established by Part 4 of the Regulation of Investigatory Powers Act 2000. By s65(2) of the 2000 Act, read with s7 Human Rights Act 1998, it is the only appropriate tribunal for determining a claim that the Agencies have acted in a way that is incompatible with a Convention right. The President of the Tribunal must hold (or must have previously held) high judicial office. At the time of the 2018 judgment there was no right of appeal from a decision of the Tribunal. An important part of the raison d'être of the Tribunal is to adjudicate on allegations that the Agencies have acted unlawfully and, where that has happened, to provide a remedy. It is part of the framework to ensure compliance with the legality requirements of article 8 ECHR. Many of its decisions have addressed those requirements.

Legality requirement of article 8 ECHR

28. The sharing of BPDs with a foreign agency will almost inevitably interfere with privacy rights guaranteed by article 8. It is therefore unlawful, unless it is justified in any particular case under article 8(2). That requires that the interference is "in accordance with the law" and is necessary for, and proportionate to, a legitimate aim, here the interests of national security. The obligation for any interference with privacy rights to be in accordance with the law requires (a) a sufficient legal framework to regulate the interference, and (b) compliance with that framework. This "addresses supremely important features of the rule of law" so as to ensure that the public is not vulnerable to interference with rights of privacy "by public officials acting [arbitrarily]" - *R (Gillan) v Commissioner of Police of the Metropolis* [2006] UKHL 12 [2006] 2 AC 307 *per* Lord Bingham at [34].

29. The safeguards that are required for the legal framework to be compatible with article 8 are well established and well known. The precise detail of what is required depends on the nature of the interference with privacy rights. In the context of retention of personal data by the police, there must be "clear, detailed rules governing… access of third parties… providing sufficient guarantees against the risk of abuse and arbitrariness… the rules need not be statutory, provided they operate within a framework of law and that there are effective means of enforcing them" – see *R (Catt) v Association of Chief Police Officers* [2015] AC 1065 *per* Lord Sumption JSC at [11].

30. Where interferences take place by the Agencies acting in secret, then "the risks of arbitrariness are evident" (*Malone v United Kingdom* (1985) 7 EHRR 14 at [67]). That is because any individual who is affected "will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings" (*Klass v Germany* (1979-80) 2 EHRR 214). That impacts on the nature of the regulatory safeguards that are required. In this context, "clear, detailed rules" are essential so as to provide "adequate and effective safeguards and guarantees against abuse" (*Zakharov v Russia* (2016) 63 EHRR 17).

31. The rules must make sufficient provision for the authorisation and supervision of actions by intelligence agencies that interfere with privacy rights – see *Weber v Germany* (2008) 46 EHRR SE5 at [106]:

> "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."

32. In carrying out that assessment what is required is (see *Klass* at [54]):

> "[a determination] whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the 'interference' to what is 'necessary in a democratic society…'"

33. In *Weber* the court summarised its previous case-law as to the minimum safeguards that are required to regulate "secret measures of surveillance" (in the specific context of telephone intercept)– see at [95] (with numbering added):

> "(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."

34. In *Kennedy v United Kingdom* (2011) 52 EHRR 4 the court concluded that the regulation of telephone intercept under UK law was compatible with article 8. It relied on the system of supervision that was in place, particularly:

(1) the role of the Interception of Communications Commissioner (noting that he was "independent of the executive" and had "held high judicial office", that his annual report was published, that he had access to all relevant documents and could require disclosure of any material he requires, and that he undertook a biannual review of a random selection of specific cases),

(2) the role of the Tribunal (which, "[u]nlike in many other domestic systems" could receive applications from anyone and which could require the provision of assistance from the Commissioner and which published its legal rulings),

(3) the obligation to maintain proper records by the Agencies,

(4) the absence of evidence of any significant shortcomings on the application and operation of the regime.

35. It concluded at [169]:

> "Having regard to the safeguards against abuse in the procedures as well as the more general safeguards offered by the supervision of the Commissioner and the review of the IPT, the impugned surveillance measures, insofar as they may have been applied to the applicant… are justified under art 8(2)."

36. In *Big Brother Watch v United Kingdom* (judgment 25 May 2021) the Grand Chamber of the European Court of Human Rights considered the safeguards that are required in the context of bulk interception of communications. It drew on its previous case law, including *Klass, Weber, Zakharov* and *Kennedy*. It considered whether there was a need "to develop the case-law" (see at [340]). It recognised (at [348]) that the first two *Weber*

criteria are not applicable to bulk interception (as opposed to targeted supervision). This meant (see at [349]-[350]):

> "349. …the importance of supervision and review will be amplified, because of the inherent risk of abuse and because the legitimate need for secrecy will inevitably mean that, for reasons of national security, States will often not be at liberty to disclose information concerning the operation of the impugned regime.
>
> 350. Therefore, in order to minimise the risk of the bulk interception power being abused, the Court considers that the process must be subject to "end-to-end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent *ex post facto* review. In the Court's view, these are fundamental safeguards which will be the cornerstone of any article 8 compliant bulk interception regime…"

37. The Court addressed the requirement of supervision at [356]:

> "Each stage of the bulk interception process – including… onward transmission… of the intercept material – should also be subject to supervision by an independent authority and that supervision should be sufficiently robust to keep the "interference" to what is "necessary in a democratic society". In particular, the supervising body should be in a position to assess the necessity and proportionality of the action being taken, having due regard to the corresponding level of intrusion into the Convention rights of the persons likely to be affected. In order to facilitate this supervision, detailed records should be kept by the intelligence services at each stage of the process."

38. At [362] the court observed that it had not previously "provided specific guidance regarding the precautions to be taken when communicating intercept material to other parties." It said that (1) such transmission should be limited to material that has been collected and stored in a Convention compliant manner, (2) the circumstances in which transfers may take place must be set out clearly in domestic law, (3) the transferring State must ensure that the receiving state has in place safeguards capable of preventing abuse and disproportionate interference, (4) the receiving state must guarantee secure storage of the material and restrict onward disclosure, (5) heightened safeguards are required in the case of material "requiring special confidentiality" (such as journalistic material), (6) the transfer of material should be subject to independent control.

39. The court was satisfied that the UK had in place sufficient safeguards in relation to the communication of intercepted material to third parties. In relation to the transfer of such material to foreign agencies, it said, at [396]:

> "…the transfer… to a foreign intelligence partner… would only give rise to an issue under Article 8 of the Convention if the intercepting State did not first ensure that its intelligence partner, in handling the material, had in place safeguards capable of preventing abuse and disproportionate interference, and

> in particular, could guarantee the secure storage of the material and restrict its onward disclosure."

40. The court was satisfied that these safeguards were provided by the statutory regime and the applicable code of practice. It also attached "particular weight" to "the oversight provided by the IC Commissioner and the IPT…" It found that the Interception of Communications Commissioner "provided independent and effective supervision" (see [412]) and the Tribunal provided "*Ex post facto* review" and "a robust judicial remedy" (see [413] and [415]). It described the role of the Commissioner and the Tribunal as providing "robust" safeguards (see at [425]). It therefore did not consider that the system in relation to the sharing of bulk intercept with foreign agencies was, in itself, flawed. It did, however, consider that there were failings in the broader system for bulk interception, including "the absence of independent authorisation, the failure to include the categories of selectors in the application for a warrant, and the failure to subject selectors linked to an individual to prior internal authorisation" (see at [425]).

The proceedings before the Tribunal

The claim

41. The claimant is a UK charity that was described by the Tribunal in its 2016 judgment as "a Non-Governmental Organisation, working in the field of defending human rights at both national and international levels." As part of that, it seeks to ensure that surveillance and the collection and use of data is carried out within the law and in a manner that is compatible with the right to privacy.

42. On 5 June 2015 the claimant brought a claim before the Tribunal challenging the Agencies' acquisition, use, retention, disclosure, storage and deletion of BPDs. The claim was precipitated by the publication of the ISC report (see paragraph 9 above), and the revelations as to the use of BPDs by the Agencies. The claim was amended in September 2015 to extend the challenge to a particular type of BPD, namely bulk communications data ("BCD") secured in response to directions issued under s94 of the Telecommunications Act 1984. BCD is a particular form of BPD. We do not consider it raises any separate issue so far as these proceedings are concerned, and we will use the term "BPD" to encompass also BCD, save where it is necessary to make separate reference to BCD.

The 2016 judgment

43. The issues raised by the claimant's underlying claim before the Tribunal included the question of whether the BPD regime is compatible with the "in accordance with the law" requirement of article 8. This issue was considered by the Tribunal in its 2016 judgment.

44. The principles that underpin the "in accordance with the law" requirement (as summarised at paragraphs 28 - 40 above) are well known to the Tribunal. It has rehearsed and applied them in many of its judgments. It summarised them as follows in its 2016 judgment at [62]:

> "(i) There must not be an unfettered discretion for executive action. There must be controls on the arbitrariness of that action. We must be satisfied there exist adequate and effective guarantees against abuse.

> (ii) The nature of the rules fettering such discretion and laying down safeguards must be clear and the ambit of them must be in the public domain so far as possible; there must be an adequate indication or signposting, so that the existence of interference with privacy may in general terms be foreseeable.
> (iii) Foreseeability is only expected to a degree that is reasonable in the circumstances, being in particular the circumstances of national security, and the foreseeability requirement cannot mean that an individual should be enabled to foresee when the authorities are likely to resort to secret measures, so that he can adapt his conduct accordingly.
> (iv) It is not necessary for the detailed procedures and conditions which are to be observed to be incorporated in rules of substantive law.
> (v) It is permissible for the Tribunal to consider rules, requirements or arrangements which are "below the waterline" ie which are not publicly accessible, provided that what is disclosed sufficiently indicates the scope of the discretion and the manner of its exercise.
> (vi) The degree and effectiveness of the supervision or oversight of the executive by independent Commissioners is of great importance, and can, for example, in such a case as *Kennedy* be a decisive factor."

45. Applying these principles, the Tribunal concluded that the use of BPDs by the Agencies was not compatible with article 8 prior to 12 March 2015 (the date of the ISC report), or, in the case of BCDs, November 2015 (when the use of BCD was publicly disclosed for the first time by the draft Investigatory Powers Bill). This was because, before March 2015, the use of BPDs was not foreseeable to the public and there was no statutory oversight. To the extent that there had been some independent non-statutory oversight by the Commissioners, that had been inadequate. The Tribunal concluded that following avowal of the powers, the publication of the internal arrangements and changes to the oversight arrangements (and subject to reserving questions of the disclosure of BPDs to third parties, and the impact of EU law) the regime was compatible with article 8. In reaching that conclusion it considered, in close detail, the system of oversight that operated - see at [72]-[82]. It concluded, at [82], that "during the period of Sir Mark Waller's supervision the independent oversight of BPD had been and continued to be adequate."

46. The Tribunal's 2016 judgment deliberately left out of account two matters which it considered required separate consideration: (1) issues of proportionality and compatibility with EU law, and (2) the compatibility of the transfer of datasets abroad with article 8.

47. In respect of (1), compatibility with EU law, the Tribunal held further hearings in June 2017. It gave a judgment on 8 September 2017 in which it explained its reasoning for referring questions to the Court of Justice of the European Union in relation to the application of EU law to BCDs.

48. As to (2), the transfer of BPDs abroad, that was addressed in the proceedings which resulted in the 2018 judgment, which is the subject of this claim for judicial review.

49. On 6 October 2020 the Grand Chamber of the CJEU gave judgment on the Tribunal's reference - C/623/17. On 21 July 2021 the Tribunal held a further hearing at which it heard submissions as to the consequences of the CJEU's judgment. It gave a judgment the following day. It concluded that, in the light of the judgment of the CJEU, s94 of the

1984 Act is incompatible with EU law. It granted a declaration to that effect. The Tribunal expressly reserved the question as to the consequences of this for the sharing of BPDs with foreign agencies – see at [27]:

> "At the hearing a point was also raised by Mr de la Mare about the consequences for sharing arrangements with foreign agencies and others. This was a topic which was dealt with by the Tribunal in its [2018 judgment]… Mr de la Mare accepted that this is one of those topics which will have to be considered at a later stage in these proceedings."

The 2018 judgment

50. Leaving aside the impact of EU law, the Tribunal identified 4 issues that remained for resolution from its 2016 judgment. The third of these concerned the sharing of BPDs. That itself gave rise to three sub-issues, the first of which concerned sharing with foreign agencies. It is the Tribunal's decision on that sub-issue which is under challenge in this claim for judicial review.

51. The Tribunal held open and closed hearings over 8 days between October 2017 and March 2018. It considered a significant amount of written and oral evidence. It was dissatisfied with the way in which the evidence emerged from GCHQ. This involved, on a number of occasions, statements made by GCHQ having "to be subsequently corrected" as a result of "re-thinking or double-checking". The Tribunal found that GCHQ had breached its duty to make disclosure to the Tribunal under s68(6) RIPA (although, it was satisfied, by the end of the proceedings, that this had been remedied). In these circumstances, the witness was cross-examined by counsel for the Claimant, Mr de la Mare QC. The Tribunal described this as "an exceptional step… because of the concerns about [the witness' evidence]." It also heard extensive submissions on behalf of the claimant and the Agencies. In the course of these hearings, the claimant made an application to reopen the 2016 judgment insofar as it concluded the oversight of the Commissioners had been adequate. The application was based on a number of different factors. They included that Sir Mark Waller had carried out oversight personally and had not had a team of inspectors (in contrast to Sir Stanley Burnton who appointed a team to assist him). They also included correspondence with IPCO in which "amber warnings" were given and "criticisms" expressed. The Tribunal considered that a sufficient case had been made to justify consideration of reopening the judgment, and so it separately considered that as a fifth issue. The Tribunal commended the claimant's representatives for their "dedication and hard work… throughout this exercise" and acknowledged that "the public and indeed [the Agencies] owe them a debt of gratitude for their patience and perseverance, as well as their considerable and valuable inquisitiveness."

52. The Tribunal received evidence as to the safeguards that were in place in relation to the sharing of BPDs with foreign agencies. It also received evidence from a GCHQ witness about the steps that would be taken in the event that BPDs were shared with foreign agencies. The witness said the Agencies would:

> "● Follow the principles and approach set out in our respective handing arrangements and policy/guidance
>
> ● Take into account the nature of the BPD/BCD that was due to be disclosed

> ● Take into account the nature/remit of the body to which we were considering disclosing the BPD/BCD
>
> ● Take into account the approach taken by any other [intelligence agency] who may have shared bulk data and have regard to any protocols/understandings that the other agencies may have used/followed
>
> ● Depending on the individual circumstances seek assurances that the BPD/BCD in question would be handled in accordance with RIPA safeguards…
>
> ● If relevant to the particular circumstances, seek assurances that its use was in accordance with the UK's international obligations.
>
> ● Any data shared with the organisation 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 Agencies."

53. The Tribunal gave judgment on 23 July 2018 ([2018] UKIPTrib IPT_15_110-CH [2018] 2 All ER 166).

54. The Tribunal rejected the application to reopen its 2016 judgment (see at [95]-[112]). It observed that different Commissioners could legitimately take different views as to "the appropriateness of technical assistance." Sir Mark Waller had preferred to carry out work himself, so he had personal oversight which was not delegated to others. Sir Stanley Burnton had appointed a team of Inspectors. However, the Tribunal had "no doubt that [Sir Mark Waller] did carry out supervision, with diligence and regularity" which was demonstrated by the detail of his reports and the technical points he had explored with the Agencies. The Tribunal considered that the new regime, under IPCO, which involved a team of experts "may be an improvement… but it does not… evidence prior inadequacy." The observations that had been made by IPCO did not undermine, but instead exemplified "the nature and adequacy of ongoing oversight."

55. At [64], the Tribunal referred to its previous judgments in which it had considered the safeguards required by article 8. It emphasised that the sharing of BPDs could only be lawful if there were adequate safeguards against abuse, including sufficient oversight arrangements. It referred (at [68]) to case law that shows safeguards must be "practical and effective" rather than "theoretical and illusory" and that that the safeguards must include "independence, powers and competence which are sufficient to exercise an effective and continuous control, public scrutiny and effectiveness in practice."

56. The Tribunal therefore recognised that it is not enough for there to be robust safeguards in place. It is necessary that they are operated in a manner that is effective. The Tribunal made it clear at the outset of the open judgment (at [6(iv)]) that the Agencies had identified five serious errors which they had since corrected. It observed that, to the extent that those errors were present in information provided to the Commissioners, "this will have meant that the Commissioners were not overseeing GCHQ on the basis of a complete and accurate picture of what it was actually doing." This therefore raised in

stark form the question of whether the safeguards were effective in practice or whether the errors that had been identified meant that the system was incompatible with article 8.

57. The Tribunal cited *Catt* at [33] for the proposition that a system of oversight can be satisfactory even if it is "not proof against mistakes". Against that background it set out its approach as follows (at [69]):

> "(i) The fact that errors occur in the handling of data does not necessarily establish that safeguards or oversight were not effective; no oversight can be expected to prevent any errors occurring.
>
> (ii) The mere fact that errors are reported, or are detected by internal or external audit, may be evidence that the oversight system is working, not that it is defective.
>
> (iii) There is a duty on the Agencies… to report to the Commissioner anything that is material for the Commissioner to know in order to perform his oversight function properly; if there has been a failure to report a material use of data of which the commissioner might not be aware… then that is to be treated as a failure… to ensure proper safeguards and oversight.
>
> (iv) A Commissioner has a considerable margin of appreciation as to what resources he needs to perform his functions correctly, and there are no grounds for criticism of his decisions as to how he applies those resources; it is not the function of the Tribunal to audit the performance of a Commissioner's functions; the fact that a new Commissioner might take a different view on an issue does not establish that there were not adequate and effective arrangements before.
>
> (v) The question may well be capable of being resolved by reference to whether there has been a systemic failure in oversight arrangements, not whether in particular respects the performance of the Agencies can be criticised."

58. Applying this approach, the majority concluded that the system for sharing BPDs with foreign agencies was compatible with article 8, notwithstanding the errors that had been identified. There were two dissenting members, Charles Flint QC and Susan O'Brien QC. They each set out their reasons for dissent in a closed judgment. The majority explained in the closed judgment that they shared some of the concerns expressed in the dissenting judgments, but did not consider that they rendered the regime incompatible with article 8.

59. The Tribunal therefore concluded by a majority that the regime in respect of sharing BPDs with foreign agencies complied with article 8 (see at [61]-[71]). This was expressly subject to any question that might arise under EU law - see at [72]:

> "As for the position under EU law, in relation to transfer of intelligence out of the EU to foreign agencies, that must obviously await the outcome of the Reference to the CJEU."

60. We have explained above the steps that the Tribunal has since taken in relation the Reference to the CJEU (see paragraphs 47 and 49 above).

The claim for judicial review

61. The claimant filed an application for judicial review of the Tribunal's 2018 judgment (and in particular the conclusion that the sharing of BPDs with foreign agencies is compatible with article 8) on 22 October 2018. It recognised that its claim was, on the face of it, barred by s67(8) Regulation of Investigatory Powers Act 2000 (which provides that "…determinations… and other decisions of the Tribunal… shall not be… liable to be questioned in any court.") The Divisional Court and the Court of Appeal had held that this wording precluded a claim for judicial review, which was "the aim that Parliament clearly intended" [2017] EWHC 114 (Admin) at [44]. The claim was stayed pending an appeal to the Supreme Court. On 15 May 2019 the Supreme Court allowed an appeal from the Court of Appeal's judgment, holding by a majority that s67(8) of the 2000 Act does not oust a claim for judicial review – [2019] UKSC 22 [2020] AC 491. The stay on the claim was therefore lifted.

62. The claimant's sole ground of challenge was that it could be "inferred that arguable issues of law arise that ought to be authoritatively determined by the Administrative Court", but the claimant was unable to say more because "the basis for the decision of the minority of the IPT is entirely secret."

63. Following the decision in *Big Brother Watch* the claimant amended the claim to contend that the Tribunal erred in law as to the legal principles concerning article 8. It drew attention to the requirements set out in *Big Brother Watch* at [350] and [362] (see paragraphs 36 and 38 above). The claimant contends that (1) BPDs were not obtained in circumstances where there were relevant "end to end safeguards", and the sharing was not limited to such material as was collected and stored in a Convention-compliant manner; and (2) the circumstances in which sharing of BPDs may take place are not set out clearly in domestic law.

64. The claimant invited the court to appoint a Special Advocate, and adopt a closed material procedure, to ensure that the claimant's interests were properly represented. As we have explained, the court acceded to that invitation. The Special Advocates have advanced closed grounds of challenge to the Tribunal's 2018 judgment. With the agreement of the Agencies, extracts from those closed grounds were disclosed to the claimant.

65. The Special Advocates' grounds, so far as they were disclosed to the claimant, are that (1) the Tribunal did not recognise and apply the correct article 8 legal principles, including in particular the requirements explained in *Big Brother Watch*, and (2) the majority of the Tribunal erred in concluding that the sharing by GCHQ of BPDs with foreign agencies would be compatible with article 8. The Special Advocates advance further grounds which were not disclosed to the claimant, but they are, in effect, different ways of expressing the two grounds that have been disclosed.

Submissions

The claimant's case

66. Mr de la Mare QC challenged the application of NCND to the question of whether BPDs have been shared by GCHQ with foreign agencies. He said that was not tenable given the content of IPCO's 2019 report (see paragraph 26 above). That, he says, makes it plain that there has been a fact-led review of the sharing that has taken place in the past, with

a view to implementing change. The principle of open justice requires the court to hear submissions on all issues in public and to resolve all issues in a public judgment, unless there is strong justification for taking a different course. There are, he says, real dangers in allowing the development of "closed" jurisprudence on issues of legal principle – see the judgments in *R (Binyam Mohamed) v Secretary of State for Foreign and Commonwealth Affairs* [2008] EWHC 2519 (Admin) (at [7] and [56]-[57]), [2009] EWHC 152 (Admin) [2009] 1 WLR 2653 (at [18]-[19] and [40]-[53]) and [2009] EWHC 2549 (Admin) [2009] 1 WLR 2653 (at [113]-[120]). This was an issue that had not been raised in the written grounds. It arose only shortly before the hearing (when counsel for the claimant noticed the reference in the 2019 IPCO report) and was raised with the court for the first time in the course of the hearing. At the conclusion of the closed hearing we invited, and subsequently received, further written submissions from the parties (in the first instance, in closed, from the Agencies and the Special Advocates, and then, after those submissions were disclosed to the claimant, from the claimant). The Agencies maintained that the content of the 2019 report does not, on close analysis, disclose whether sharing of BPDs had taken place by the time of the Tribunal's judgment. The Special Advocates argued that this was an issue that could and should be resolved in open and after receiving submissions from the claimant. A redacted version of the Agencies' submissions was disclosed to the claimant and the claimant then made written submissions. They maintained that the approach of the Agencies was not realistic and that the principle of open justice required that the Agencies should no longer be permitted to rely on NCND.

67. Mr de la Mare adopted an argument of the Special Advocates as to the role of the Administrative Court in this type of claim, namely one that is a challenge to a decision of the Tribunal that the Agencies have acted compatibly with Convention rights. The argument is that the court is a public authority that is itself bound to act compatibly with Convention rights, that it should consider for itself whether there has been a breach of a Convention right and, if so, it should grant a declaration to that effect. In such a case, it is not open to the court simply to quash the decision and remit the issue back to the Tribunal. Principle, and authority, require the court to declare that the Agencies acted incompatibly with Convention rights, and then remit the question of remedy (and only that question) to the Tribunal. Reliance was placed on the decisions of the Supreme Court in *Huang v Secretary of State for the Home Department* [2007] 2 AC 167 *per* Lord Bingham at [8] and [11] and *R (R) v Chief Constable of Greater Manchester Police* [2018] UKSC 47 [2018] 1 WLR 4079 *per* Lord Carnwath at [53].

68. The claimant's first ground of challenge (see paragraph 63 above) is that the BPDs were not lawfully obtained, and therefore any sharing of the BPDs is necessarily incompatible with article 8 ECHR. Mr de la Mare QC submitted that the acquisition of some BPDs by the Agencies has now been shown to be unlawful. That is because s94 of the 1984 Act is incompatible with EU law, and so any acquisition of BCDs pursuant to s94 of the 1984 Act was necessarily unlawful. It is also because, he says, the acquisition of BPDs does not comply with the "end-to-end" safeguards that are required. The Grand Chamber has said that it is only permissible to share bulk intelligence material that has been lawfully obtained (see paragraph 38 above). It follows that the sharing of those BPDs with foreign agencies was necessarily unlawful, because it was not "in accordance with the law" for the purposes of article 8.

69. In respect of the substance of the claim, Mr de la Mare QC made submissions of principle as to the requirements of article 8 in the light of *Big Brother Watch*, recognising that it would be for the Special Advocates to advance the claimant's case as to whether there had been a departure from those requirements in the light of the evidence and findings that had not been disclosed to the claimant. He emphasised the practical impact of sharing BPDs on privacy interests. The increasing use of mobile telephones, email and the internet mean that BPDs (and particularly BCDs) allow intelligence agencies to build a detailed picture of a person's private life. Communication metadata ("the who, where, when and how" of each communication) can be more revelatory and of greater value to the Agencies than the content of communications because the metadata "does not lie." BPDs can be used to locate targets of interest. That is particularly relevant in the context of the time period covered by this case because of the use of rendition operations (potentially involving torture or inhuman and degrading treatment), and drone strikes, which are known to have taken place.

70. *Big Brother Watch* was the first occasion on which the European Court of Human Rights had considered the article 8 safeguards that should be applied to the use of bulk data by intelligence agencies. It also dealt "head on" with the question of sharing data. It recognised that because the first two *Weber* criteria are inapt in the context of bulk data, supervision and review take on amplified importance (see paragraphs 33 and 36 above) – as Mr de la Mare QC put it, they have to do "more of the heavy lifting."

71. So far as sharing is concerned, the first safeguard identified by the court (see paragraph 38 above) is that the data has been gathered lawfully in the first place. Here, the Tribunal has already found that the gathering of BCD was in breach of EU law. This causes "the whole system to fall down." Moreover, the court said in terms that there must be independent oversight of data sharing. The court was satisfied, in that case, that the system of supervision and oversight was compatible with the requirements of article 8 (see paragraphs 39 - 40 above), but those assessments were made without the benefit of the identification by the Tribunal in this case of errors that had occurred.

72. Mr de la Mare QC adopted an argument that was advanced by the Special Advocates to the effect that the Tribunal failed to recognise and apply well-known principles as to the "in accordance with the law" requirement of article 8 ECHR. The Tribunal's explanation of what is required is "generic." In particular, it does not state whether the supervisory body was in a position to assess the proportionality and necessity of any sharing. Moreover, it is clear (for example from the 2019 IPCO report) that there have been problems as to the degree of oversight that had previously been applied. The report indicates that the whole topic is now approached in an organised, systematic, systemic and procedural fashion, with the implementation of checks and balances to record sharing, caveats, limitations on use and undertakings, and to cross-check that nothing is happening that is inconsistent with those conditions. But that all serves to indicate that the pre-existing regime was deficient.

73. The critical finding of the majority of the Tribunal was that the "episodic" problems it identifies do not demonstrate that there was "systemic failure". That, however, depends on the closed evidence and findings, and everything would "turn on close examination of the facts by the Special Advocates."

The Agencies' response to the claimant's case

74. Sir James Eadie QC submitted that the Tribunal's summary of the Strasbourg caselaw and the core requirements was "concise" but legally accurate. Rather than repeating all of the requirements, it referred back to its previous judgments which analyse in detail the case law setting out the safeguards that are required. This is a legitimate approach: the Tribunal does not need to "reinvent the wheel" each time it gives judgment in a case concerned with article 8. In considering the application of the safeguards, the Tribunal recognised that a critical element is the *ex post facto* oversight that is provided by a combination of the Commissioners and the Tribunal itself. Neither the claimant nor the Special Advocates have identified any inaccuracy in the Tribunal's summary of what is necessary to comply with article 8.

75. The judgment of the Grand Chamber in *Big Brother Watch* does not undercut any of the principles identified by the Tribunal as applicable to the question of sharing BPDs with foreign agencies. *Big Brother Watch* was concerned with bulk intercept, which is "a different game, with different issues" compared to cases that have previously been considered. It explains how the principles that were developed in earlier cases should be applied "in the world of big data." Nothing in *Big Brother Watch* shows that the domestic regime for BPDs is incompatible with article 8. Critically, there is no suggestion in *Big Brother Watch* that advance independent authorisation is required (see at [362]) – an *ex post facto* system of oversight by the Commissioners and the Tribunal can suffice.

76. Insofar as the claimants raised concerns about the legality of acquiring BPDs, that was an attempt to "open up other aspects of the data cycle" which were not the subject of the Tribunal's 2018 judgment. That judgment (so far as is now challenged) is only concerned with the sharing of BPDs with foreign agencies.

Discussion

Application of "NCND" to question of whether BPDs have been shared with foreign agencies

77. In the proceedings before the Tribunal, the Agencies refused publicly to admit or deny whether BPDs had been shared with foreign agencies. The application of "NCND" was explained in evidence put before the Tribunal. The Tribunal recognised that "unauthorised and unadmitted disclosures" had been made by Edward Snowden, a former US contractor. It did not consider that those disclosures could be treated as amounting to, or being equivalent to, admission or avowal by the Agencies. The Tribunal was content to permit the Agencies to maintain a public "NCND" stance, whilst conducting the open hearings "on the hypothesis that the fact that such sharing has taken place is to be assumed."

78. The issue is whether that stance is tenable in the light of IPCO's 2019 report. That report was published. It must have been carefully vetted by the Agencies before publication took place (see s234(7) of the 2016 Act). We are satisfied that the content of the 2019 report amounts to public avowal that BPDs are shared by GCHQ with foreign agencies. It is not, therefore, tenable for GCHQ to continue to maintain an "NCND" response to the question of whether sharing now takes place. The 2019 report does not, however, state when BPDs were first shared by GCHQ with foreign agencies, and, in particular, does not state whether they were shared by GCHQ during the period considered by the Tribunal.

79. We accept the claimant's submissions as to the undesirability of resolving issues of legal principle in closed judgments. Here, however, all issues of legal principle have been debated in the course of the open submissions and are determined in this judgment. The closed judgment is concerned only with the application of those principles to the factual findings made, in closed, by the Tribunal. We do not consider that this approach is incompatible with the important principle of open justice. The question of NCND had not been raised in the grounds of claim, and it is not necessary to resolve that question in order to determine the grounds of claim. It is a side issue. The balance as to what could be dealt with in open and what had to remain in closed was considered in detail by the Tribunal. We have, so far as is consistent with the unchallenged approach of the Tribunal, dealt with this claim in public proceedings and in this public judgment. That is consistent with the general approach that was sanctioned by the Supreme Court (in the context of reviewing search warrants, where some of the evidence considered by the Magistrates' Court is sensitive) in *R (Haralambous) v Crown Court at St Albans and another* [2018] UKSC 1 [2018] AC 236 *per* Lord Mance DPSC at [59].

80. It is therefore not necessary or appropriate, on this claim for judicial review, to adjudicate on the claimant's contention that it is no longer permissible to maintain NCND in respect of that earlier period. That is an issue that is more appropriately determined (if it is necessary to do so) by the Investigatory Powers Tribunal, as a specialist first instance Tribunal, than by us on a claim for judicial review which did not raise this issue until a late stage. We therefore adopt the same approach as the unchallenged approach of the Tribunal of assuming, for the purpose of this open judgment, that sharing was taking place during the period considered by the Tribunal.

Role of the Court on claim for judicial review of the Tribunal

81. The consequence of the decision of the Supreme Court in *Privacy International* is that, notwithstanding s67(8) of the 2000 Act, the Court may review a decision of the Tribunal, exercising its powers under s29 Senior Courts Act 1981. If the Court concludes that the determination of the Tribunal was legally flawed then, on the approach taken by the Supreme Court, "it is no decision at all" and there is no ouster of the Court's reviewing jurisdiction.

82. The Agencies accept this analysis. They contend that if the Court considers that the decision of the IPT is flawed on public law grounds then the Court may quash the determination and remit the case back to the Tribunal. We agree. We do not accept the submission of the claimant, and the Special Advocates, that it is necessary for us to reach our own view as to whether the Agencies have acted compatibly with Convention rights.

83. We are exercising a reviewing jurisdiction. The appropriate remedy if the Tribunal's determination is vitiated by error of law is to quash the determination and to remit the matter back to the Tribunal pursuant to s31(5)(a) Senior Courts Act 1981. There is, in narrow circumstances, power for the Court to substitute its own decision (s31(5)(b) read with s31(5A)). That does not seem to us to be appropriate in the circumstances of this case, for two reasons. First, Parliament has provided, by s65(2)(a) and (3)(a) of the 2000 Act, that the Tribunal is "the only appropriate tribunal for the purposes of section 7 of the Human Rights Act 1998 in relation to any proceedings [against any of the intelligence services] under subsection (1)(a) of that section (proceedings for actions incompatible with Convention rights)…" It would be inconsistent with that legislative choice for us to declare that the Agencies have acted incompatibly with Convention rights. Second, the

Tribunal continues to be seized of the general proceedings in any event (see the 2021 judgment at [27], at paragraph 49 above). If its 2018 Judgment contains a legal error it is more appropriate for the consequences of that error to be worked through by the Tribunal in the context of those continuing proceedings. We do not consider that the authorities relied on by the claimant and Special Advocates (see paragraph 67 above) mandate any different approach. *Huang* was concerned with the role of the immigration appellate authority, which exercises an appellate rather than a reviewing jurisdiction. *R* was concerned with the role of an appellate court exercising the jurisdiction under CPR 52.11(3) to allow an appeal where the decision of the lower court is "wrong." We accept that if we consider that the Tribunal's decision discloses an error of law then we should say so and quash its decision. We do not, however, consider that anything in *Huang* or *R* requires us to usurp the role allocated by Parliament to the Tribunal of determining claims under s6 of the 1998 Act.

84. Accordingly, the appropriate remedy, if this claim is otherwise well-founded, is to quash the decision of the Tribunal and remit the case back to the Tribunal for reconsideration.

Impact of unlawful acquisition of BPD

85. We do not express any view on the claimant's argument that BPD were not lawfully obtained, with the result that the sharing of BPD is necessarily incompatible with article 8. That is because:

(1) This argument was not advanced before the Tribunal in the hearings that resulted in the 2018 judgment.

(2) The Tribunal did not purport to rule on the question of whether any particular instance of sharing was compatible with article 8. The Tribunal expressly limited its judgment on the issues that are now under challenge to the question of whether the supervision and oversight of sharing BPDs with foreign agencies was compatible with article 8.

(3) At the time of the 2018 judgment the Tribunal had, separately, referred to the CJEU two questions as to the impact of EU law on directions made under s94 of the 1984 Act.

(4) Following the judgment of the CJEU on those questions, the Tribunal held a further hearing on 21 July 2021. It was common ground between the parties that, in the light of the judgment of the CJEU, s94 of the 1984 Act was incompatible with EU law. The Tribunal granted a declaration as to the incompatibility of s94 of the 1984 Act with EU law.

(5) At the time of the 21 July 2021 hearing, the Tribunal expressly reserved the question as to the consequences of this for the sharing of BPDs with foreign agencies – see at [27] (see paragraph 47 above).

(6) The arguments that Mr de la Mare now advances do not therefore fall within the scope of the Tribunal's 2018 judgment. Nor are they matters upon which the Tribunal was obliged to adjudicate in its 2018 judgment. It has legitimately left the matter open for future consideration.

86. It follows that the Tribunal has not yet considered the point that Mr de la Mare wishes to make, but has recognised that it may need to do so at a future hearing. We cannot see any basis on which it would be appropriate for this court to rule on the issue.

Tribunal's analysis of safeguards required by article 8

87. The assertion in the written grounds that the domestic regime does not adequately set out the circumstances in which BPDs may be shared (see paragraph 63 above) was not pressed in oral submissions. We do not consider that there was any flaw in the Tribunal's analysis of this issue. The Tribunal was well aware of the requirements for an adequate regime of regulation. It had, in its 2016 judgment, found that any use of BPDs prior to March 2015 was incompatible with article 8 because the test of foreseeability had not been met. It observed (at [61]) that it had set out in its 2016 judgment the "[s]trict rules relating to the disclosure of [BPD]" outside the Agencies, and that there had subsequently been more detailed disclosure of the safeguards, which it set out in Appendix 2 to its judgment (see paragraphs 16 – 27 above). It summarised the evidence that had been adduced on the issue (see paragraph 52 above). It recognised (at [64(ii)] that there must be "sufficient disclosure of the capability to share, and of such safeguards, for the purposes of the test of foreseeability." It concluded (at [71]) that the regime was compliant with article 8.

88. We consider the Tribunal was right not to find that the domestic regime was incompatible with article 8 on the grounds of a failure to prescribe the circumstances in which BPDs may be shared. The 1989 and 1994 Acts require that sharing may only take place where that is necessary for the purposes of national security (see paragraph 16 above). The BPD policy requires that sharing may only take place where the supplying agency is satisfied that sharing is "necessary and proportionate", and where advance authorisation has been given by a senior individual within the agency, and where a log is maintained (see paragraph 21 above). The BPD handling arrangements require that before sharing takes place steps are taken to ensure that the data is appropriately handled by the recipient (see paragraph 22 above).

89. The focus of the open submissions concerned the safeguards (and particularly the oversight) that is required by article 8. Mr de la Mare QC recognised that the Strasbourg case law does not require prior judicial authorisation before bulk data can be shared. Nor is prior independent scrutiny required. Neither the claimant nor the Special Advocates identified anything incorrect in what the Tribunal said about the safeguards required by article 8. The submission was that the analysis was insufficiently detailed and failed to identify all of the principles that have been developed in the Strasbourg case law. However, those principles are very well known, and are particularly well known by the Tribunal which has stated and applied them in a number of its decisions. At [64] it said that it had considered and set out the law in its previous decisions. We do not consider that it was incumbent on the Tribunal to repeat all of the principles in its 2018 judgment. There is no indication that it did not take all of them fully into account.

90. The Tribunal did not have the benefit of the *Big Brother Watch* judgment. We agree with the claimant that although that decision is concerned with the use of bulk interception of communications, many of the observations made apply to the use of BPDs more generally. In particular, we agree that the first two *Weber* criteria do not apply and that, instead, the requirement for adequate supervision takes on an amplified significance. It is, however, clear that the Tribunal attached importance to the system of supervision that

was in place. That was the prime focus of its consideration of the evidence, including in relation to the "action-on" arrangements. At [64] it said that compatibility with article 8 "depends… upon" (among other matters) "existence of sufficient oversight arrangements", and at [65] it confirmed that it had considered "the existence, operation and effectiveness of… the "action-on policy.""

91. We are therefore satisfied that there is no legal error in the Tribunal's analysis of the safeguards and oversight that is necessary to comply with article 8. Its analysis is consistent with the approach required by *Big Brother Watch*.

Application of the legal principles to the facts

92. The Tribunal was far from satisfied with the evidence that was initially placed before it by GCHQ, which contained "mistakes" that had to be corrected. The Tribunal made it clear in its open judgment that "five further serious such errors" were identified. It recognised that so far as "these errors" were present in information provided to the Commissioners then the Commissioners' oversight of GCHQ was not based on a full picture.

93. Against this background the Tribunal assessed with evident care whether these were "episodic" errors such that they did not invalidate the system itself, or whether they were systemic flaws such that the system could not satisfy the requirements of article 8. It set out the approach it took to this assessment in five propositions at [69] (see paragraph 537 above). It has not been suggested that any of the Tribunal's five propositions are flawed. We are satisfied that its approach is correct. We are also satisfied that this is the approach that the Tribunal applied when assessing whether the errors were "episodic" or "systemic". Having undertaken that assessment, the view of the majority was that the regime was compliant with article 8. That is an assessment that can only be reviewed in our closed judgment, because it depends on closed evidence that was before the Tribunal and the Tribunal's closed assessment of that evidence. It is an assessment that has been vigorously challenged by the Special Advocates. However, for the reasons we give in our closed judgment, we do not consider that the Tribunal's assessment is irrational or otherwise flawed on public law grounds.

Outcome

94. The Tribunal correctly identified the measures necessary to comply with the "in accordance with the law" criterion of article 8. It identified serious errors that had been made by GCHQ. It concluded, by a majority, that notwithstanding those errors the regime was compatible with article 8. That conclusion does not contain any legal error. We dismiss the claim for judicial review.