[Home] [Databases] [World Law] [Multidatabase Search] [Help] [Feedback]

United Kingdom Investigatory Powers Tribunal

You are here: BAILII >> Databases >> United Kingdom Investigatory Powers Tribunal >> Privacy International v Secretary of State for Foreign And Commonwealth Affairs & Ors (Rev 2) [2016] UKIPTrib 15_110-CH (17 October 2016)
URL: *http://www.bailii.org/uk/cases/UKIPTrib/2016/15_110-CH.html*
Cite as: [2016] HRLR 21, [2016] UKIPTrib PT_15_110-CH, [2017] 3 All ER 647, [2016] UKIPTrib 15_110-CH

[New search] [Context] [View without highlighting] [Printable PDF version] [Help]

Neutral Citation Number: [2016] UKIPTrib 15_110-CH

No. IPT/15/110/CH

IN THE INVESTIGATORY POWERS TRIBUNAL

No. IPT/15/110/CH
Rolls Building
17 October **2016**

B e f o r e :

THE HON. MR. JUSTICE BURTON (PRESIDENT)
THE HON. MR. JUSTICE MITTING (VICE-PRESIDENT)
SIR RICHARD MCLAUGHLIN
MR. CHARLES FLINT QC
MS. SUSAN O'BRIEN QC

_____

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**

APPEARANCES

MR. T. DE LA MARE QC, MR. B. JAFFEY and MR. D. CASHMAN (instructed by Bhatt Murphy Solicitors) appeared on behalf of the Claimant.
MR. J. EADIE QC, MR. A. O'CONNOR QC and MR. R. O'BRIEN (instructed by Government Legal Department) appeared on behalf of the Respondents.
MR. J. GLASSON QC (instructed by Government Legal Department) appeared as Counsel to the Tribunal.

26, 27,28,29 July 2016

HTML VERSION OF JUDGMENT APPROVED

Crown Copyright ©

MR JUSTICE BURTON:

1. This is the judgment of the Tribunal, to which all Members have contributed.

2. The Claimant before the Tribunal is Privacy International, a Non- Governmental Organisation, working in the field of defending human rights at both national and international levels; they are represented by Mr. Thomas de la Mare QC, Mr. Ben Jaffey and Mr. Daniel Cashman. The Respondents are the Secretary of State for Foreign and Commonwealth Affairs ("the Foreign Secretary") and the Secretary of State for the Home Department ("the Home Secretary"), and the three Security and Intelligence Agencies (SIAs), being GCHQ, the Security Service (MI5), and the Secret Intelligence Service (MI6), for all of whom Mr. James Eadie QC, Mr. Andrew O'Connor QC, and Mr. Richard O'Brien have appeared. Mr Jonathon Glasson QC has appeared as counsel for the Tribunal, and gave particular assistance during the interlocutory period leading up to the hearing.

3. The proceedings were brought on 5th June 2015 relating to the SIAs' acquisition, use, retention, disclosure, storage and deletion of Bulk Personal Datasets ("BPDs"), whose existence was publicly acknowledged in March 2015 by the Respondents in evidence to, and then in a Report by, the Intelligence Security Committee of Parliament ("ISC"). The proceedings were amended in September 2015 to add claims in relation to the use of s.94 of the Telecommunications Act 1984 ("s.94" and "the 1984 Act") by the Home and Foreign Secretaries to give directions to Public Electronic Communications Networks ("PECNs") to transfer bulk communications data to GCHQ and MI5 ("BCD").

4. This case concerns the acquisition and use by the SIAs of bulk data. BCD is acquired by GCHQ and MI5 under directions issued under s.94. The communications data thus collected will include the "who, when, where and how" of both telephone and internet use (as it is put in paragraph 12 below), and this may include the location of mobile and fixed line phones from which calls are made or received, and the location of computers used to access the internet. BCD does not include the content of any such communications, which may only be obtained under an interception warrant. BPD is acquired and used by GCHQ, MI5 and MI6. Such data, acquired by overt or covert means, includes considerable volumes of data about biographical details, commercial and financial activities, communications and travel, as well as communications data obtained under s.94 arrangements or by interception under a warrant. All such bulk data, both BCD and BPD, may be searched by the SIAs to discover details about persons of intelligence interest. These are important and wide ranging capabilities, which have only recently come to light. The Claimant contends that

they infringe the right to private life under Article 8 of the ECHR. The Respondents contend that their use of such powers is lawful and essential for, inter alia, the protection of national security.

BPD

5. BPD was explained as follows by the Respondents in their Response dated 11th April 2016 ("the April Response"):-

> *"(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, and too large to be processed manually.*
>
> *(2) The* [SIAs] *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* [SIAs] *includes a number of broad categories of data. By way of example only these include: biographical and travel (e.g. passport databases); communications (e.g. telephone directory); and financial (e.g. 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* [SIAs] *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."*

6. The ISC in its March 2015 Report gave the following description of BPD:-

> *"157. Whereas the* [SIAs'] *capabilities to intercept communications and acquire Communications Data are regulated by* [the Regulation of Investigatory Powers Act 2000] *(RIPA) the rules governing the use of Bulk Personal Datasets are not defined in legislation. Instead, the* [SIAs] *derive the authority to acquire and use Bulk Personal Datasets 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* [SIAs] *under the Intelligence Services Act 1994* [ISA 1994] *and the Security Service Act 1989* [SSA 1989] ...
>
> *159. While Ministers are not required to authorise the acquisition or use of Bulk Personal Datasets in any way, the Home Secretary explained that he had some involvement: "*[*MI5*] *do come to me and I receive submissions on acquisition on bulk datasets and the holding of bulk datasets." In relation to the Bulk Personal Datasets held by GCHQ and* [*MI6*]*, the Foreign Secretary explained to the Committee that, "There is not a formal process by which we have looked* [*at those datasets*]*."... He explained ... "... I have ... asked for twice yearly reporting of the holdings of bulk*

personal data by the [SIAs]."

160. In terms of independent review, the Intelligence Services Commissioner has non-statutory responsibility for overseeing the [SIAs'] *holdings of Bulk Personal Datasets (since 2010) ... The Commissioner explained to the Committee that he retrospectively reviews the* [SIAs'] *holdings of Bulk Personal Datasets 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*."

7. The MI5 witness explained in his evidence as follows:-

"*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. These datasets allow the identification of individuals where the basis of information held is primarily related to communications data, e.g. 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, e.g. 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 acquires 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 BPD's 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

8. Included in BPD there will be information obtained as a result of the lawful operations of the SIAs themselves, pursuant to interception in accordance with s.8 (4) of RIPA (considered by this Tribunal in **Liberty/Privacy (No. 1)** [2015] 3 All ER 142) and from Computer Network Exploitation ("CNE") (considered by this Tribunal in **Privacy International and Greennet Limited v. Secretary of State for Foreign and Commonwealth Affairs ("Greennet")** [**2016**] UKIP Trib 14_85-CH).

BCD

9. The issue as to BCD arises out of directions to PECNs given by the Home and Foreign Secretaries pursuant to s.94 for the provision of communications data. S.94 reads in material part - as amended in 2003, and we leave the original in square brackets:-

"*94 - **Directions in the interests of national security, etc.***

(1) The Secretary of State may, after consultation with a person to whom this section applies, give to that person such directions of a general character as appear to the Secretary of State to be necessary [requisite or expedient] *in the interests of national security or relations with the government of a country or territory outside the United Kingdom.*

(2) If it appears to the Secretary of State to be necessary [requisite or expedient] *to do so in the interests of national security or relations with the government of a country or territory outside the United Kingdom, he may, after consultation with a person to whom the section applies, give to that person a direction requiring him (according to the circumstances of the case) to do, or not to do, a particular thing specified in the direction.*

10. In the April Response, the Respondents gave the following account in relation to BCD:-

"*7) Both GCHQ and ... MI5 acquire Bulk Communications Data pursuant to directions made under s.94 of the 1984 Act. For the avoidance of doubt,* [MI6] *do not do so.*

GCHQ

8) [In 1998 and then regularly] *since 2001, GCHQ has sought and obtained from successive Foreign Secretaries a number of s.94 directions relating to the ongoing provision of various forms of bulk communications data. In keeping with GCHQ's external intelligence mission, the datasets received under these directions are predominantly foreign-focussed, and the data acquired is accordingly in most cases only a fraction of that possessed by the* [PECN's].

9) The data involved is held by GCHQ and ingested into their broader data holdings, where it is merged with communications data intercepted under the authority of external warrants issued in accordance with s.8(4) of RIPA. The s.94 data represents a more reliable and comprehensive feed of particular types of communication data than may usually be obtained from interception. The intelligence value of the s.94 data is derived from the merger with GCHQ's wider datasets, thus enriching the results of

analytic queries made on those systems.

10) Such analysis of bulk communications data is vital for identifying and developing intelligence targets. Approximately 5 per cent of GCHQ's original intelligence reporting is based wholly or partly on s.94 data.

MI5

11) Since 2005 successive Home Secretaries have issued and/or decided to maintain directions under s.94 of the 1984 Act requiring a number of [PECN's] *to provide MI5 with ... communications data in the interests of national security. The data obtained is aggregated in a database. Successive Home Secretaries have agreed that they would keep these arrangements under review at six-monthly intervals. The review process involves a detailed submission being made to the Home Office by MI5, setting out the ongoing case for the database, including specific examples of its usefulness in the intervening period and setting out any errors in the use of the database, which have occurred in that time. The Home Secretary considers the submission with the advice and assistance of Senior Home Office officials.*

*12) The communications data provided by the [*PECNs*] under the s.94 directions is limited to "traffic data" and "Service Use Information".*

13) The data provided does not contain communication content or Subscriber Information (information held or obtained by a [PECN] *about persons to whom the* [PECN] *provides or has provided communication services). The data provided is therefore anonymous. It is also data which is in any event maintained and retained by* [PECN's] *for their own commercial purposes (particularly billing and fraud prevention).*

14) Such data is of significant intelligence and security value."

11. In the recent Report of the Interception of Communications Commissioner ("I C C"), Sir Stanley Burnton, being a Review of directions given under s.94 dated July **2016** ("the July Review"), the I C C stated at paragraph 8.34 that:

> *"All of the current directions require regular feeds of bulk communications data to be disclosed by the relevant PECN."*

12. The MI5 witness explained at paragraph 25 of his statement:-

> *"The use of communications data (the who, where, when and how of a communication but not its content) is a vital tool in the investigation of threats and safeguarding the public. The DG for MI5 discussed the importance of communications data in meeting the challenges that the SIA's face in his BBC interview of 17th September 2015:-*
>
> *"We need to be able to use datasets so we can join the dots, to be able to find and stop the terrorists who mean us harm before they are able to bring the plots to fruition. We have been pretty successful at that in recent years but it is becoming more difficult to do that as technology changes faster and faster.""*

Avowal

13. 'Avowal' has become something of a term of art in the course of proceedings before this Tribunal, namely being the date when the Respondents have publicly avowed the activity the subject of consideration in the relevant proceedings. In this case the existence of BPD was only avowed in

March 2015, when disclosure was made to the ISC. By a Direction dated 11th March 2015 (the **Intelligence Services Commissioner Additional Review Functions) (Bulk Personal Datasets) Direction 2015**) the Prime Minister, pursuant to his power under s.59(a) of RIPA, directed the Intelligence Services Commissioner ("I S 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.*"

14. S.94 directions, and BCD, which had previously been disclosed to the ISC, were not publicly avowed until November 2015, when they were disclosed in the context of the draft Investigatory Powers Bill then being presented to Parliament. Although Sir Stanley Burnton's predecessor as I C C, Sir Anthony May, was asked in February 2015 by the Prime Minister to oversee the s.94 directions on a non-statutory basis, and agreed to do so, provided that he was given extra staff, the I C C was not able effectively to start doing so until at least October 2015.

15. Handling Arrangements for BPD and for s.94 were both published on 4th November 2015, and were supplemented by Closed Handling Arrangements in relation to each of the SIAs, which have been subsequently, during the course of these proceedings, disclosed, redacted in part.

The Issues

16. On 7th July **2016** the parties agreed an amended list of issues. They are helpfully summarised in paragraph 11 of the Claimant's Skeleton:-

> *a) Issue 1: Section 94 TA under domestic law: Is it lawful as a matter of domestic law to use section 94 TA to obtain BCD?*
>
> *b) Issue 2: Is the section 94 TA regime in accordance with the law? This issue is to be considered in three time periods. First, prior to the avowal of the use of section 94 to obtain BCD* [4th November 2015]. *Secondly, from avowal to the date of hearing. Thirdly, as at the date of hearing.*
>
> *c) Issue 3: Is the BPD regime in accordance with the law? This issue is to be considered in four time periods. First, prior to the avowal of the holding of BPDs* [March 2015]. *Secondly, from avowal to the publication of the BPD handling arrangements. Thirdly, from publication to the date of the hearing. Finally, as at the date of hearing.*
>
> *d) Issue 4: Are the section 94 regime and the BPD regime proportionate?*

There are also EU Law issues, which have been adjourned to a hearing in December.

17. These issues require some elucidation:

> (i) Although the first issue is confined to the legality of the use of the power under s. 94 to obtain communications data in bulk, the other issues are not so confined. The other issues extend not just to the obtaining of data, but also to the uses to which such data may be put by the SIAs. As argued by the Claimant, the claim concerns the arrangements for and safeguards attaching to the acquisition, use, retention, disclosure, storage and deletion of bulk data, whether obtained under s.94 or by other means.
>
> (ii) BPD may include communications data lawfully obtained by the SIAs (as referred

to in paragraph 64 below), but may also include data lawfully obtained commercially or otherwise without the use of any statutory power to procure or compel the acquisition of bulk data.

Agreed/Assumed Facts

18. The procedure which has been operated by this Tribunal in recent hearings has been that issues are agreed so as to facilitate a public hearing in open court, enabling full *inter partes* argument, based upon facts which are agreed or assumed for the purposes of that hearing. In this case the Claimant served a schedule of 41 proposed agreed facts (and a small number of assumed facts), which the Respondents largely accepted, in almost every case with the rubric that their acceptance was subject to the full context provided in their pleadings and evidence. We were supplied with closed evidence by the Respondents (much of which we decided should be disclosed in open, redacted as necessary), but it played no part in our judgment.

19. The most material of the Agreed Facts are as follows (we do not repeat matters already specifically mentioned above):-

(a) BCD

(i) GCHQ and MI5 collect and hold BCD, relying upon s.94 as the legal basis for doing so. MI6 does not collect or hold BCD. GCHQ also acquires related communications data pursuant to warrants issued pursuant to RIPA s.5 in respect of external communications under the terms of s.8(4).

(ii) GCHQ requires any access to BCD to be justified on the same grounds and to the same standards as access to related communications data obtained pursuant to s.8(4) of RIPA.

(iii) GCHQ treats BCD acquired under s.94 Directions in the same way as it treats related communications data obtained pursuant to s.8(4), storing data obtained under those statutory regimes within the same databases.

(iv) MI5's procedures include a process under RIPA, Part 1, Chapter II for accessing its BCD database, which is not followed by GCHQ.

(v) MI5 generally retains BCD for one year.

(vi) BCD contains communications data in the form of "traffic data" and "service use information" (as defined in s.21(4) of RIPA), or the "who, where, when and how of a communication." BCD may have contained subscriber information and may include locational data from mobile and fixed telephone lines and internet devices: GCHQ's BCD collection includes bulk internet communications data, which may include the "who, where, when and how," of a communication on the internet, including automated communications between machines.

(vii) S.94 Directions have not been, and cannot be, used to authorise the interception of the content of communications.

(viii) BCD contains large amounts of data, most of which relates to individuals who are unlikely to be of any intelligence interest.

(ix) BCD may be disclosed to persons outside the agency holding the BCD (subject to safeguards contained in the relevant Handling Arrangements).

(x) Prior to the publication of the Investigatory Powers Bill, the use of s.94 to collect BCD was not publicly acknowledged.

(xi) There have been instances of non-compliance with internal procedures and safeguards in relation to access of BCD databases at GCHQ and MI5, revealed in the various Commissioners' Reports.

(b) BPD

(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 s.2 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.

(viii) GCHQ, MI5 and MI6 do not currently hold and have never held a BPD of medical records, although medical data may appear in BPDs.

(ix) There have been instances of non compliance with BPD safeguards at GCHQ, MI5 and MI6, as disclosed in the various Commissioners' Reports.

(x) There was no statutory oversight of BPD's by the I S Commissioner prior to the March 2015 ISC Report.

(xi) Prior to the publication of that ISC Report, the holding of BPDs was not publicly acknowledged.

20. Since the proceedings commenced, as referred to above, there is now before Parliament a Bill. Although the Claimant has referred to some parts of the Bill as examples of improvements which the Claimant asserts can and should be made to the present arrangements, or as indicating that the present arrangements are not satisfactory or compliant with Article 8, the Bill itself, and of course Parliament's consideration of it, will for obvious reasons not form part of our consideration.

21. It is important to emphasise that the Tribunal and the parties recognise that there is a serious threat to public safety, particularly from international terrorism, and that the SIAs are dedicated to discharging their responsibility to protect the public. It is understandable in the circumstances that the Respondents, both through Mr. Eadie orally and by their evidence, have emphasised the important part which the use of BCD and BPD have played in furthering that protection, particularly where those who pose the threat are using increasingly sophisticated methods to protect their communications. In a Report published on 19th August **2016** (the "Bulk Powers Review") David Anderson QC, the Independent Reviewer of Terrorism Legislation, concluded that there is a proven operational case for the use of the powers to obtain and use BCD and BPD, that those

powers are used across the range of activities of the SIA, from cyber-security, counter-espionage and counter-terrorism to child sexual abuse and organised crime, and that such powers play an important part in identifying, understanding and averting threats to Great Britain, Northern Ireland and elsewhere. This Report was published after the hearing and the parties will be given an opportunity to make submissions on the weight which should be attached to it on the issue of proportionality, Issue 4. At this stage we merely record these conclusions of the Report as indicating the purposes for which the SIAs seek to use the powers which are in issue in this case. The issue for this hearing is whether the use of such powers is justifiable at domestic law and in accordance with the Convention, and we turn to the four issues accordingly.

ISSUE 1

22. The issue, as posed, requires to be refined in the light of the facts which are agreed between the parties: "Is it lawful under domestic law for a Secretary of State to issue directions to telecommunications and internet service providers (PECNs) to supply communications data to the Security Service and to GCHQ and for them to store and examine it?"

23. We will address this first issue at domestic law, independently of the law of the European Union and of the rights protected under the European Convention on Human Rights (ECHR).

24. "*Communications data*" is defined by s. 21(4) Regulation of Investigatory Powers Act 2000 ("RIPA"):

> "*(4). In this Chapter "Communications data" means any of the following --*
>
> *(a) any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunications system by means of which it is being or may be transmitted;*
>
> *(b) any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person --*
>
> *(i) of any postal service or telecommunications service; or*
>
> *(ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunications system;*
>
> *(c) any information not falling within paragraph (a)or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service.*"

25. The relevant part of the definition of "*Traffic data*" is contained in s.21(6)(a) and (b):

> "*(6). In this section "Traffic data", in relation to any communication, means*
>
> *(a) any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted,*
>
> *(b) any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted….*"

26. Communications data, therefore, comprises, or includes, the date and time on which a call or electronic communication is made and received, the parties to it, the apparatus by which it is made and received and, in the case of a mobile telephone communication, the location from which it is made and in which it is received. It can include billing records and subscriber information. Just about the only information not included is the content of communications.

27. There is a detailed statutory scheme under which communications data can be lawfully obtained and disclosed, set out in Chapter II of Part I RIPA. The Claimant's case is that the obtaining of communications data is only lawful under these provisions. The Respondents' case is that communications data may also lawfully be provided to the Security Service and GCHQ under a direction given by the Secretary of State under s. 94 of the 1984 Act.

28. The starting point must be to analyse the power granted to a Secretary of State under s. 94 when it was originally enacted. The Bill received Royal assent on 12 April 1984. The Act and s.94 should be set in context. In 1984 the only commercially available telecommunications services in the United Kingdom were by landline. The first commercial mobile telephone call was made on 1 January 1985 via Cellnet. There was no internet. The first dial-up service was introduced in March 1992. The Foreign Secretary and the Home Secretary had, since the introduction of landline telephones, been empowered under the royal prerogative to issue personally warrants to intercept, via tapping, landline telephone calls. The only communications data held by telecommunications operators was subscriber information and call records from which statements of account were prepared to send to subscribers. Apart from telephone numbers which were ex-directory, subscriber information was publicly available in telephone directories. The only communications data which the Security Service or GCHQ (the existence of which was not formally acknowledged) might have been expected to wish to acquire was subscriber information for ex-directory numbers and call records, to enable them to fulfil their (then) primary defensive tasks of counterespionage (against the Soviet Union and its satellites) and counter-terrorism (against Northern Ireland terrorists).

29. This context was also the setting for s. 45 of the 1984 Act, which as originally enacted provided (in material part):

> *"(1). A person engaged in the running of a public telecommunications system who otherwise than in the course of his duty --*
>
> > *(a) intentionally intercepts a message sent by means of that system; or*
> >
> > *(b) where a message so sent has been intercepted, intentionally discloses to any person the contents* of *that message, shall be guilty of an offence.*
>
> *(2). A person engaged in the running of a public telecommunication system who otherwise than in the course of his duty intentionally discloses to any person the contents of any statement of account specifying the telecommunications services provided for any other person by means of that system shall be guilty of an offence.*
>
> *(3). Subsection (1) above does not apply to anything done in obedience to a warrant under the hand of the Secretary of State; and paragraph (b) of that subsection and subsection (2) above do not apply to any disclosure in connection with the investigation of any criminal offence or for the purposes of any criminal proceedings."*

30. S.45 therefore recognised the lawfulness of obedience to an intercept warrant under the hand of the Secretary of State and established a prohibition on disclosing the contents of a statement of account specifying the telecommunication services provided for any other person "*otherwise than in the course of his duty*".

31. As Mr de la Mare acknowledged, the Secretary of State could not secure compulsory disclosure of information specifying the telecommunications services provided to a subscriber ("billing records") unless there was a statutory power which imposed on telecommunications providers a duty to do so.

32. The only available power was to be found in s. 94(1) and (2). S. 94(3) imposed a duty on the person to whom a direction had been given to comply with it:

> *"(3). A person to whom this section applies shall give effect to any direction given to him by the Secretary of State under this section, notwithstanding any other duty imposed on him under this Act."*

33. The clear words of s. 94(1) to (3), read with s. 45(2), empowered the Secretary of State to direct telecommunications providers to provide billing and subscriber records to the Security Service and GCHQ in the interests of national security or foreign relations and required the telecommunications providers to comply with the direction. Nothing in the context available to Parliament would have necessitated any implied limitation on that right and duty: if the Secretary of State could, by a warrant, require telecommunications providers to intercept, or to facilitate the interception by the Security Service and GCHQ of telephone communications, there was no reason to construe the statutory power and duty under s. 94 so as to exclude the lesser intrusion effected by the disclosure of communications data to the Secretary of State.

34. Consequently, the billing records could only be obtained under s.94. It is plain that, in accordance with ordinary principles of statutory construction, contrary to the submissions of Mr de la Mare, s.45 must be read subject to s.94, and s.94 must be read in the context of s.45.

35. The power to issue intercept warrants was placed on a statutory footing by s.2 of the Interception of Communications Act 1985 ("the 1985 Act"), which read:

> *"2 Warrants for interception*
>
> *(1) Subject to the provisions of this section and section 3 below, the Secretary of State may issue a warrant requiring the person to whom it is addressed to intercept, in the course of their transmission by post or by means of a public telecommunication system, such communications as are described in the warrant; and such a warrant may also require the person to whom it is addressed to disclose the intercepted material to such persons and in such manner as are described in the warrant.*
>
> *(2) The Secretary of State shall not issue a warrant under this section unless he considers that the warrant is necessary—*
>
> *(a) in the interests of national security ;*
>
> *(b) for the purpose of preventing or detecting serious crime ; or*
>
> *(c) for the purpose of safeguarding the economic well-being of the United Kingdom."*

36. S. 11(1) of and Schedule 2 to the 1985 Act established a new s. 45 in the 1984 Act:

> *"45(1). A person engaged in the running of a public telecommunications system who otherwise than in the course of his duty intentionally discloses to any person -- (a) the contents of any message which has been intercepted in the course of its transmission by means of that system; or (b) any information concerning the use made of telecommunication services provided for any other person by means of that system, shall be guilty of an offence.*

(2). Subsection (1) above does not apply to -- (a) any disclosure which is made for the prevention or detection of crime or for the purposes of any criminal proceedings; (b) any disclosure of matter falling within paragraph (a) of that subsection which is made obedience to a warrant issued by the Secretary of State under section 2 of the Interception of Communications Act 1985 ... or (c) any disclosure of matter falling within paragraph (b) of that subsection which is made in the interests of national security or in pursuance of the order of a court."

The new s.45 (3) introduced the provision for a PII certificate to be conclusive evidence of the interests of national security.

37. On a natural reading, s.45, as amended by the 1985 Act, preserved the power of the Secretary of State and the duty of the telecommunications provider under s.94. Mr. de la Mare submits that the savings in s.45 (2) (c) applied only to voluntary disclosure. We disagree. As a matter of ordinary language, it applied both to voluntary disclosure and to disclosure in fulfilment of a duty under s.94. As in the case of s.45 as originally worded, there is no reason to construe the amended section restrictively. Therefore, until RIPA came into force, the Secretary of State was entitled to give directions to telecommunications providers, and by then internet service providers, to provide communications data as then existing to MI5 and GCHQ. By then communications data would have permitted the location of the maker and recipient of a mobile telephone call to be identified.

38. Prior to RIPA, the statutory powers of MI5 and GCHQ, in relation to communications data, were contained in the two Acts which acknowledged their existence. In s.1(2) of SSA 1989:

"*The function of the service shall be the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine Parliamentary democracy by political, industrial or violent means*."

Its general functions were circumscribed by duties placed on the Director General by s.2 (2).

"*The Director General shall be responsible for the efficiency of the service and it shall be his duty to ensure --*

(a) that there are arrangements for securing that no information is obtained by the service except so far as necessary for the proper discharge of its functions or disclosed by it, except so far as necessary for that purpose…"

In the case of GCHQ, its functions are set out in s.3 (1) of the ISA 1994:

"*… its functions shall be --*

(a) to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material…"

Its functions are circumscribed by the responsibility of the Director of GCHQ, defined in the same terms as his counterpart in MI5 in s.4 (2). These powers provide ample power to cover the storage and examination of communications data obtained under s.94.

39. S.82 (1) of and Schedule 4 to RIPA amended s.45 (2), but did not amend s.45 (1) of the 1984 Act (so that the exception there provided for "*in the course of ... duty*" remained):

"*(2) Subsection (1) above does not apply to any disclosure made --*

(a) in accordance with the order of any court or for the purposes of any criminal proceedings;

(b) in accordance with any warrant, authorisation or notice issued, granted or given under any provision of [RIPA].

(c) in compliance with any requirement imposed (apart from that Act) in consequence of the exercise by any person of any statutory power exercisable by him for the purpose of obtaining any document or other information …

(3) In subsection (2) above … '*statutory power*' [has] *the same meanings as in* [RIPA]."

"*Statutory power*" is defined in s. 81(1) of RIPA*: "'statutory', in relation to any power or duty, means conferred or imposed by or under any enactment or subordinate legislation*".

40 Thus, as a matter of ordinary language, s.45, as amended by RIPA, recognised that disclosure might be made under RIPA or in consequence of the exercise by any person of any other statutory power exercisable for the purpose of obtaining any document or other information. It did so, by amendment of the Act in which s.94 appears. It would therefore be surprising if Parliament can be taken to have intended by these words to do other than preserve that power.

41. The position is put beyond doubt by s.80 of RIPA:

"*Nothing in any of the provisions in this Act, by virtue of which conduct of any description is or may be authorised by any warrant, authorisation or notice, or by virtue of which information may be obtained in any manner, shall be construed –*

(a) *as making it unlawful to engage in any conduct of that description which is not otherwise unlawful under this Act and would not be unlawful apart from this Act;*

...

(c) as prejudicing any power to obtain information by any means not involving conduct that may be authorised under this Act."

As a matter of construction, therefore, RIPA did not revoke the power of the Secretary of State under s.94 to give directions for the provision of communications data to PECNs or their duty to comply with such a direction. In any event, so far as collection of communications data is concerned, s.45 continued in force (as amended). S. 1(1) of RIPA, which made it an offence to intercept communications, did not, in any event, apply to communications data (s.2 (5) of RIPA).

42. The power under s.94 was preserved by the Communications Act 2003 which repealed the operative provisions of the 1984 Act, apart from s.94. Further, as set out in paragraph 9 above, it amended s.94 to substitute "*necessary*" for "*requisite or expedient*" in subsection (1), and it added subsection (2A):

"*The Secretary of State shall not give a direction under subsection (1) or (2) unless he believes that the conduct required by the direction is proportionate to what is sought to be achieved by that conduct*."

Mr. de la Mare submits that these words are directed only or principally at Article 1, Protocol 1 ECHR to ensure that telecommunications providers and internet service providers are not required to bear the cost of interference with their property rights in communications data. We disagree. There is no reason so to limit the occasions on which the obligation can arise. The words are especially apt to cover interference with the Article 8 rights of the users of communications services. S.94, and its power to give directions, thus amended, was left effective.

43. The Data Retention and Investigatory Powers Act 2014 ("DRIPA") made new provision for the retention and disclosure of communications data in s.1(1) and (6):

> "(1) *The Secretary of State may by a notice (a 'retention notice') require a public telecommunications operator to retain relevant communications data if the Secretary of State considers that the requirement is necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (h) of section 22(2)* [of RIPA] …
>
> *(6) A public telecommunications operator who retains relevant communications data by virtue of this section must not disclose the data except -- (a) in accordance with (i) Chapter 2 of Part 1 of* [RIPA] …"

The regime created by these provisions is self-contained: it only applies to data retained by a public telecommunications operator pursuant to a retention notice "*by virtue of* [that] *section*". It does not apply to arrangements already in place to comply with a direction under s.94. This is consistent with the Retention of Communications Data Code of Practice of March 2015 paragraph 8.1 and 8.2.

44. Mr. de la Mare submits that Part I Chapter II of RIPA provides a comprehensive and exclusive statutory scheme for the acquisition and disclosure of communications data and that s.94 cannot lawfully be used to circumvent it. It is necessary therefore to set out the RIPA scheme. S.21(1), (2) and (3) provides:

> "*(1) This Chapter applies to --*
>
> *(a) any conduct in relation to a postal service or telecommunications system for obtaining communications data, other than conduct consisting in the interception of communications in the course of their transmission by means of such a service or system; and*
>
> *(b) the disclosure to any person of communications data.*
>
> *(2) Conduct to which this Chapter applies shall be lawful for all purposes if --*
>
> *(a) it is conduct in which any person is authorised or required to engage by an authorisation or notice granted or given under this Chapter; and*
>
> *(b) the conduct is in accordance with, or in pursuance of, the authorisation or requirement.*
>
> *(3) A person shall not be subject to any civil liability in respect of any conduct of his which --*
>
> *(a) is incidental to any conduct that is lawful by virtue of subsection (2); and*

(b) is not itself conduct, an authorisation or warrant for which it is capable of being granted under a relevant enactment and might reasonably have been expected to have been sought in the case in question."

There then follow the definition provisions already set out above.

45. S.22 deals with the circumstances in which a "*designated person*" believes it is necessary to obtain communications data. A "*designated person*" is a person identified in Schedule 1 to the Regulation of Investigatory Powers (Order) 2003 (now 2010) -- senior officers of a variety of public authorities. They include, but are not limited to, officers of MI5 and GCHQ. Designated persons must have a belief of the kind set out in s.22(2):-

> "*It is necessary on grounds falling within this subsection to obtain communications data if it is necessary --*
>
> *(a) in the interests of national security;*
>
> *(b) for the purpose of preventing or detecting crime or of preventing disorder;*
>
> *(c) in the interests of the economic well-being of the United Kingdom;*
>
> *(d) in the interests of public safety;*
>
> *(e) for the purpose of protecting public health;*
>
> *(f) for the purpose of assessing or collection any tax, duty, levy or other imposition, contribution or charge payable to a government department;*
>
> *(g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or*
>
> *(h) for any purpose not falling within paragraphs (a) to (g) which is specified for the purposes of this subsection by an order made by the Secretary of State*."

46. Subsections (4) to (7) set out what a designated person may require and what a telecommunications operator must do:

> "*(4) Subject to subsection (5) where it appears to the designated person that a postal or telecommunications operator is or may be in possession of, or be capable of obtaining, any communications data, a designated person may, by notice to the postal or telecommunications operator, require the operator --*
>
> *(a) if the operator is not already in possession of the data, to obtain the data; and*
>
> *(b) in any case to disclose all of the data in his possession or subsequently obtained by him.*
>
> *(5) The designated person shall not … give a notice under subsection (4) unless he believes that obtaining the data in question by the … notice is proportionate to what is sought to be achieved by so obtaining the data.*

(6) It shall be the duty of the postal or telecommunications operator to comply with the requirements of any notice given to him under subsection (4).

(7) A person who is under a duty by virtue of subsection (6) shall not be required to do anything in pursuance of that duty which it is not reasonably practicable for him to do."

Subsection (8) provides that the duty imposed upon the telecommunications operator is enforceable by civil proceedings.

47. S.23 (2) sets out detailed provisions for the giving of a notice under s.22 (4) and sets a limit of one month on its duration, subject to renewal.

48. Ss.71 and 72 provide for the issuing of codes of practice relating to the exercise of powers under Part I, Chapter II, and as to their effect.

49. Mr. de la Mare relied in general terms upon the 'principle of legality' whereby "*fundamental rights cannot be overridden by general or ambiguous words*" (per Lord Hoffman in **R v Home Secretary ex p Simms** [2000] 2 AC 115 at 131F). Mr. Eadie pointed out that, in this case, the ECHR rights are qualified not absolute, and that the principle of legality does not apply in every case in which legislation may interfere with ECHR rights (as opposed to overriding them). The 'principle of legality' will thus in any event, in that regard, as Lord Hoffman points out in **RB (Algeria) v Secretary of State** [2010] 2 AC 110 at 181, have been "*largely superseded in its application to human rights by s.3 of the 1998 Act*".

50. However, the foundation for Mr. de la Mare's submission is the statement by Lord Bingham CJ in **R v Liverpool County Council ex parte Baby Products Association**, 23 November 1999, reported in (2000) LGR 171 at 178(e)-(f) "*A power conferred in very general terms plainly cannot be relied on to defeat the intention of clear and particular statutory provisions*", as approved in **R (W) v Secretary of State for Health** [2016] 1 WLR 698 CA.

51. A little needs to be said about the facts of the case and the legal context of the arguments considered in it. Liverpool County Council was the weights and measures authority for their area. It published a statement to the effect that samples of ten models of baby walkers had been tested and found not to comply with the British Safety Specification. The association, to which distributors of the baby walkers belonged, claimed that the press statement was unlawful. Under the General Product Safety Regulations 1994, made under Council Directive 92/59/EEC and under powers granted to them under the Consumer Protection Act 1987, Liverpool County Council had the power to issue a suspension notice of up to six months duration where there were reasonable grounds to suspect that a safety provision of the regulations had been contravened, against which the person on whom the notice had been served had the right to apply to a Magistrates' Court to have it set aside. It was common ground that the intention of Liverpool City Council was to cause a suspension of the supply of the baby walkers described in the press release. Liverpool County Council contended that it had a statutory power to issue the press release under its general ancillary powers in the Local Government Act 1972 and as weights and measure authority under the Weights and Measures Act 1985.

52. Lord Bingham's conclusion was baldly stated but, on the facts, was plainly justified: Liverpool County Council was attempting to achieve, by the exercise of ancillary powers in general legislation defining their functions, a specific purpose which could only be achieved by the exercise of powers under the regulations and the 1987 Act. It has no application to the circumstances we are considering, for four reasons:

(i) The regulations contained no saving provision for other statutory powers. By contrast, s.80 of RIPA expressly preserves the power to issue directions such as those under s.94.

(ii) As set out in paragraph 41 above, s.94 was still effective, as amended in 2003, after RIPA.

(iii) The powers relied on by Liverpool County Council were general and ancillary powers. Again by contrast, s.94 is not a general and ancillary power. It may only be exercised on one of two grounds -- national security or foreign relations -- and may only be exercised in relation to the director of Ofcom and a person who is a public telecommunications operator or an approved contractor (s.94(8)).

(iv) The exercise of the power to give directions under s. 94 does not defeat the provisions of Part I, Chapter II of RIPA. It is the exercise of a different and separate power, by the Secretary of State, not by designated persons.

53. Mr. Eadie mounted a sustained argument to the effect that Mr. de la Mare's submission could only succeed if he could show that RIPA had repealed or circumscribed the s.94 power to give directions. He relied on settled case law - primarily principles enunciated by AL Smith J in **Kutner v Phillips** [1981] 2 QB 267 at 271 and by Laws LJ in **O'Byrne v Secretary of State for the Environment, Transport and the Regions** [2001] EWCA [2002] HLR 30 Civ 499 at para.68 - that there is a strong presumption against implied repeal (see also Waller LJ in **Henry Boot Construction (UK) Limited v Malmaison Hotel (Manchester) Limited** [2001] QB 388), and that the later enactment must be so inconsistent with or repugnant to the provisions of the earlier Act that they cannot stand together, or that there must be an insuperable logical contradiction between the two. We agree that neither situation applies here; but do not consider it necessary to undertake an elaborate analysis, because s.80 (a) and (c) of RIPA expressly preserves the pre-existing power to obtain communications data, ruling out any question of implied repeal.

54. There was a further contention by the Respondents that is not necessary for our conclusion, namely that in any event ss.21 and 22 of RIPA, the sections said to constitute a 'comprehensive code' for the acquisition or obtaining of communications data, and which apply where (s.22) a designated person believes it is necessary to obtain communications data, do not apply at all where the communications data have already been obtained by virtue of a s.94 direction, and the Secretary of State has (after the necessary consultation) considered it necessary (and proportionate) to obtain the data. It is certainly right that when the use of s.94 was discussed in 2004 with the then I C C, Sir Swinton Thomas, as disclosed in documents in these proceedings by the Respondents, access to the communications data, already acquired by virtue of the s.94 direction, was discussed in the context of 'obtaining' the information. It is also the case that the procedures for access operated by MI5 (but not by GCHQ) for accessing the communications data obtained under s.94 are analogous to those adopted for accessing data obtained by intercept, (although the terms of the Acquisition and Disclosure of Communications Data Code of Practice of March 2015 in s.1 appear clearly to contrast acquisition of communications data under RIPA with data obtained under other powers). However, given our conclusion that Part I, Chapter II of RIPA is not a comprehensive code

excluding the operation of s.94, there is no need to resolve this issue. The result is as discussed by Patten LJ in **Snelling v Burstow Parish Council** [2014] 1 WLR 2388, and as Aikens LJ in **RK (Nepal) v SSHD** [2009] EWCA Civ 359 postulated, namely that the two routes are parallel and alternative.

55. Mr. de la Mare submitted that Mr. Eadie's construction of s.94 was impossible or implausible, because it depended upon his limiting s.94 to giving directions for delivery of communications data, whereas the section could be construed as permitting the use of s.94 to obtain interception of the contents of communications, which Mr Eadie was abjuring. We have already explained why, upon construction of the context of s.94, taken together with s.45, its purpose was to enable the obtaining of billing information, or what is now called communications data. In addition, it is plain that, as set out in paragraph 198 of the Respondents' Amended Open Response of 19 February **2016,** "*directions under s.94 can lawfully be made to require* [PECNs] *to facilitate conduct that has already been made lawful by authorisations under* [other statutory] *provisions*". However we are satisfied that a direction under s.94 could not be used, and in any event was not intended, for the purpose of itself authorising or directing interception of contents. At the time of the passage of the 1984 Act the prerogative was used for such interception, and that was then replaced by the provisions of s.2 of the 1985 Act (see paragraph 35 above). S. 1 of RIPA made interception of content an offence, save insofar as otherwise pursuant to lawful authority, and the exemption was provided by s.1(5) of RIPA, which read as follows:-

> "*(5) Conduct has lawful authority for the purposes of this section if and only if [*apart from the provisions of RIPA*] …;*
>
> *(c) it is in exercise, in relation to any stored communication, of any statutory power that is exercised (apart from this section) for the purpose of obtaining information or of taking possession of any document or other property.*"

Mr. de la Mare seeks to get round the problem that this exemption would only apply to "*stored communication*" by postulating that there could be two directions, or a two-stage direction, by the Secretary of State, for the communications to be first stored and then intercepted. But this would plainly be an impermissible evasion of the criminal offence. In any event it is agreed that s.94 has not been used for such purpose.

56. The Claimant in a written Note delivered after the hearing, which extended more widely than had been permitted by the Tribunal when we agreed that there could be a response to the Respondents' speaking note in relation to Issues 2 and 3, referred to other statutes which on their face give the Secretary of State a power to issue broadly worded directions in the interests of national security. We do not consider that any of them assist us in relation to the construction of the context and history of s.94, with which we have already dealt, and which was the subject of careful argument by both parties. The Note also referred to a Zimbabwean case, which appears to address the alleged untrammelled discretion of the President of Zimbabwe; if relevant at all it would, in our judgment, be only material in the context of what we in any event have to consider, namely the applicability of the ECHR, which is the bulwark which the UK Courts adopt to restrain arbitrary conduct by the executive, and which will be the subject of our consideration in Issues 2 and 3.

57. For the reasons given, we are satisfied that the relevant Secretary of State pursuant to s.94 was and is entitled to issue directions to telecommunications and internet service providers to supply communications data to MI5 and GCHQ. It is clear, notwithstanding Mr. de la Mare's reference to passages in the 1999 White Paper, or in Hansard, that neither RIPA nor DRIPA constituted a 'comprehensive code', as he submits, such as to exclude, override or repeal the operation of s.94, which was preserved by s.80 of RIPA. In any event, subject to Issues 2 and 3 below:-

(i) The law is clear, and the directions may be given if necessary and proportionate, so as to facilitate access by the SIAs to communications data supplied by the PECNs.

(ii) As in **Snelling**, there are two lawful routes for the SIAs to obtain communications data in the interests of protecting national security.

The continued existence of the directions under s.94, and the Respondents' contentions by reference to s.45 of the 1984 Act, to s.80 of RIPA, to the Communications Act 2003 and to s.1 of DRIPA, do not constitute a series of "*trapdoors*", such as Mr. de la Mare submitted. Rather, as we have found, they constitute the correct legal analysis.

58. Consequently we resolve Issue 1 in favour of the Respondents: it is lawful at domestic law to use s 94 to obtain BCD.

ISSUES 2 and 3

Article 8

59. As noted above, Issues 2 and 3 are framed by reference to the "in accordance with law" requirement in Article 8. That requirement is generally stated to comprise (a) that the measures under review should have a basis in domestic law, and (b) that the laws in question should be compatible with the rule of law, in being generally accessible, foreseeable and contain adequate safeguards against arbitrary use (**Weber & Saravia v Germany** [2008] 46 EHRR SE5, at paragraphs 84, 92 – 94).

60. The Tribunal has considered the impact of Article 8 on the SIAs, and the balance to be struck between national security and privacy, in a number of cases, in which we took fully into account the judgments of the ECtHR, the most material judgments being **Weber** and **Kennedy v United Kingdom** [2011] 52 EHRR 4. We considered the jurisprudence and we set out our conclusions, in particular in **Liberty/Privacy** at paragraphs 37-39, 82-91, 116-122, 125 and 137, and again in **Greennet**, to the judgments in both of which cases we refer. There has been some development in Luxembourg jurisprudence, by reference to **Digital Rights Ireland v Minister for Communications, Marine and Natural Resources and Others** [2015] QB 127 and the Advocate General's opinion in **Tele2 Sverige AB v Post-Och Telestyrelsen and Others** [C-203/15 and C-698/15], delivered on 19 July **2016,** which we shall have more opportunity to consider when we deal with the adjourned EU law issues. So far as ECHR jurisprudence is concerned, there have only been two recent cases bearing on the position, **R E v United Kingdom** [**2016]** 63 EHRR 2, which we considered in **Greennet** at paragraphs 79-80, and **Szabo & Vissy v Hungary** [Application 37128/14, 12 January **2016].** **Szabo** was a decision of the Fourth Section of the Court: there were no safeguards in place at all, and it is clear from paragraph 70 of the Judgment that it was not a case which was appropriate to lead to any new jurisprudence, because: "*It is not warranted to embark on [such consideration] in the present case, since the Hungarian system of safeguards appears to fall short even of the previously existing principles*." The decision of the Court, at paragraphs 88 and 89, was that the Hungarian legislation was not sufficiently precise, effective and comprehensive on surveillance and the Government had not proved the practical effectiveness of any supervision arrangements. On its face the section 7/E (3) power granted to the anti-terrorist organ was unlimited in the cases in which intelligence gathering might be used. Both **R E** and **Szabo** were applying the principles in **Weber** and **Kennedy** to the particular facts.

61. If there is to be any new jurisprudence, this Tribunal and indeed the UK Courts are not required to anticipate it, as is made clear by **R (Ullah) v Special Adjudicator** [2004] 2 AC 323, not least in that the Respondents have no right of appeal. Insofar as there is some support for a requirement for judicial pre-authorisation, notwithstanding the view of this Tribunal in **Liberty/Privacy** at paragraph 116(vi), or for someone who has been the subject of interception to be notified when there has been a material error by the Respondents (as proposed in clause 209 [Error Reporting] of the Investigatory Powers Bill), it is not for this Tribunal to lay down new requirements, and (see

the transcript at Day 2, page 109) it does not appear that Mr. de la Mare was submitting that we should do so.

62. Accordingly, by reference to our considered assessment of the ECHR jurisprudence, we can summarise in short terms what we conclude the proper approach is:

(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 that 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' i.e. 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.

As we concluded at paragraph 125 of **Liberty/Privacy**, there must be: "*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*." In addition, as we concluded at paragraph 82 of **Greennet**: "*Compliance with **Weber** ... will in our judgment mean the provision, particularly in a national security context, of as much information as can be provided without material risk to national security. In our judgment, not least because of the consequences of a conclusion of unlawfulness simply by virtue of a perceived procedural insufficiency, a conclusion that procedural requirements, or the publication of them, can be improved (i) does not have the necessary consequence that there has prior thereto been insufficient compliance with Weber ... and (ii) does not constitute such a material non-compliance as to create a contravention of Article 8. This Tribunal sees it as an important by-product of the exercise of its statutory function to encourage continuing improvement in the procedures adopted by the Intelligence Agencies, and their publication (and indeed such improvement took place as a consequence of our judgments in **Liberty/Privacy No 1**, **Liberty/Privacy No 2** and **Belhadj**), but it does not conclude that it is necessary, every time an inadequacy, particularly an inadequate publication, is identified, to conclude that that renders all previous conduct by the Respondents unlawful*."

63. We are in this case addressing the issue of collection of personal data or communications data in bulk. Contrary to the view set out by Sir Swinton Thomas in the 2004 correspondence with the Home Office referred to in paragraph 54 above, Article 8 is engaged by the transfer and storage of

communications data even if it is not accessed.

64. We have resolved the challenge to the domestic legality of BCD. There has been no challenge to the domestic legality of the collection of BPD. The relevant underlying statutory provisions apart from s.94 (ss 5 and 7 of ISA 1994 and ss 5, 8, 28, 29 and 43 of RIPA) both provide for and incorporate safeguards, and there are relevant codes of practice (Covert Human Intelligence Sources Codes of Practice (2002, 2010 and 2014), Covert Surveillance and Property Interference Codes of Practice (2002, 2010 and 2014), the Equipment Interference Code of Practice (**2016)** and the Interception of Communications Codes of Practice (2002 and **2016).**

65. The ISC described the position as to BPD in its March report:

> "***Internal controls.***
>
> *161. The [SIAs] have told the Committee that the acquisition and use of Bulk Personal Datasets is tightly controlled and that the HRA 'triple test' (i.e. 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 [SIAs] each have a review panel, chaired by a senior official, which meets every six months to review the Bulk Personal Datasets currently held by the Agency. Within MI5 each Bulk Personal Dataset has a different review period, depending on the level of intrusion and corporate risk it carries. Datasets that are found not to have sufficient operational value are deleted.*
>
> *163. The [SIAs] 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."*

66. The Respondents in the April Response set out what they submit to be the adequate safeguards by way of protection against arbitrary conduct. As to both BCD and BPD they recite the following: --

> *(a) Detailed internal guidance on the requirements of necessity and proportionality (having regard to the privacy of those whose data is contained in the BPD) including the need to consider other, less intrusive, methods of obtaining the information;*
>
> *(b) Specific consideration of sensitive data and confidential data;*
>
> *(c) A clear policy on the storage of and access to BPD;*
>
> *(d) Specific retention periods and retention/deletion policies which apply to BPD;*
>
> *(e) Policies on the handling and disclosure of BPD;*
>
> *(f) Clear guidance on the serious consequences of failure to comply with the Handling Arrangements, which include disciplinary action, including potentially dismissal, and*

prosecution;

(g) Training;

(h) Oversight, both internal and external."

Prior to avowal

67. The two significant questions to be asked in relation to the period prior to avowal, in the light of the principles of ECHR jurisprudence which we have set out, are as follows:

(i) Given that there were 'under the waterline' rules and arrangements, was there sufficient foreseeability or accessibility, or 'signposting', to comply with the requirements which we have set out above, as to (a) the existence of BCD and BPD, (b) the nature of the controls over them?

(ii) Whereas in **Kennedy** the ECtHR , and in **Liberty/Privacy** and **Greennet** the Tribunal, was satisfied as to the degree and effectiveness of oversight by independent Commissioners, does the same apply here, or if there be an inadequacy of supervision, what is the effect on our conclusion?

Foreseeability

68. As to foreseeability, we refer to what we said in **Greennet** with regard to Computer Network Exploitation (CNE):

"*81 ...* [I]*t is clear that prior to February 2015 there was no admission that property interference by GCHQ (governed by the Property Code) extended to CNE by the use of a s. 5 warrant ... Nevertheless it was quite clear that at least since 1994 the powers of GCHQ have extended to computer interference (under s. 3 of ISA). It was thus apparent in the public domain that there was likely to be interference with computers, 'hacking' being an ever more familiar activity, namely interference with property by GCHQ (and see in particular the 1990 Hansard references ...), and that if it occurred it would be covered by the Property Code. Use of it was thus foreseeable, even if the precise form of it and the existence of its use was not admitted.*"

69. The Respondents submitted in paragraph 66 of their Skeleton Argument that:

"*This applies with equal force to the present case where:*

(a) although the use of s. 94 to obtain BCD had not been publicly avowed, it was nonetheless foreseeable, because (i) GCHQ and MI5's acquisition of communications data in more general terms was publicly known (albeit pursuant to a warrant issued under s. 8(4) of RIPA or by an authorisation under Part 1 Chapter II of RIPA). There was therefore nothing secret about the essential activity of acquisition of such data by those agencies; and (ii) s94 itself clearly extended to requiring [PSENs] to provide BCD in the interests of national security; and

(b) although the use by the SIA of Bulk Personal Datasets had not been avowed, the acquisition of personal data in bulk was foreseeable because (i) the Respondents' powers to obtain information clearly extend to obtaining personal data; (ii) the acquisition of large volumes of such personal information was also foreseeable, albeit subject to statutory requirements of necessity and proportionality; and (iii) the inclusion

within such bulk personal data of information relating to individuals who were unlikely to be of intelligence interest (which would include, for instance, a telephone directory or electoral roll) was also foreseeable, again subject to the requirement that any acquisition of such data was necessary and proportionate; and

(c) in both cases, the use of BCD/BPD was foreseeable "even if the precise form of it and the existence of its use was not admitted."

70. The situation here in our judgment is however quite distinct. In that case there was a Property Code. In this case there were, at the relevant times, no Codes of Practice relating to either BCD or BPD, or anything approximating to them. Interception, even bulk interception, by warrant was sufficiently known about, but this is a long way from BCD or BPD. At least in the case of BPD, concern was expressed, emanating from the SIAs themselves, in the Respondents' own documents now disclosed during the course of these proceedings, as to the absence of knowledge on the part of the public about it:

(i) In a Review of Agency Handling of Bulk Personal Data dated February 2010 by a Mr Hannigan, then of the Cabinet Office, he wrote

(a) at paragraph 6.2: "*It is difficult to assess the extent to which the public is aware of agencies' holding and exploiting in-house personal bulk datasets, including data on individuals of no intelligence interest*." and

(b) at paragraph 36: "*Although existing legislation allows companies and UK Government Departments to share personal data with the agencies if necessary in the interests of national security, the extent to which this sharing takes place may not be evident to the public*."

(ii) In the (then unpublished, but now disclosed) MI5 Policy for Bulk Data Acquisition, Sharing, Retention & Deletion issued on 19 October 2010 it was stated: "*The fact that the Service holds bulk financial, albeit anonymised, data is assessed to be a HIGH corporate risk, since there is no public expectation that the Service will hold or have access to this data in bulk. Were it to become widely known that the Service held this data, the media response would most likely be unfavourable and probably inaccurate*."

In any event it seems difficult to conclude that the use of BCD was foreseeable by the public, when it was not explained to Parliament; and several opportunities arose when legislation or Codes of Practice were being introduced or amended (and particularly in 2000 when s.80 of RIPA was passed), when the government of the day did not avow the use of s.94.

71. The Respondents attached helpful Appendices to their Skeleton Argument, setting out, by reference to the disclosed evidence (some of it redacted), the detailed rules and arrangements which related to BCD (GCHQ and MI5) and BPD (all three SIAs) during the period since at least 2010. However, none of those rules or arrangements were previously disclosed or signposted, prior to the publication of the Handling Arrangements in November 2015.

<u>Supervision/Oversight</u>

72. This is the other underlying question, and it is not a straightforward picture. We shall consider the position separately in respect of BCD and BPD.

73. What is clear is that, as set out in the Agreed Facts in paragraph 19 above, there was no statutory oversight of BPD prior to March 2015, when the Prime Minister gave his Direction as set out in

paragraph 13 above, and that there has never been any statutory oversight of BCD, save in respect (in both cases) of data obtained under RIPA, which would fall under the responsibility of the I C C under ss.57 and 58 of RIPA, or under the ISA 1994, in which case the I S Commissioner had responsibility for its oversight under ss.59 and 60 of RIPA.

74. Mr. de la Mare submits that any but statutory supervision is wholly ineffective, because of the absence of the statutory powers and duties contained in those sections. We are not persuaded that that is a sufficient answer to the Respondents' case that there was in fact effective independent oversight by the Commissioners which indeed led to the disclosure of errors from time to time, which they caused to be remedied. It is necessary to look at what in fact occurred.

75. As for BCD, dealing with the successive I C Cs, Sir Swinton Thomas carried out some oversight from 2006, and as from the appointment of his successor, Sir Paul Kennedy, and then Sir Anthony May, there were six-monthly reviews of the databases and of their use. They were provided with a list setting out details of all s.94 Directions and any that had been cancelled, although in the July Review the current I C C, Sir Stanley Burnton, criticises the lack of codified procedures and a sufficiently accessible and particularised list.

76. Sir Mark Waller as I S Commissioner also included a review of BCD within his responsibility upon his six-monthly visits, and he reviewed the use of the datasets and the case for their acquisition and retention, including necessity, proportionality and the risk of collateral intrusion. He included consideration of BCD in all his Reports between 2011 and 2015. Those Reports and the witness evidence from the SIAs show that he was concerned to carry out a perceptive examination and analysis both of the directions and the use of the data, but he did not carry out a detailed audit.

77. Both Commissioners approved and subsequently reviewed the ('under the waterline') GCHQ Compliance Guide relating to s.94 Directions.

78. From March 2015 Sir Anthony May was asked to take over full responsibility for oversight of BCD, and agreed to do so as from July 2015, provided that he was given additional staff and enabled to carry out the work properly, and it was only by December 2015 that his successor Sir Stanley Burnton was in a position to do so. At this stage his inspectors were provided with full access to the MI5 electronic systems which processed authorisations for access to the database and communications data requests made to the PECNs, and they undertook query-based searches and random sampling of the MI5 system for authorising access to the database and reviewed requests for authorisations relating to the database, and that process, as we have been informed by the I C C's office, continues in place.

79. Sir Stanley Burnton recorded his conclusion in paragraph 2.5 of the July Review that, leaving aside the involvement of the I S Commissioner, oversight by the I C C of BCD prior to 2015 was "*limited because it was only concerned with the authorisations to access the communications data obtained pursuant to the directions. The oversight was not concerned with, for example, the giving of the section 94 directions by the Secretary of State (including the necessity and proportionality judgments by the agency or Secretary of State) or the arrangements for the retention, storage and destruction of the data*."

80. There were internal audits pursuant to the internal Compliance Guidance, and there was a regular review of the Directions by the Home Secretary (MI5) and the Foreign Secretary (GCHQ). However, we are not satisfied that, particularly given the fragmented nature of the responsibility apparently shared between the Commissioners, there can be said to have been an adequate oversight of the BCD system, until after July 2015. In the absence of the necessary oversight and supervision by the I C C, the secondary roles of this Tribunal and the ISC were no replacement.

81. We turn to BPD, in respect of which it is plain that it was determined as a result of the 2010 report

by Mr. Hannigan referred to in paragraph 70 above (and as later recorded in the Introduction to the Joint Bulk Personal Data Policy of November 2015), that there should then be an improvement in respect of its oversight. Although there had been some oversight of BPD prior to 2010 by the then I S Commissioner Sir Peter Gibson, and Sir Paul Kennedy as I C C included consideration of BPD on his visits between January 2011 and May 2015, the major oversight of BPD was by Sir Mark Waller, Sir Peter Gibson's successor, as from December 2010, on his bi-annual visits. There is a short summary of his supervision in paragraph 56 of the Respondents' Amended Response to the Claimant's Supplemental Request for Further Information. This does not adequately take into account (because it was prior to their disclosure in open) the content of the Confidential Annexes to his Reports, particularly those between 2011 and 2013, which we have read, and, for example, in the 2013 Annexe he referred to the nature of his oversight of BPD:

> "**Firstly I require the services to provide me with a list of all data sets held. What I am concerned to do is to assess whether the tests of the necessity and proportionality of acquiring and retaining the data sets has been properly applied in relation to decisions to acquire, retain or delete those data sets. This is normally quite straightforward because each service has an internal review body which considers the retention of data sets on a regular basis and records the decision in writing. These documents are available for me to inspect.*
>
> **I then consider how operatives and which operatives gain access to the data sets and review how the necessity and proportionality (i.e. the justification) of that intrusion is maintained.*
>
> **Finally I review the possible misuse of data and how this is prevented. I consider this to be the most important part of my oversight in that it seems to me that*
>
> **it is critical to that access to bulk data is properly controlled and*
>
> **it is the risk that some individuals will misuse the powers of access to private data which **must** be most carefully guarded against.*"

We have considered the relevant parts of his recent Report of 8th September, since the hearing, and the short written submissions of the parties in relation to it, which we invited. It is apparent that he has continued a rigorous oversight, and he will no doubt consider as such oversight continues, the important suggestions which the Claimant makes.

82. Although the oversight by the I S Commissioner was not made statutory until March 2015, as set out in paragraph 13 above, the careful recital was that:

> "*The Intelligence Services Commissioner must <u>continue</u>* [our underlining] *to keep under review ...*"

It was thus recognised that the supervision had previously existed. We are satisfied that during the period of Sir Mark Waller's supervision the independent oversight of BPD had been and continued to be adequate.

<u>Conclusions as to BCD and BPD in the period pre-Avowal</u>

83. Criticisms are made by the Claimant of the BPD and BCD systems which antedate March 2015, including specifically processes relating to BPD, which were discontinued (or corrected) in (severally) 2012, 2013, 2014 and February 2015 (paragraphs 78(b), 78(e), 77 and 78(c) of the Claimant's Skeleton Argument), and in relation to BCD in November 2015 (paragraph 68(d)). In particular there was no adequate dealing with legal and professional privilege until after this Tribunal's decision in **<u>Belhadj</u>** in February 2015. However most of the criticisms were either

overtaken by the public avowal of the existence of BCD and BPD and the publication of the Handling Arrangements, or they remain as criticisms now, to consideration of which we shall return below.

84. Our conclusion is in any event that by virtue of the matters which we have set out in paragraphs 67 to 81 above:

> (i) The BPD regime failed to comply with the ECHR principles which we have above set out throughout the period prior to its avowal in March 2015.
>
> (ii) The BCD regime failed to comply with such principles in the period prior to its avowal in November 2015, and the institution of a more adequate system of supervision as at the same date.

In those circumstances there is no call for consideration of the details of such systems prior to those dates, save insofar as there are continuing criticisms, as considered below.

Post-Avowal

85. We shall therefore consider whether there can be said to be compliance of the regimes with the "in accordance with law" requirement of Article 8 in respect of the period since November 2015 (BCD) and March 2015 (BPD).

86. We have already stated in paragraph 61 above that we do not change our previously concluded views in **Liberty/Privacy** that, provided there are otherwise adequate safeguards, the absence of prior judicial authorisation or of subsequent notification to a subject of interception does not render the system in breach of Article 8, though in respect of both of these aspects there may be changes if Parliament passes the new Bill as it presently stands. However, neither in that regard nor in any other do we consider it necessary or appropriate (as stated in paragraph 19 above) to carry out (nor have we been invited to carry out) some kind of tick-box exercise to see what changes or improvements are contained in the present Bill. Further, just as the fact that there have been improvements does not necessarily mean that the previous system prior to the improvements was non-compliant (paragraph 62 above), similarly the fact that there could be further improvements does not mean of itself that the present system is non-compliant.

87. As noted at paragraph 64 above the statutory framework (set out in detail in the Appendices to this Judgment), which governs the use by the SIAs of BCD and BPD, is significant:

> (i) in relation to the matters we are considering, each of the SIAs may only exercise its powers for the purpose of exercising the statutory functions of protecting national security, safeguarding the economic well-being of the United Kingdom from external threats, or supporting law enforcement agencies in the prevention or detection of serious crime:
>
> (ii) each of the SIAs is under a duty, imposed by arrangements made under statute (e.g. SSA 1989 s.2 (2)(a)) not to obtain any information, by any means, except so far as is necessary for the proper discharge of its functions or disclosed to others except for prescribed purposes and
>
> (iii) there are substantial statutory protections, in particular under the Official Secrets Act 1989, against the misuse by any person of information obtained by the SIAs.

88. We turn to deal with the specific criticisms made by the Claimant in respect of the present and continuing arrangements, which we have set out in Appendices A (BCD) and B (BPD) to this Judgment, extracted from the Appendices to the Respondents' Skeleton, referred to in paragraph 71

above. There were few such criticisms, but they seem to us all (with one potential exception, referred to in paragraph 95 below) not to amount to invalidation of the arrangements presently constituted and published, which are all subject to the statutory duties of the SIAs under the SSA 1989 and the ISA 1994, to the other statutory provisions there referred to (including the Data Protection Act 1998) and to the continuing oversight by the Commissioners.

89. In the July Review of directions given under s.94, published in July **2016,** the I C C made recommendations at section 12, and made observations at section 4 as to matters which could be included in a code of practice, if one were to be promulgated. The Claimant in its skeleton argument at paragraph 73 places reliance on the point that not all the matters referred to in paragraphs 4.14 and 4.15 have yet been adopted in practice. However the Commissioner acknowledges that there is no provision under s.94 for a Code of Practice to be issued, and his formal recommendations are those set out at section 12, and we repeat what we said in paragraph 86 above as to the relevance of improvements, or proposed improvements.

90. It is important to note that the July Review was not addressing compliance with Article 8 (because of the fact that this application to this Tribunal was outstanding), nor are all the formal recommendations in section 12 material to the issues which we have to consider. Many of those recommendations as to the process to be followed are designed to ensure that adequate records are kept, and notifications made, so that the Commissioner can properly review the operation of the s.94 regime. Other recommendations are intended to ensure that the scope of the requirements imposed on the PECNs are clear. However the issue for us to consider is whether any of the recommendations indicate that there are not currently effective safeguards against arbitrary or abusive use of the s.94 power. The fact that the Commissioner has himself identified administrative improvements that should be made is indicative of the effective operation of oversight of the SIAs in this area.

91. The most significant of the points emerging from the July Review and from the Claimant's submissions relating to it are these:

    (i) There is no present limit on the duration of a s. 94 direction, i.e. to the period during which the PECNs should continue to comply with it and provide data. The Commissioner did not make a recommendation that there should be a maximum duration imposed on directions made under s.94, but advised at paragraph 4.14 its proposed inclusion in a code of practice; such a requirement was not included in his recommendations in section 12. However, we are satisfied that under the Handling Arrangements (and as appears in the Agreed Facts, at paragraph 19(a)(v)) there are adequate restrictions imposed on the SIAs in relation to the duration for which the data can be retained (thus protecting the interests of the persons whose communications data has been obtained), and there are also provisions for a review of the directions.

    (ii) The Commissioner did recommend that there should be standardised processes for the review of directions, and the reporting of errors. We consider that the comprehensive Handling Arrangements, combined with proper oversight by the Commissioners, do adequately provide effective safeguards.

    (iii) There are recommendations by the Commissioner as to what should be included in a s.94 direction. A further specification may in due course be introduced, but in our Judgment, given the adequacy of the safeguards provided by the published Handling Arrangements, such is not necessary for compliance with Article 8.

The I C C concluded (at paragraph 11.10) that the relevant agencies had introduced comprehensive procedures, in accordance with the Handling Arrangements, to ensure that they only acquired and retained bulk communications data, and then accessed and undertook analysis of that data, in order to pursue their functions under SSA 1989 or ISA 1994. The essential protection against a potential

abuse of power under s.94, namely a requirement that the BCD may only be obtained and used for proper purposes, is thus provided by law, and subject to effective oversight.

92. MI5 and GCHQ differ in the systems they operate so far as access to BCD is concerned. Neither of them adopt the need for a warrant, as will be provided by the new Bill, if enacted. The Claimant submits that there is inappropriate reliance by GCHQ upon the RIPA safeguards relating to intercept, which they operate, without appreciating the difference, namely the absence of the specific safeguards effected by ss.15 and 16 of RIPA. MI5 adopt (as discussed in paragraph 54 above) a system analogous to that under ss.21 and 22 of RIPA, but did not, a matter of severe criticism by the I C C, have a system with a sufficiently independent designated person such as would comply with the Communications Data Code of Practice. This is a matter which, while not accepting such criticism, the Respondents have met by agreeing, by a letter dated 7th July **2016** written by MI5 to the Home Secretary, to introduce a new procedure. While it is not yet known whether this will be satisfactory to the I C C, this indicates the effectiveness of the I C C's oversight.

93. In considering acquisition of BCD, and access to such data held, the essential requirement in this context is that the BCD is acquired only for proper purposes, where the acquisition of the data is necessary and proportionate. The Handling Arrangements are clear in this respect (see Appendix A at paragraphs 35 and 39). As noted above, the I C C, having reviewed the directions which have been made under s.94, was satisfied that they had all been issued for proper purposes. In relation to BPD, the statutory duties imposed on the SIAs govern the obtaining of all information, with or without a warrant, so that information used to constitute BPDs can only be obtained for proper purposes. If the data is required to be obtained by the exercise of any statutory power (e.g. under RIPA or ISA) then the relevant statute will provide the necessary protection. If no statutory power is required to be exercised, for example if the information may be purchased commercially, then the relevant issue is how such data is retained and used. The material potential intrusion on privacy arises from the retention and use of such data, and it is at that point that safeguards must be applied. As noted above, the Handling Arrangements are clear as to the conditions under which any BPD may be obtained or accessed, and the operation of those arrangements is subject to independent oversight

94. Whatever the failings in the system of oversight obtaining prior to avowal of these powers, the system now in operation does, in our judgment, operate effectively. The I C C has conducted a review of the s. 94 powers. The lines of demarcation between the two Commissioners in relation to the use of BCD have been agreed. The I S Commissioner has, as referred to in paragraph 81 above, recently published his annual Report for 2015, which contains a review of the BPD regime. The fact that these reviews are not uncritical, and, particularly on the part of the I C C, contain recommendations for improvement, indicates that the system of oversight is effective.

95. The only area in which we need to give further consideration relates 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. There are detailed provisions in the Handling Arrangements which would appear to allow for the placing of restrictions in relation to such transfer upon the subsequent use and retention of the data by those parties. It is unclear to us whether such restrictions are in fact placed, and in paragraph 48.2 of their Note of 29 July **2016** the Respondents submit that the Tribunal is not in a position to decide this issue. We would like to do so and invite further submissions.

96. This leaves the question, in relation to BPD, of the period between Avowal in March 2015 and 4 November 2015 when the Handling Arrangements were published, given our conclusion that in relation to BPD, unlike BCD, the independent oversight was and continued to be adequate, and in any event so far as Avowal is concerned, the earlier date applied to BPD but not to BCD. The question is whether during the period between March and November 2015 there was compliance

with Article 8 in respect of the BPD regime, when there was not publication of the Handling Arrangements until 4 November 2015.

97. A joint SIA Bulk Personal Data Policy came into force in February 2015, which was to very similar effect as the subsequently published 4 November joint Handling Arrangements, so far as concerned arrangements for acquisition, use, sharing, retention and deletion/destruction; and in addition the relevant provisions of GCHQ's Compliance Guide and the underlying forms and guidance continued in effect, as did the MI5 Bulk Personal Data Guidance, with new versions of various forms continuing to be issued thereafter. MI6 also continued to be subject to similar Guidance. Of course none of these were in the public domain, but formed the basis for the fully considered open and closed handling arrangements once issued on 4 November 2015.

98. The issue for us is to decide whether the absence of publication of these arrangements ('below the waterline'), which were at all times subject to the approval and supervision of the I S Commissioner, renders the BPD non-compliant with Article 8 prior to 4 November 2015. We have referred to the ISC, and quoted from its Report in some detail in paragraph 65 above, from which it is plain that it contained considerable open description, not only of the existence of the BPD process and system, but of the way it operated and the controls to which it was subject.

99. The ISC had a concern, which it expressed, that the supervision was non-statutory, and that of course was immediately resolved in March 2015, and that there was no express legislation in respect of BPD. The only other concern which it expressed (paragraph 163 of the Report) is that to which we have referred in paragraph 95 above, namely that "*while these controls apply inside the [SIAs], they do not apply to overseas partners with whom the [SIAs] may share the datasets*."

100. We are satisfied, in respect of the BPD regime, that as from 12 March 2015 (the date of the ISC Report) there was sufficient satisfaction of the principle of foreseeability.

101. Accordingly, our conclusion is, in respect of Issues 2 and 3, that, subject to the issue of transfer of data, and to resolution of Issue 4 below, the s.94 BCD regime did not comply with Article 8 until November 4 2015 and thereafter complies, and that the BPD regime did not comply with Article 8 until 12 March 2015 and thereafter complies. We so decide.

102. It does not follow that a complainant who establishes that his or her complaint falls within the jurisdiction of this Tribunal, as explained in paragraphs 49 to 63 of our Judgment in **Human Rights Watch & Ors v Secretary of State for the Foreign & Commonwealth Office & Ors** [2016] UKIP Trib 15_165-CH, but who has no ground to believe that his or her data have been accessed and examined, would have an actionable personal complaint on the grounds that the BCD and BPD regimes under which such data were obtained and retained were, until those dates, non-compliant with Article 8 and therefore unlawful.

ISSUE 4:Proportionality

102. Since the hearing, Mr. Anderson QC has published, as referred to in paragraph 21 above, his Bulk Powers Review. It is plainly highly relevant to this issue, and we propose to grant both parties the opportunity to make submissions upon it before reaching our conclusions in respect of this issue, which we consequently adjourn, to come on to be heard at the same time as the EU law issues.

APPENDIX A: THE SECTION 94 REGIME

1. The regime in respect of section 94 of the Telecommunications Act 1984 which is relevant to the activities of the Intelligence Services principally derives from the following statutes:

(a) the Security Services Act 1989 ("the SSA") and the Intelligence Services Act 1994 ("the ISA");

(b) the Counter-Terrorism Act 2008 ("the CTA");

(c) Section 94 of the Telecommunications Act 1984;

(d) the Human Rights Act 1998 ("the HRA");

(e) the Data Protection Act 1998 ("the DPA"); and

(f) the Official Secrets Act 1989 ("the OSA").

2. In addition, GCHQ and MI5 have a number of **internal arrangements** in relation to Section 94; see below.

3. In addition:

(a) MI5 has, as a matter of practice and policy, applied the procedures and safeguards contained in the **Acquisition and Disclosure of Communications Data Codes of Practice** 2007 and 2015 to its access to Bulk Communications Data obtained under Section 94 of the Telecommunications Act 1984:

(b) GCHQ has throughout the periods under consideration as a matter of policy applied the appropriate safeguards set out in the Interception of Communications Code of Practice 2002 and, subsequently, the Interception of Communications Code of Practice **2016,** to all operational data, including BCD obtained under s.94 directions.

The SSA and ISA

Security Service functions

4. By s.1(2) to (4) of the Security Service Act 1989 ("SSA"), the functions of the Security Service are the following:

"the protection of national security and, in particular, its protection against threats from:

espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means."

"to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands."

"to act in support of the activities of police forces, the National Crime Agency and other law enforcement agencies in the prevention and detection of serious crime."

5. The Security Service's operations are under the control of a Director-General who is appointed by the Secretary of State (s.2(1)). By s.2(2)(a) it is the Director-General's duty to ensure:

"…that there are arrangements for securing that no information is obtained by the Service except so far as necessary for the proper discharge of its functions or disclosed by it except so far as necessary for that purpose or for the purpose of the prevention or detection of serious crime or for the purpose of any criminal proceedings;…"

GCHQ functions

6. By s. 3(1)(a) of the ISA, the functions of GCHQ include the following:

> *"... to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material ...."*

7. By s. 3(2) of the ISA, these functions are only exercisable:

> *"(a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or*
>
> *(b) in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or*
>
> *(c) in support of the prevention or detection of serious crime*."

8. GCHQ's operations are under the control of a Director, who is appointed by the Secretary of State (s. 4(1)). By s. 4(2)(a), it is the duty of the Director to ensure:

> *"... that there are arrangements for securing that no information is obtained by GCHQ except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or for the purpose of any criminal proceedings ..."*

9. The functions of each of the Intelligence Services, and the purposes for which those functions may properly be exercised, are thus prescribed by statute. In addition, the duty-conferring provisions in section 2(2)(a) of the SSA and sections 2(2)(a) and 4(2)(a) of the ISA, otherwise known as *"the information gateway provisions"*, place specific statutory limits on the information that each of the Intelligence Services can obtain and disclose. These statutory limits apply to the obtaining and disclosing of information from or to other persons both in the United Kingdom and abroad.

Counter-Terrorism Act 2008

10. By s.19 (1) of the Counter-Terrorism Act 2008 ("CTA") *"A person may disclose information to any of the intelligence services for the purposes of the exercise by that service of any of its functions*."

11. By s. 19(2) of the CTA:

> *"Information obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that service in connection with the exercise of any of its other functions*."

12. By s.19 (3) to (5) of the CTA, information obtained by the Intelligence Services for the purposes of any of their functions may:

> (a) In the case of the Security Service *"be disclosed by it – (a) for the purpose of the proper discharge of its functions, (b) for the purpose of the prevention or detection of serious crime, or (c) for the purpose of any criminal proceedings*." (s.19(3))
>
> (b) In the case of GCHQ "*be disclosed by it - (a) for the purpose of the proper discharge of its functions, or (b) for the purpose of any criminal proceedings*." (s.19(5))

13. By s.19 (6) any disclosure under s.19 "*does not breach –*

(a) any obligation of confidence owed by the person making the disclosure, or

(b) any other restriction on the disclosure of information (however imposed)."

14. Furthermore:

(a) s.19 does not affect the duties imposed by the information gateway provisions (s.19 (7) and s.20 (1) of the CTA).

(b) by s.20 (2) of the CTA, nothing in s.19 "*authorises a disclosure that-*

(a) contravenes the Data Protection Act 1998 (c.29), or

(b) is prohibited by Part 1 of the Regulations of Investigatory Powers Act 2000 (c.23)."

15. Thus, specific statutory limits are imposed on the information that the Intelligence Services can obtain, and on the information that it can disclose under the CTA.

Section 94 of the Telecommunications Act 1984

16. S.94 of the Telecommunications Act 1984 ("TA") provides:

"***94.- Directions in the interests of national security etc.***

(1) The Secretary of State may, after consultation with a person to whom this section applies, give to that person such directions of a general character as appear to the Secretary of State to:

be necessary in the interests of national security or relations with the government of a country or territory outside the United Kingdom.

(2) If it appears to the Secretary of State to be necessary to do so in the interests of national security or relations with the government of a country or territory outside the United Kingdom, he may, after consultation with a person to whom this section applies, give to that person a direction requiring him (according to the circumstances of the case) to do, or not to do, a particular thing specified in the direction.

(2A) The Secretary of State shall not give a direction under subsection (1) or (2) unless he believes that the conduct required by the direction is proportionate to what is sought to be achieved by that conduct.

(3) A person to whom this section applies shall give effect to any direction given to him by the Secretary of State under this section notwithstanding any other duty imposed on him by or under Part 1 or Chapter 1 of Part 2 of the Communications Act 2003 and, in the case of a direction to a provider of a public electronic communications network, notwithstanding that it relates to him in a capacity other than as the provider of such a network.

(4) The Secretary of State shall lay before each House of Parliament a copy of every direction given under this section unless he is of opinion that disclosure of the direction is against the interests of national security or relations with the government of a country or territory outside the United Kingdom, or the commercial interests of any person.

(5) A person shall not disclose, or be required by virtue of any enactment or otherwise to disclose, anything done by virtue of this section if the Secretary of State has notified him that the Secretary of

State is of the opinion that disclosure of that thing is against the interests of national security or relations with the government of a country or territory outside the United Kingdom, or the commercial interests of some other person.

(6) The Secretary of State may, with the approval of the Treasury, make grants to providers of public electronic communications networks for the purposes of defraying or contributing towards any losses they may sustain by reason of compliance with the directions given under this section.

(7) There shall be paid out of money provided by Parliament any sums required by the Secretary of State for making grants under this section.

(8) This section applies to OFCOM and to providers of public electronic communications networks."

17. The Secretary of State's power to give directions under section 94, whether of a general character (s.94 (1)) or requiring specific action (s.94 (2)) is limited to directions which appear to the Secretary of State to be "*necessary*" in the interests of national security or international relations (s.94 (1)) and which the Secretary of State believes to be "*proportionate*" to what is sought to be achieved. The Secretary of State must also first consult with the person to whom the direction is to be given (s.94(1) and (2)).

The HRA

18. Article 8 of the ECHR is a "Convention right" for the purposes of the HRA: s. 1(1) of the HRA. Art. 8, set out in Sch. 1 to the HRA, provides as follows:

"(1) Everyone has the right to respect for his private and family life, his home and his correspondence.

(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevent of disorder or crime, for the protection of health and morals, or for the protection of the rights and freedoms of others."

19. By s. 6(1):

"*It is unlawful for a public authority to act in a way which is incompatible with a Convention right.*"

20. Each of the Intelligence Services is a public authority for this purpose. Thus, when undertaking any activity that interferes with Art. 8 rights, the Respondents must (among other things) act proportionately and in accordance with law. In terms of bulk activity relating to and section 94 of the Telecommunications Act 1984, the HRA applies at every stage of the process i.e. authorisation/acquisition, use/access, disclosure, retention and deletion.

21. S. 7(1) of the HRA provides in relevant part:

"*A person who claims that a public authority has acted (or proposes to act) in a way which is made unlawful by section 6(1) may—*

(a) bring proceedings against the authority under this Act in the appropriate court or tribunal ...."

The DPA

22. Each of the Intelligence Services is a data controller (as defined in s. 1(1) of the DPA) in relation to all the personal data that it holds. "Personal data" is defined in s.1(1) of the DPA as

follows:

"*data which relate to a living individual who can be identified-*

> *i. from those data; or*
>
> *ii. from those data and other information which is in the possession of, or is likely to come into the possession of the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.*"

23. Insofar as the obtaining of an item of information by any of the Intelligence Services amounts to an interference with Art. 8 rights, that item of information will in general amount to personal data.

24. Consequently as a data controller, the Respondents are in general required by s. 4(4) of the DPA to comply with the data protection principles in Part I of Sch. 1 to the DPA. That obligation is subject to ss. 27(1) and 28(1) of the DPA, which exempt personal data from (among other things) the data protection principles if the exemption "*is required for the purpose of safeguarding national security*". By s. 28(2) of the DPA, a Minister may certify that exemption from the data protection principles is so required. Copies of the ministerial certificates for each of the Intelligence Services are available on request. Those certificates certify that personal data that are processed in performance of the Intelligence Services' functions are exempt from the first, second and eighth data protection principles (and are also exempt in part from the sixth data protection principle). Thus the certificates do not exempt the Intelligence Services from their obligation to comply with the fifth and seventh data protection principles, which provide:

"*5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. …*

1 The term "processing" is broadly defined in s. 1(1) of the DPA to include (among other things), obtaining, recording and using.

2 The content of the obligation imposed by the seventh data protection principle is further elaborated in §§9-12 of Part II of Sch. 1 to the DPA.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

25. Accordingly, when the Respondents obtain any information which amounts to personal data, they are obliged:

(a) not to keep that data for longer than is necessary having regard to the purposes for which they have been obtained and are being retained / used; and

(b) to take appropriate technical and organisational measures to guard against unauthorised or unlawful processing of the data in question and against accidental loss of the data in question.

The OSA

26. A member of the Intelligence Services commits an offence if "*without lawful authority he discloses any information, document or other article relating to security or intelligence which is or has been in his possession by virtue of his position as a member of any of those services*": s. 1(1) of the OSA. A disclosure is made with lawful authority if, and only if, it is made in accordance with the member's official duty (s. 7(1) of the OSA). Thus, a disclosure of information by a member of

any of the Respondents that is *e.g.* in breach of the relevant "arrangements" (under s. 4(2)(a) of the ISA) will amount to a criminal offence. Conviction may lead to an imprisonment for a term not exceeding two years and/or a fine (s. 10(1) of the OSA).

27. Further, a member of the Intelligence Services commits an offence if he fails to take such care, to prevent the unauthorised disclosure of any document or other article relating to security or intelligence which is in his possession by virtue of his position as a member of any of those services, as a person in his position may reasonably be expected to take. See s. 8(1) of the OSA, as read with s. 1(1). Conviction may lead to an imprisonment for a term not exceeding three months and/or a fine (s. 10(2) of the OSA).

Internal Handling Arrangements from 4 November 2015 to the date of the hearing and as at the date of the hearing

28. The Section 94 Handling Arrangements, which came into force on 4 November 2015, apply to bulk communications data obtained under section 94 of the Telecommunications Act 1984. They are mandatory and required to be followed by staff in the Intelligence Services. Failure to comply may lead to disciplinary action, which can include dismissal and prosecution (§§1.1-1.3).

29. The Section 94 Handling Arrangements expressly relate to communications data which is limited to "traffic data" and "service use information" (§2.2). These terms are defined at §3.5.1 and §3.5.2 by reference to s.21(4) and (6) of RIPA:

"3.5.1 ***Section 21(4)*** *of* ***RIPA*** *defines 'communications data' as meaning any of the following:*

- ***Traffic Data*** *– this is data that is or has been comprised in or attached to a communication for the purpose of its transmission [section 21(4)(a)];*

- ***Service Use Information*** *– this is the data relating to the use made by a person of a communications service [section 21(4)(b)];*

3.5.2 ***Section 21(6)*** *defines 'traffic data' for these purposes, in relation to any communication, as meaning:*

> *- any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted;*
>
> *- any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted;*
>
> *- any data comprising signals for the actuation of apparatus used for the purposes of a telecommunications system for effecting (in whole or in part) the transmission of any communication; and*
>
> *- any data identifying the data or other data as data comprised in or attached to a particular communication, but that expression includes data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored."*

30. The data provided does not contain communication content or Subscriber Information or Internet Connection Records (§2.3). Subscriber Information is defined at §3.5.1:

*"****Subscriber Information*** *– this relates to information held or obtained by a communications service provider about persons to whom the communications service provider provides or has*

provided communications services [section 21(4)(c)]."

31. §2.4 sets out the requirements contained in section 94 itself that the Secretary of State must be satisfied that a Section 94 direction is **necessary** and **proportionate**:

"*2.4 Any section 94 Directions under which this communications data is acquired requires the relevant Secretary of State to be satisfied that acquisition is necessary in the interests of national security or international relations and that the level of interference with privacy involved in doing so is proportionate to what it seeks to achieve*."

32. The requirement that acquisition, use, retention and disclosure of BCD have "*clear justification, accompanied by detailed and comprehensive safeguards against misuse*" and be "*subject to rigorous oversight*" is made clear (§4.0.1). The Section 94 Handling Arrangements are intended to provide such safeguards (§4.0.2).

33. The Section 94 Handling Arrangements set out provisions in respect of each of the stages of the lifecycle of BCD.

Acquisition

34. §§4.1.1-4.1.2 sets out the key considerations which must be presented to the Secretary of State when he/she considers whether to make a Section 94 Direction. These include the family considerations of necessity and proportionality, including whether a less intrusive method of obtaining the information is available, and the level of collateral intrusion involved:

"*4.1.1 Where the head of the relevant Intelligence Service has decided to request a Section 94 Direction from the relevant Secretary of State, it is essential that a submission is then presented to the Secretary of State by the Home Office/Foreign Office in order to enable them to consider:*

- whether acquisition and retention of the BCD to be authorised by the Direction is necessary in the interests of national security or international relations;

- whether the acquisition and retention of the BCD would be proportionate to what is sought to be achieved;

- whether there is a less intrusive method of obtaining the BCD or achieving the national security objective;

- the level of collateral intrusion caused by acquiring and utilising the requested BCD.

4.1.2 The submission must also outline any national security or international relations argument as to why the Secretary of State cannot lay the Direction before each House of Parliament in accordance with 94(4) of the Act."

35. Clear guidance is provided to staff on the considerations of **necessity** and **proportionality**:

"When will acquisition be "necessary"?

*4.1.3 What is **necessary** in a particular case is ultimately a question of fact and judgement, taking all the relevant circumstances into account. In order to meet the '**necessity**' requirement in relation to acquisition and retention, before presenting the submission referred to in paragraph 4.1.1 above, staff in the relevant Intelligence Service must consider why obtaining the BCD in question is 'really needed' for the purpose of discharging a statutory function of that Intelligence Service. In practice this means identifying the intelligence aim which is likely to be met and giving careful consideration as to how the data could be used to support achievement of that aim.*

The obtaining must also be "proportionate"

4.1.4 The obtaining and retention of the bulk communications dataset must also be ***proportionate*** *to the purpose in question. In order to meet the '****proportionality****' requirement, before presenting the submission referred to in paragraph 4.1.1 above, staff in the relevant Intelligence Service must balance (a) the level of interference with the right to privacy of individuals whose communications data is being obtained (albeit that at the point of initial acquisition of the BCD the identity of the individuals will be unknown), both in relation to subjects of intelligence interest and in relation to other individuals who may be of no intelligence interest, against (b) the expected value of the intelligence to be derived from the data. Staff must be satisfied that the level of interference with the individual's right to privacy is justified by the value of the intelligence that is sought to be derived from the data and the importance of the objective to be achieved. Staff must also consider whether there is a reasonable alternative that will still meet the proposed objective - i.e. which involves less intrusion.*"

36. Once made, a Section 94 Direction must be served on the CNP concerned in order that the relevant Agency can receive the requested dataset (§4.2.1).

37. Safeguards against unauthorised access are set out at §4.2.2:

"4.2.2 It is essential that any BCD is acquired in a safe and secure manner and that Intelligence Services safeguard against unauthorised access. Intelligence Services must therefore adhere to the controls outlined in the CESG6 Good Practice Guide for transferring and storage of data electronically or physically."

Access/Use

38. The Section 94 Handling Arrangements emphasise the importance of data security and protective security standards, confidentiality of data and preventing/disciplining misuse of such data:

"4.3.1 Each Intelligence Service must attach the highest priority to maintaining data security and protective security standards. Moreover, each Intelligence Service must establish handling procedures so as to ensure that the integrity and confidentiality of the information in BCD held is fully protected, and that there are adequate safeguards in place to minimise the risk of any misuse of such data and, in the event that such misuse occurs, to ensure that appropriate disciplinary action is taken."

39. As with BPD, specific, detailed measures are also set out 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:

"4.3.2 In particular, each Intelligence Service must apply the following protective security measures:

- *Physical security to protect any premises where the information may be accessed;*
- *IT security to minimise the risk of unauthorised access to IT systems;*
- *A security vetting regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy.*

4.3.3 Furthermore, each Intelligence Service is obliged to put in place the following additional measures:

- *Access to BCD must be strictly limited to those with an appropriate business requirement to use these data and managed by a strict authorisation process;*

- *Requests to access BCD must be justified on the grounds of **necessity** and **proportionality** and must demonstrate consideration of collateral intrusion and the use of any other less intrusive means of achieving the desired intelligence dividend.*

- *Intelligence Service staff who apply to access BCD must have regard to the further guidance on the application of the **necessity** and **proportionality** tests set out in paragraph 4.1.3 - 4.1.4 above.*

- *Where Intelligence Service staff intend to access BCD relating to the communications of an individual known to be a member of a profession that handles privileged information or information that is otherwise confidential (medical doctors, lawyers, journalists, Members of Parliament, Ministers of religion), they must give **special consideration** to the necessity and proportionality justification for the interference with privacy that will be involved;*

- *In addition, Intelligence Service staff must take particular care when deciding whether to seek access to BCD and must consider whether there might be unintended consequences of such access to BCD and whether the public interest is best served by seeking such access;*

- *In all cases where Intelligence Service staff intentionally seek to access and retain BCD relating to the communications of individuals known to be members of the professions referred to above, they must record the fact that such communications data has been accessed and retained and must flag this to the Interception of Communications Commissioner at the next inspection;*

- *In the exceptional event that Intelligence Service staff were to seek access to BCD specifically in order to determine a journalist's source, they should only do this if the proposal had been approved beforehand at Director level. Any communications data obtained and retained as a result of such access must be reported to the Interception of Communications Commissioner at the next inspection;*

- *Users must be trained on their professional and legal responsibilities, and refresher training and/or updated guidance must be provided when systems or policies are updated;*

- *A range of audit functions must be put in place: users should be made aware that their access to BCD will be monitored and that they must always be able to justify their activity on the systems;*

- *Appropriate disciplinary action will be taken in the event of inappropriate behaviour being identified;*

- *Users must be warned, through the use of internal procedures and guidance, about the consequences of any unjustified access to data, which can include dismissal and prosecution.*

- *In the exceptional event that Intelligence Service staff were to abuse their access to BCD – for example, by seeking to access the communications data of an individual without a valid business need – the relevant Intelligence Service must report the incident to the Interception of Communications Commissioner at the next inspection."*

Disclosure

40. The disclosure of BCD outside the Agency which holds can only occur if certain conditions are complied with:

"4.4.1 The disclosure of BCD must be carefully managed to ensure that it only takes place when it is

justified on the basis of the relevant statutory disclosure gateway. The disclosure of an entire bulk communications dataset, or a subset, outside the Intelligence Service may only be authorised by a Senior Official or the Secretary of State.

4.4.2 Disclosure of individual items of BCD outside the relevant Intelligence Service may only be made if the following conditions are met:

> *- that the objective of the disclosure falls within the Service's statutory functions or is for the additional limited purposes set out in sections 2(2)(a) and 4(2)(a) of the ISA 1994 and section 2(2)(a) of the SSA 1989;*
>
> *- that it is **necessary** to disclose the information in question in order to achieve that objective;*
>
> *- that the disclosure is **proportionate** to the objective;*
>
> *- that only as much of the information will be disclosed as is **necessary** to achieve that objective."*

41. Again, guidance is given to staff on the requirements of **necessity** and **proportionality**, in terms similar to those relating to acquisition, but with specific reference to disclosure:

"When will disclosure be necessary?

*4.4.3 In order to meet the '**necessity**' requirement in relation to disclosure, staff in the relevant Intelligence Service and (as the case may be) the Secretary of State must be satisfied that disclosure of the BCD is 'really needed' for the purpose of discharging a statutory function of that Intelligence Service.*

The disclosure must also be "proportionate"

*4.4.4 The disclosure of the BCD must also be **proportionate** to the purpose in question. In order to meet the 'proportionality' requirement, staff in the relevant Intelligence Service and (as the case may be) the Secretary of State must be satisfied that the level of interference with the right to privacy of individuals whose communications data is being disclosed, both in relation to subjects of intelligence interest and in relation to other individuals who may be of no intelligence interest, is justified by the benefit to the discharge of the Intelligence Service's statutory functions which is expected as a result of disclosing the data and the importance of the objective to be achieved. Staff must consider whether there is a reasonable alternative that will still meet the proposed objective - i.e. which involves less intrusion. For example, this could mean disclosure of individual pieces of communications data or of a subset of the bulk communications data rather than of the whole bulk communications dataset."*

42. Prior to any disclosure of BCD, staff must also take reasonable steps to ensure the intended recipient organisation "*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 with respect to such arrangements (§4.4.5). This applies to all disclosure, including to other Agencies (§4.4.6), and whether disclosure is of an entire BCD, a subset of a BCD or an individual piece of data from a BCD (§4.4.6).

43. Disclosure of the whole or subset of a BCD may only be authorised by a Senior Official (equivalent to a member of the Senior Civil Service) or the Secretary of State (§4.4.1).

<u>Retention/review/deletion</u>

44. The requirement on each of the Intelligence Services to review the justification for continued retention and use of BCD is set out at §§4.5.1-4.5.2:

"4.5.1 Each Intelligence Service must regularly review, i.e. at intervals of no less than six months, the operational and legal justification for its continued retention and use of BCD. This should be managed through a review panel comprised of senior representatives from Information Governance/Compliance, Operational and Legal teams.

4.5.2 The retention and review process requires consideration of:

> *- An assessment of the value and use of the dataset during the period under review and in a historical context;*
>
> *- the operational and legal justification for ongoing acquisition, continued retention, including its necessity and proportionality;*
>
> *- The extent of use and specific examples to illustrate the benefits;*
>
> *- The level of actual and collateral intrusion posed by retention and exploitation;*
>
> *- The extent of corporate, legal, reputational or political risk;*
>
> *- Whether such information could be acquired elsewhere through less intrusive means.*

4.5.3 Should the review process find that there remains an ongoing case for acquiring and retaining BCD, a formal review will be submitted at intervals of no less than six months for consideration by the relevant Secretary of State. In the event that the Intelligence Service or Secretary of State no longer deem it to be necessary and proportionate to acquire and retain the BCD, the Secretary of State will cancel the relevant Section 94 Direction and instruct the CNP concerned to cease supply. The relevant Intelligence Service must then task the technical team[s] responsible for Retention and Deletion with a view to ensuring that any retained data is destroyed and notify the Interception of Communications Commissioner accordingly. Confirmation of completed deletion must be recorded with the relevant Information Governance/Compliance team."

Oversight

45. The Section 94 Handling Arrangements also set out provisions in relation to internal and external oversight.

46. §§4.6.1-4.6.2 concern internal oversight. A senior member of an Intelligence Service's internal review panel (see paragraph 44 above) must keep that Service's Executive Board apprised of BCD holdings (§4.6.1). In addition internal audit teams must monitor use of IT systems:

"4.6.2 Use of IT systems is monitored by the audit team in order to detect misuse or identify activity that may give rise to security concerns. Any such identified activity initiates a formal investigation process in which legal, policy and HR (Human Resources) input will be requested where appropriate. Disciplinary action may be taken, which in the most serious cases could lead to dismissal and/or the possibility of prosecution under the Computer Misuse Act 1990, the Data Protection Act 1998, the Official Secrets Act 1989 and Misfeasance in Public Office depending on circumstances."

47. All reports on audit investigations are made available to the Interception of Communications Commissioner (§4.6.3).

48. §§4.6.4 to 4.6.7 address oversight by the Interception of Communications Commissioner:

*"4.6.4 The **Interception of Communications Commissioner** has oversight of:*

a) the issue of Section 94 Directions by the Secretary of State enabling the Intelligence Services to acquire BCD;

b) the Intelligence Services' arrangements in respect of acquisition, storage, access, disclosure, retention and destruction; and

c) the management controls and safeguards against misuse which the Intelligence Services have put in place.

4.6.5 This oversight is exercised by the Interception of Communications Commissioner on at least an annual basis, or as may be otherwise agreed between the Commissioner and the relevant Intelligence Service.

4.6.6 The purpose of this oversight is to review and test judgements made by the Secretary of State and the Intelligence Services on the necessity and proportionality of the Section 94 Directions and on the Intelligence Services' acquisition and use of BCD, and to ensure that the Intelligence Services' policies and procedures for the control of, and access to BCD are (a) are sound and provide adequate safeguards against misuse and (b) are strictly observed.

4.6.7 The Interception of Communications Commissioner also has oversight of controls to prevent and detect misuse of data acquired under Section 94, as outlined in paragraph 4.6.2 and 4.6.3 above."

49. The Secretary of State and the Intelligence Services must provide the Interception of Communications Commissioner with *"all such documents and information as he may require for the purpose of enabling him to exercise the oversight described…"* (§4.6.8)

Internal Section 94 Handling Arrangements

50. In addition to the published Section 94 Handling Arrangements, both GCHQ and MI5 have their own internal Section 94 Handling Arrangements, which were also in force from 4 November 2015. These reflect and supplement the published Section 94 Handling Arrangements. They are not separately set out in detail here.

GCHQ Compliance Guide

51. The relevant sections of the GCHQ Compliance Guide relating to the period from June 2014, which have been disclosed by the Respondents in these proceedings, continued after November 2015. In the October 2015 version of the Compliance Guide, the section dealing with review and retention provided that continued retention beyond the prescribed default periods must be subject to formal approval. Although the previous version of the Compliance Guide required that such retention should be reviewed and rejustified, in most cases annually, it had not previously been subject to the requirement of formal approval.

MI5 internal arrangements

52. MI5 continues to have internal guidance in addition to the Section 94 Handling Arrangements. In particular:

(a) From November 2015 the "Communications Data – Guidance on Justifications and Priorities" guidance was amended so that:

(a) Specific attention was drawn (and a link provided to) the MI5 Section 94 Handling

Arrangements which came into force on 4 November 2015; and

(b) Detailed guidance was provided in respect of communications data applications relating to members of sensitive professions.

Acquisition and Disclosure of Communications Data Codes of Practice

53. The authorisation process for access to the Section 94 database was, from the outset, the same as for requests to CSPs for CD under Part 1 Chapter II of RIPA. As a matter of practice and policy, MI5 has applied the applicable Codes of Conduct for the acquisition of communications data to the regime that it has operated for the database. In particular, investigators would – when completing requests for CD – be expected to comply with applicable parts of the Code of Practice relating to the acquisition of CD.

Acquisition and Disclosure of Communications Data Code of Practice 2007

54. The Acquisition and Disclosure of Communications Data Code of Practice 2007 ("the 2007 CD Code") related to the powers and duties conferred under Part 1 Chapter II of RIPA.

55. Relevant provisions of the 2007 CD Code include:

(a) Provisions emphasising and explaining the requirements of necessity and proportionality:

> (a) "*The acquisition of communications data under the Act will be a justifiable interference with an individual's human rights under Article 8 of the European Convention on Human Rights only if the conduct being authorised or required to take place is both necessary and proportionate and in accordance with law.*" (§2.1)
>
> (b) "*Consideration must also be given to any actual or potential infringement of the privacy of individuals who are not the subject of the investigation or operation. An application for the acquisition of communications data should draw attention to any circumstances which give rise to a meaningful degree of collateral intrusion.*" (§2.6)
>
> (c) Further explanation of proportionality at §§2.7-2.8.

(b) The procedure for making an application: at §§3.3-3.6, §§3.56-3.62.

(c) The role of "Designated Persons":

> (a) "*Exercise of the powers in the Act to acquire communications data is restricted to designated persons in relevant public authorities. A designated person is someone holding a prescribed office, rank or position with a relevant public authority that has been designated for the purpose of acquiring communications data by order.*" (§2.9)
>
> (b) "*The designated person must believe that the conduct required by any authorisation or notice is necessary. He or she must also believe that conduct to be proportionate to what is sought to be achieved by obtaining the specified communications data – that the conduct is no more than is required in the circumstances. This involves balancing the extent of the intrusiveness of the interference with an individual's right of respect for their private life against a specific benefit to the investigation or operation being undertaken by a relevant public authority in the public interest*" (§2.5) Further details were given at §§3.7-3.14.

(d) Provisions concerning disclosure, handling and storage of communications data: Chapter 7.

Acquisition and Disclosure of Communications Data Code of Practice 2015

56. The Acquisition and Disclosure of Communications Data Code of Practice of March 2015 ("the 2015 CD Code") contained similar provisions as to:

(a) Necessity and proportionality: see §2.1; §§2.6-2.9. However, more detailed guidance on necessity and proportionality was given at §§2.36-2.45.

(b) The procedure for making an application: §§3.3-3.6.

(c) Designated Persons: §2.10; §3.7ff.

(d) Disclosure, handling and storage of communications data: Chapter 7.

57. Guidance was also given in the 2015 CD Code about Communications Data involving specified professions: §3.72-§3.84.

Interception of Communications Codes of Practice (2002 and 2016)

58. GCHQ has throughout the periods under consideration as a matter of policy applied the appropriate safeguards set out in the Interception of Communications Code of Practice 2002 and, subsequently, the Interception of Communications Code of Practice **2016,** to all operational data, including BCD obtained under s.94 directions. Those Codes of Practice included provisions as to:

(a) **Necessity** and **proportionality** in relation to

(a) Applications for and the granting of warrants: **2016 Code**, §3.5-§3.7, §5.2-§5.5, §6.9-§6.11, §6.13.

(b) Renewal/cancellation of warrants: **2016 Code**, §3.21; §5.14; §5.17; §6.22.

(b) Requirement to consider potential collateral intrusion: **2016 Code**, §4.1;

(c) Safeguards in respect of disclosure, handling, copying and retention of material (**2016 Code**, §7.3, §7.5-§7.6, §7.9); storage and destruction (**2016 Code**, §6.8, §7.8).

APPENDIX B: THE BPD REGIME

1. The regime in respect of Bulk Personal Datasets ("BPD") which is relevant to the activities of the Intelligence Services principally derives from the following statutes:

(a) the Security Services Act 1989 ("the SSA") and the Intelligence Services Act 1994 ("the ISA");

(b) the Counter-Terrorism Act 2008 ("the CTA");

(c) the Human Rights Act 1998 ("the HRA");

(d) the Data Protection Act 1998 ("the DPA"); and

(e) the Official Secrets Act 1989 ("the OSA").

These are addressed below.

2. In addition,

(a) Where BPDs have been obtained by means of RIPA/ISA powers, the relevant **Codes of Practice** have been applied (see below); and

(b) GCHQ, MI5 and SIS have a number of **internal arrangements** in relation to BPD.

The SSA and ISA

Security Service functions

3. By s.1 (2) to (4) of the Security Service Act 1989 ("SSA"), the functions of the Security Service are the following:

"the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means."

> *"to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands*."
>
> *"to act in support of the activities of police forces, the National Crime Agency and other law enforcement agencies in the prevention and detection of serious crime*."

4. The Security Service's operations are under the control of a Director-General who is appointed by the Secretary of State (s.2 (1)). By s.2(2)(a) it is the Director-General's

duty to ensure:

"…that there are arrangements for securing that no information is obtained by the Service except so far as necessary for the proper discharge of its functions or disclosed by it except so far as necessary for that purpose or for the purpose of the prevention or detection of serious crime or for the purpose of any criminal proceedings;…"

SIS functions

5. By s.1 (1) of the ISA, the functions of SIS are:

"(a) to obtain and provide information relating to the actions or intentions of persons outside the British Islands; and

(b) to perform other tasks relating to the actions or intentions of such persons."

6. By s.1 (2) those functions are "*exercisable only-*

"(a) in the interests of national security, with particular reference to the defence and foreign polices of Her Majesty's Government in the United Kingdom; or

(b) in the interests of the economic well-being of the United Kingdom; or

(c) in support of the prevention or detection of serious crime."

7. SIS's operations are under the control of a Chief, who is appointed by the Secretary of State (s.2 (1)). The Chief of SIS has a duty under s.2(2)(a) of the ISA to ensure:

"(a) that there are arrangements for securing that no information is obtained by the Intelligence Service except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary-

> *(i) for that purpose;*

(ii) in the interests of national security;

(iii) for the purpose of the prevention or detection of serious crime; or

(iv) for the purpose of any criminal proceedings;"

GCHQ functions

8. By s. 3(1) (a) of the ISA, the functions of GCHQ include the following:

"*... to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material ....*"

9. By s. 3(2) of the ISA, these functions are only exercisable:

"*(a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or* 3

(b) in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or

(c) in support of the prevention or detection of serious crime."

10. GCHQ's operations are under the control of a Director, who is appointed by the Secretary of State (s. 4(1)). By s. 4(2)(a), it is the duty of the Director to ensure:

"*... that there are arrangements for securing that no information is obtained by GCHQ except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or for the purpose of any criminal proceedings ...*"

11. The functions of each of the Intelligence Services, and the purposes for which those functions may properly be exercised, are thus prescribed by statute. In addition, the duty-conferring provisions in section 2(2)(a) of the SSA and sections 2(2)(a) and 4(2)(a) of the ISA, otherwise known as "*the information gateway provisions*", place specific statutory limits on the information that each of the Intelligence Services can obtain and disclose. These statutory limits apply to the obtaining and disclosing of information from or to other persons both in the United Kingdom and abroad.

Counter-Terrorism Act 2008

12. By s.19 (1) of the Counter-Terrorism Act 2008 ("CTA") "*A person may disclose information to any of the intelligence services for the purposes of the exercise by that service of any of its functions*."

13. By s. 19(2) of the CTA:

"*Information obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that service in connection with the exercise of any of its other functions*."

14. By s.19 (3) to (5) of the CTA, information obtained by the Intelligence Services for the purposes of any of their functions may:

(a) In the case of the Security Service "*be disclosed by it – (a) for the purpose of the proper discharge of its functions, (b) for the purpose of the prevention or detection of serious crime, or (c)*

for the purpose of any criminal proceedings." (s.19(3))

(b) In the case of SIS "*be disclosed by it – (a) for the purpose of the proper discharge of its functions, (b) in the interests of national security, (c) for the purpose of the prevention or detection of serious crime, or (d) for the purpose of any criminal proceedings*." (s.19(4))

(c) In the case of GCHQ "*be disclosed by it - (a) for the purpose of the proper discharge of its functions, or (b) for the purpose of any criminal proceedings*." (s.19(5))

15. By s.19(6) any disclosure under s.19 "*does not breach –*

(a) any obligation of confidence owed by the person making the disclosure, or

(b) any other restriction on the disclosure of information (however imposed)."

16. Furthermore:

(a) s.19 does not affect the duties imposed by the information gateway provisions (s.19(7) and s.20(1) of the CTA).

(b) by s.20(2) of the CTA, nothing in s.19 "*authorises a disclosure that-*

(a) contravenes the Data Protection Act 1998 (c.29), or

(b) is prohibited by Part 1 of the Regulations of Investigatory Powers Act 2000 (c.23)."

17. Thus, specific statutory limits are imposed on the information that the Intelligence Services can obtain, and on the information that it can disclose under the CTA.

Other statutory bases for obtaining information

18. Information contained in a Bulk Personal Dataset may be obtained by other means, including pursuant to:

(a) Warrants issued under section 5 of the ISA in respect of property and equipment interference;

(b) Authorisations issued under section 7 of the ISA in respect of property and equipment interference;

(c) Intrusive surveillance warrants issued under section 43 of the Regulation of Investigatory Powers Act 2000 ("RIPA");

(d) Directed surveillance authorisations issued under section 28 of RIPA;

(e) Covert human intelligence authorisations issued under section 29 of RIPA; and

(f) Warrants for the interception of communications issued under section 5 of RIPA

19. It is important to note that these other statutory means of obtaining information are themselves subject to their own statutory requirements, in addition to any further requirements derived from the Handling Arrangements set out below.

The HRA

20. Article 8 of the ECHR is a "Convention right" for the purposes of the HRA: s. 1(1) of the HRA. Art. 8, set out in Sch. 1 to the HRA, provides as follows:

"(1) Everyone has the right to respect for his private and family life, his home and his correspondence.

(2) There shall be no interference by a public authority with the exercise of this right except 5 *such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevent of disorder or crime, for the protection of health and morals, or for the protection of the rights and freedoms of others*."

21. By s. 6(1):

"*It is unlawful for a public authority to act in a way which is incompatible with a Convention right*."

22. Each of the Intelligence Services is a public authority for this purpose. Thus, when undertaking any activity that interferes with Art. 8 rights, the Respondents must (among other things) act proportionately and in accordance with law. In terms of BPD-related activity, the HRA applies at every stage of the process i.e. authorisation/acquisition, use/access, disclosure, retention and deletion.

23. S. 7(1) of the HRA provides in relevant part:

"*A person who claims that a public authority has acted (or proposes to act) in a way which is made unlawful by section 6(1) may—*

(a) bring proceedings against the authority under this Act in the appropriate court or tribunal ...."

The DPA

24. Each of the Intelligence Services is a data controller (as defined in s. 1(1) of the DPA) in relation to all the personal data that it holds. "Personal data" is defined in s.1(1) of the DPA as follows:

"*data which relate to a living individual who can be identified-*

> *i. from those data; or*
>
> *ii. from those data and other information which is in the possession of, or is likely to come into the possession of the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual*."

25. Insofar as the obtaining of an item of information by any of the Intelligence Services amounts to an interference with Art. 8 rights, that item of information will in general amount to personal data.

26. Consequently as a data controller, the Respondents are in general required by s. 4(4) of the DPA to comply with the data protection principles in Part I of Sch. 1 to the DPA. That obligation is subject to ss. 27(1) and 28(1) of the DPA, which exempt personal data from (among other things) the data protection principles if the exemption "*is required for the purpose of safeguarding national security*". By s. 28(2) of the DPA, a Minister may certify that exemption from the data protection principles is so required. Copies of the ministerial certificates for each of the Intelligence Services are available on request. Those certificates certify that personal data that are processed in performance of the Intelligence Services' functions are exempt from the first, second and eighth data protection principles (and are also exempt in part from the sixth data protection principle). Thus the certificates do not exempt the Intelligence Services from their obligation to comply with the fifth and seventh data protection principles, which provide:

"*5. Personal data processed1 for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. …*

1 The term "processing" is broadly defined in s. 1(1) of the DPA to include (among other things), obtaining, recording and using.

2 The content of the obligation imposed by the seventh data protection principle is further elaborated in §§9-12 of Part II of Sch. 1 to the DPA.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

27. Accordingly, when the Respondents obtain any information which amounts to personal data, they are obliged:

(a) not to keep that data for longer than is necessary having regard to the purposes for which they have been obtained and are being retained / used; and

(b) to take appropriate technical and organisational measures to guard against unauthorised or unlawful processing of the data in question and against accidental loss of the data in question.

The OSA

28. A member of the Intelligence Services commits an offence if "*without lawful authority he discloses any information, document or other article relating to security or intelligence which is or has been in his possession by virtue of his position as a member of any of those services*": s. 1(1) of the OSA. A disclosure is made with lawful authority if, and only if, it is made in accordance with the member's official duty (s. 7(1) of the OSA). Thus, a disclosure of information by a member of any of the Respondents that is *e.g.* in breach of the relevant "arrangements" (under s. 4(2)(a) of the ISA) will amount to a criminal offence. Conviction may lead to an imprisonment for a term not exceeding two years and/or a fine (s. 10(1) of the OSA).

29. Further, a member of the Intelligence Services commits an offence if he fails to take such care, to prevent the unauthorised disclosure of any document or other article relating to security or intelligence which is in his possession by virtue of his position as a member of any of those services, as a person in his position may reasonably be expected to take. See s. 8(1) of the OSA, as read with s. 1(1). Conviction may lead to an imprisonment for a term not exceeding three months and/or a fine (s. 10(2) of the OSA).

RIPA/ISA Codes of Practice

30. As noted above at paragraph 18, BPDs may be obtained, inter alia, pursuant to warrants/authorisations issued under RIPA or ISA. The relevant statutory regimes themselves contain published safeguards (in relation to acquisition, retention, storage and destruction of material)) which are found in the following published Codes of Practice:

(a) Covert Human Intelligence Sources Codes of Practice (2002, 2010, 2014):

(a) Tests of **necessity** and **proportionality** in relation to:

> (i) Applications for and the granting of CHIS authorisations under Part II of RIPA: **2002 Code**: §§2.4-2.5, §4.14; **2010 Code**: §2.9, §§3.2-3.5, §§5.1-5.2, §5.10; **2014 Code**: §§3.4-3.5.

(ii) Renewal/cancellation of CHIS authorisations: **2002 Code**: §4.19, §4.25; **2010 Code**: §3.12, §3.14, §5.15, §5.18; **2014 Code**: §3.14, §3.16, §5.16, §5.18, §5.22, §5.28.

(b) Requirement to consider potential collateral intrusion: **2002 Code**: §§2.6-2.8, §4.19; **2010 Code**: §§3.8-3.11, §3.14, §5.10, §5.15; **2014 Code**: §§3.8-3.11, §3.16, §3.22.

(c) Safeguards in respect of disclosure, handling, copying and retention of intercepted material: **2002 Code**: §2.17; **2010 Code**: §8.1; **2014 Code:** §8.1; destruction: **2002 Code**: §2.17; **2010 Code**: §8.1; **2014 Code**: §8.1.

(b) Covert Surveillance and Property Interference Codes of Practice (2002, 2010 and 2014):

(a) Tests of **necessity** and **proportionality** in relation to:

(i) Applications for covert / intrusive / directed surveillance warrants under Part II of RIPA/property interference warrants under s.5 ISA: **2002 Code**, §§2.4-2.5, §2.10, §§4.9-4.10, §§5.8-5.9, §5.16, §§6.6-6.7; **2010 Code**, §§3.3-3.6, §5.8, §§6.3-6.4, §6.19, §§7.10-7.11, §§7.37-7.38; **2014 Code**, §§3.3-3.6, §5.8, §§6.3-6.4, §6.19, §6.30, §§7.10-7.11, §7.38.

(ii) Renewal/cancellation of : **2002 Code**: §§4.23-4.26, §4.28, §§5.36-5.37; **2010 Code**, §5.12, §5.16, §6.30, §7.27, §7.30, §§7.40-7.42; **2014 Code**, §5.12, §5.16, §6.25, §6.32, §7.40.

(b) Requirement to consider potential collateral intrusion: **2002 Code**: §§2.6-2.8, §5.16, §6.27; **2010 Code**, §3.6, §§3.8-3.11, §6.19, §6.32; **2014 Code**, §§3.8-3.11, §7.18.

(c) Safeguards in respect of disclosure, handling, copying and retention of intercepted material: **2002 Code**: §2.16; **2010 Code**: §9.3; **2014 Code**:

§9.3); and destruction: **2002 Code**: §2.18; **2010 Code**: §9.3; **2014 Code**: §9.3.

(c) Equipment Interference Code of Practice (**2016,** but published in draft form in February 2015):

(a) Tests of **necessity** and **proportionality** in relation to:

(i) Issuing of section 5 warrants/s.7 authorisations: §§2.4-2.8, §§4.6-4.7, §7.8, §7.13, ; and

(ii) Review/renewal/cancellation of s.5 warrants: §2.13, §§4.10-§4.13, §7.14, §7.17.

(b) Requirement to consider potential collateral intrusion: §§2.9-2.12.

(c) Safeguards in respect of disclosure, handling, copying and retention of material obtained by equipment interference: §3.13, §6.5, §6.7; storage (§6.8); destruction (§6.9).

(d) Interception of Communications Codes of Practice (2002 and **2016):**

(a) Tests of **necessity** and **proportionality** in relation to

(i) Applications for and the granting of s.8(1)/s.8(4) warrants: **2002 Code**, §§2.4-2.5, §§4.2-4.3, §4.5, §§5.2-5.3, §5.5; **2016 Code**, §3.5-§3.7, §5.2-§5.5, §6.9-§6.11, §6.13.

(ii) Renewal/cancellation of s. .8(1)/s.8(4) warrants: **2002 Code**, §4.13, §5.12; **2016**

Code, §3.21; §5.14; §5.17; §6.22.

(b) Requirement to consider potential collateral intrusion: **2002 Code**, §3.1; §4.2; **2016 Code**, §4.1;

(c) Safeguards in respect of disclosure, handling, copying and retention of intercepted material (**2002 Code**, §6.2, §6.4; **2016 Code**, §7.3, §7.5-§7.6, §7.9); storage (**2002 Code**, §6.7, §7.7); destruction (**2002 Code**, §6.8, §7.8).

Handling arrangements

From 4 November 2015 to the date of the hearing and as at the date of the hearing

BPD Handling Arrangements

31. On 4 November 2015 the BPD Handling Arrangements were published. These applied to each of GCHQ, MI5 and SIS.

32. The BPD Handling Arrangements apply to obtaining, use and disclosure of "bulk personal datasets" (§1.2) as defined at §2.2:

*"2.2 Among the range of information collected is **data that contain personal information about a wide range of individuals, the majority of whom are unlikely to be of any intelligence interest**. Typically these datasets are very large, and of a size which means they cannot be processed manually. Such datasets are referred to as **bulk personal datasets**. For the purposes of these Handling Arrangements, a 'bulk personal dataset' means any collection of information which:*

(a) Comprises personal data;

(b) Relates to a wide range of individuals, the majority of whom are unlikely to be of intelligence interest; and

(c) Is held, or acquired for the purpose of holding, on one or more analytical systems within the Intelligence Services."

33. "Personal data" is defined as having the meaning given to it in s.1(1) of the Data Protection Act 1998 (§2.3), but additionally includes data related to the deceased.

34. The purpose of the acquisition and use of BPD is explained at §§2.4-2.5:

"2.4 Bulk personal datasets may be acquired through overt and covert channels. Such datasets provide information about subjects of intelligence interest ("subjects of interest"), but inevitably also include information about those who are of no direct relevance to Intelligence Service operations. It is not possible to acquire the information that will be of direct value to these operations without also acquiring this additional data; indeed, at the point of acquisition it may not be known exactly which information will prove to be of value.

2.5 The Intelligence Services draw on this data and use it in conjunction with other data in order to perform their functions, for example, to identify subjects of interest, validate intelligence or to ensure the security of operations or staff. It may also be used to facilitate the exclusion of individuals from an investigation or in pursuit of other intelligence requirements. This ensures that the activities of the Intelligence Services are correctly and solely focused on those individuals or organisations that are relevant to the performance of their statutory functions."

35. The requirement that acquisition, use, retention and disclosure of BPD have *"clear justification,*

accompanied by detailed and comprehensive safeguards against misuse" and be "*subject to rigorous oversight*" is made clear (§2.6). The BPD Handling Arrangements are intended to provide such safeguards (§2.7) and must be complied with, along with the requirements of the information gateway provisions:

"*Staff must ensure that no bulk personal dataset is obtained, used, retained or disclosed* ***except in accordance with the information gateway provisions*** *and* ***these Arrangements.***"

36. The BPD Handling Arrangements apply to BPD "*howsoever obtained*", that is through whichever of the variety of statutory powers by which the Intelligence Services are entitled to obtain it (§§2.8-2.9) without prejudice to "*additional applicable statutory requirements*" which apply in the case of some statutory powers (§2.9).

37. The BPD Handling Arrangements set out provisions in respect of each of the stages of the lifecycle of a Bulk Personal Dataset.

Authorisation and Acquisition

38. The key requirements on staff of the Intelligence Services before obtaining BPD are set out at §4.2:

"based on the information available to them at the time, staff should always:

- *be satisfied that the objective in question falls within the Service's statutory functions;*

- *be satisfied that it is* ***necessary*** *to obtain and retain the information concerned in order to achieve the objective;*

- *be satisfied that obtaining and retaining the information in question is* ***proportionate*** *to the objective;*

- *be satisfied that only as much information will be obtained as is* ***necessary*** *to achieve that objective*."

39. Clear guidance is provided to staff on the considerations of **necessity** and **proportionality**:

"When will acquisition be "necessary"?

4.3 What is ***necessary*** *in a particular case is ultimately a question of fact and judgement, taking all the relevant circumstances into account. In order to meet the '****necessity****' requirement in relation to acquisition and retention, staff must consider why obtaining the bulk personal dataset is 'really needed' for the purpose of discharging a statutory function of the relevant Intelligence Service. In practice this means identifying the intelligence aim which is likely to be met and giving careful consideration as to how the data could be used to support achievement of that aim.*

The obtaining must also be "proportionate"

4.4 The obtaining and retention of the bulk personal dataset must also be ***proportionate*** *to the purpose in question. In order to meet the '****proportionality****' requirement, staff must balance (a) the level of interference with the individual's right to privacy, both in relation to subjects of interest who are included in the relevant data and in relation to other individuals who are included in the data and who may be of no intelligence interest, against (b) the expected value of the intelligence to be derived from the data. Staff must be satisfied that the level of interference with the individual's right to privacy is justified by the value of the intelligence that is sought to be derived from the data and the importance of the objective to be achieved. Staff must also consider whether there is a*

reasonable alternative that will still meet the proposed objective - i.e. which involves less intrusion.

4.5 These can be difficult and finely balanced questions of judgement. In difficult cases staff should consult line or senior management and/or legal advisers for guidance, and may seek guidance or a decision from the relevant Secretary of State."

40. A formal procedure must be followed prior to any acquisition or use as set out at §§4.6 to 4.7:

"4.6 Before a new dataset is loaded into an analytical system for use, staff in each Intelligence Service must consider the factors set out in paragraph 4.2 based on the information available to it at the time. Each Agency has a rigorous formal internal authorisation procedure which must be complied with, except in those cases where the acquisition is already authorised by a warrant or other legal authorisation issued by a Secretary of State.

4.7 Staff in each Intelligence Service must always complete the formal internal authorisation procedure before the dataset is loaded into an analytical system for use. The authorisation procedure involves an application to a senior manager designated for the purpose which is required to set out the following:

- *a description of the requested dataset, including details of the personal data requested, and any sensitive personal data;*

- *the operational and legal justification for acquisition and retention, including the purpose for which the dataset is required and the necessity and proportionality of the acquisition;*

- *an assessment of the level of intrusion into privacy;*

- *the extent of political, corporate, or reputational risk;"*

41. Thus, the need to consider the key matters set out at §4.2 of the BPD Handling Arrangements, and explained at §§4.3-4.3, is built into the formal authorisation procedure.

42. There is a requirement to consult the legal advisers of the relevant Intelligence Service "*on all new BPD acquisitions*" and to have "*confirmed the legality of the acquisition and its continued retention before authorisation to use the dataset is given.*" (§4.8)

43. A record of the application for authorisation must be kept:

"4.9 Once authorised, the completed application must be stored on a central record by the appropriate Intelligence Service's information governance/compliance team, which will include the date of approval. This record must also contain the date of acquisition of the relevant data, which should be the date used for the review process (for which see paragraph 7.1-7.5 below)."

Thus the reasons why the acquisition was authorised, including the key considerations set out at §4.2, are available to be reviewed or audited in the future.

Access/Use

44. The BPD Handling Arrangements emphasise the high priority that is put on data security and protective security standards, on confidentiality of data, and on preventing/disciplining misuse of such data:

"5.1 Each Intelligence Service attaches the highest priority to maintaining data security and protective security standards. Moreover, each Intelligence Service must establish handling procedures so as to ensure that the integrity and confidentiality of the information in the bulk personal dataset held is fully protected, and that there are adequate safeguards in place to minimise

the risk of any misuse of such data and, in the event that such misuse occurs, to ensure that appropriate disciplinary action is taken. In particular, each Intelligence Service must apply the following protective security measures:

- *Physical security to protect any premises where the information may be accessed;*

- *IT security to minimise the risk of unauthorised access to IT systems;*

- *A security vetting regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy."*

45. Specific, detailed measures are also set out 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:

"5.2 In relation to information in bulk personal datasets held, each Intelligence Service is obliged to put in place the following additional measures:

- *Access to the information contained within the bulk personal datasets must be strictly limited to those with an appropriate business requirement to use these data;*

- *Individuals must only access information within a bulk personal dataset if it is necessary for the performance of one of the statutory functions of the relevant Intelligence Service;*

- *If individuals access information within a bulk personal dataset with a view to subsequent disclosure of that information, they must only access the relevant information if such disclosure is necessary for the performance of the statutory functions of the relevant Intelligence Service, or for the additional limited purposes described in paragraph 3.1.4 above;*

- *Before accessing or disclosing information, individuals must also consider whether doing so would be proportionate (as described in paragraphs 4.4 above and 6.3 below). For instance, they must consider whether other, less intrusive methods can be used to achieve the desired outcome;*

- *Users must be trained on their professional and legal responsibilities, and refresher training and/or updated guidance must be provided when systems or policies are updated;*

- *A range of audit functions must be put in place: users should be made aware that their access to bulk personal datasets will be monitored and that they must always be able to justify their activity on the systems;*

- *Appropriate disciplinary action will be taken in the event of inappropriate*

behaviour being identified; and

- *Users must be warned, through the use of internal procedures and guidance, about the consequences of any unjustified access to data, which can include dismissal and prosecution."*

46. In addition, Intelligences Services are required to take specific measures "*to reduce the level of interference with privacy arising from the acquisition and use of bulk personal datasets*" (§5.3). Specifically:

"5.3 The Intelligence Services also take the following measures to reduce the level of interference with privacy arising from the acquisition and use of bulk personal datasets:

- *Data containing sensitive personal data (as defined in section 2 of the DPA) may be subject to further restrictions, including sensitive data fields not being acquired, sensitive fields being*

acquired but suppressed or deleted, or additional justification required to access sensitive data fields. In addition, the Intelligence Services may expand the list of sensitive data fields beyond those provided for in section 2 of the DPA to provide additional protection where appropriate.

- *Working practice seeks to minimise the number of results which are presented to analysts by framing queries in a proportionate way, although this varies in practice depending on the nature of the analytical query;*

- *If necessary, the Intelligence Services can - and will - limit access to specific data to a very limited number of analysts."*

Disclosure

47. The disclosure of BPD outside the Intelligence Service which holds it can only occur if certain conditions are complied with:

"6.1 Information in bulk personal datasets held by an Intelligence Service may only be disclosed to persons outside the relevant Service if the following conditions are met:

- *that the objective of the disclosure falls within the Service's statutory functions or is for the additional limited purposes set out in sections 2(2)(a) and 4(2)(a) of the ISA 1994 and section 2(2)(a) of the SSA 1989;*

- *that it is **necessary** to disclose the information in question in order to achieve that objective;*

- *that the disclosure is **proportionate** to the objective;*

- *that only as much of the information will be disclosed as is **necessary** to achieve that objective."*

48. Again, guidance is given to staff on the requirements of **necessity** and **proportionality**. This is in terms which are similar to those set out at §§4.3-4.4 in relation to acquisition, but with particular reference to disclosure:

*"**When will disclosure be necessary?***

*6.2 In order to meet the '**necessity**' requirement in relation to disclosure, staff must be satisfied that disclosure of the bulk personal dataset is 'really needed' for the purpose of discharging a statutory function of that Intelligence Service.*

The disclosure must also be "proportionate"

*6.3 The disclosure of the bulk personal dataset must also be **proportionate** to the purpose in question. In order to meet the 'proportionality' requirement, staff must be satisfied that the level of interference with the individual's right to privacy is justified by the benefit to the discharge of the Intelligence Service's statutory functions which is expected as a result of disclosing the data and the importance of the objective to be achieved. Staff must consider whether there is a reasonable alternative that will still meet the proposed objective - i.e. which involves less intrusion. For example, this could mean disclosure of individual pieces of data or of a subset of data rather than of the whole bulk personal dataset."*

49. Prior to any disclosure of BPD, staff must also take reasonable steps to ensure the intended recipient organisation "*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 with respect to such arrangements (§6.4). This applies to all

disclosure, including to other Agencies (§6.5), and whether disclosure is of an entire BPD, a subset of a BPD or an individual piece of data from a BPD (§6.6).

50. Disclosure of the whole or subset of a BPD is subject to internal authorisation procedures in addition to those that apply to an item of data (§6.7):

"The authorisation process requires an application to a senior manager designated for the purpose, describing the dataset it is proposed to disclose (in whole or in part) and setting out the operational and legal justification for the proposed disclosure along with the other information specified in paragraph 4.7, and whether any caveats or restrictions should be applied to the proposed disclosure. This is so that the senior manager can then consider the factors in paragraph 6.1, with operational, legal and policy advice taken as appropriate. In difficult cases, the relevant Intelligence Service may seek guidance or a decision from the Secretary of State."

Review of Retention and Deletion

51. The Intelligence Services are each required to keep the justification for continued retention and use of BPD under review, as set out at §§7.1-7.2:

"7.1 Each Intelligence Service must regularly review the operational and legal justification for its ***continued retention and use*** *of each bulk personal dataset. Where the continued retention of any such data no longer meets the tests of necessity and proportionality, all copies of it held within the relevant Intelligence Service must be deleted or destroyed.*

7.2 The retention and review process requires consideration of the following factors:

- *The operational and legal justification for continued retention, including its necessity and proportionality;*
- *Whether such information could be obtained elsewhere through less intrusive means;*
- *An assessment of the value and examples of use;*
- *Frequency of acquisition;*
- *The level of intrusion into privacy;*
- *The extent of political, corporate, or reputational risk;*
- *Whether any caveats or restrictions should be applied to continued retention."*

52. Thus, the justification for the retention of BPD, including whether it remains necessary and proportionate, the level of intrusion into privacy, and whether such information could be obtained elsewhere less intrusively, is not simply considered at the stages of acquisition, use or disclosure, but is kept under continuing review.

Other management controls

53. §§8.1-8.2 set out the requirement for each Agency to have an internal Review panel which scrutinises the acquisition, disclosure and retention of BPD:

"8.1 The acquisition, retention and disclosure of a bulk personal dataset is subject to scrutiny in each Intelligence Service by an internal Review Panel, whose function is to ensure that each bulk personal dataset has been properly acquired, that any disclosure is properly justified, that its retention remains necessary for the proper discharge of the relevant Service's statutory functions, and is proportionate to achieving that objective.

8.2 The Review Panel in each Intelligence Service meets at six-monthly intervals and are comprised of senior representatives from Information Governance/Compliance, Operational and Legal teams."

54. In addition, use of BPD is monitored by an audit team within each Agency:

"*8.3 Use of bulk personal data by staff is monitored by the relevant audit team in each Intelligence Service in order to detect misuse or identify activity that may give rise to security concerns. Any such identified activity initiates a formal investigation process in which legal, policy and HR (Human Resources) input will be requested where appropriate. Failure to provide a valid justification for a search may result in disciplinary action, which in the most serious cases could lead to dismissal and/or the possibility of prosecution*."

55. §8.4 notes that all reports on audit investigations are made available to the Intelligence Services Commissioner for scrutiny.

56. Staff within each Agency are also required to keep their senior leadership "*apprised as appropriate of the relevant Service's bulk personal data holdings and operations*." (§8.5)

Oversight

57. The BPD Handling Arrangements also set out provisions in relation to the oversight of BPD.

58. §9.1 concerns Ministerial oversight. Each of the Intelligence Services must report as appropriate on its BPD holdings and operations to the relevant Secretary of State.

59. §§10.1 to 10.4 address oversight by the Intelligence Services Commissioner:

"*10.1 The acquisition, use, retention and disclosure of bulk personal datasets by the Intelligence Services, and the management controls and safeguards against misuse they put in place, will be overseen by the Intelligence Services Commissioner on a regular six-monthly basis, or as may be otherwise agreed between the Commissioner and the relevant Intelligence Service, except where the oversight of such data already falls within the statutory remit of the Interception of Communications Commissioner.*

***Note**: The Prime Minister's section 59A RIPA direction was issued on 11 March 2015. Paragraph 3 of this makes it clear that the Commissioner's oversight extends not only to the practical operation of the Arrangements, but also to the adequacy of the Arrangements themselves.*

10.2 The Intelligence Services must ensure that they can demonstrate to the appropriate Commissioner that proper judgements have been made on the necessity and proportionality of acquisition, use, disclosure and retention of bulk personal datasets. In particular, the Intelligence Services should ensure that they can establish to the satisfaction of the appropriate Commissioner that their policies and procedures in this area (a) are sound and provide adequate safeguards against misuse and (b) are strictly complied with, including through the operation of adequate protective monitoring arrangements.

10.3 The Intelligence Services Commissioner also has oversight of controls to prevent and detect misuse of bulk personal data, as outlined in paragraph 8.3 and 8.4 above.

10.4 The Intelligence Services must provide to the appropriate Commissioner all such documents and information as the latter may require for the purpose of enabling him to exercise the oversight described in paragraph 10.1 and 10.2 above."

Internal BPD Handling Arrangements

60. In addition to the published BPD Handling Arrangements, GCHQ, MI5 and SIS have their own internal BPD Handling Arrangements, which were also in force from 4 November 2015. Gisted versions of these are in evidence. These reflect and supplement the published BPD Handling Arrangements. They are not separately set out in detail here.

GCHQ Compliance Guide

61. The relevant sections of the GCHQ Compliance Guide have been set out in evidence.

MI5 internal arrangements

62. MI5 continues to have internal guidance in addition to the BPD Handling Arrangements. In particular:

(a) In November 2015 MI5 updated its internal BPD Guidance (in evidence). That sits alongside the internal MI5 Handling Arrangements (also in evidence).

(b) An MI5-specific version of the SIA BPD Policy was used from November 2015, as produced in evidence.

(c) A new version of the Form for Retention began to be used in May **2016,** as produced in evidence.

SIS internal arrangements

63. SIS also continued to have additional internal arrangements, as disclosed in evidence.

BAILII: Copyright Policy | Disclaimers | Privacy Policy | Feedback | Donate to BAILII
URL: *http://www.bailii.org/uk/cases/UKIPTrib/2016/15_110-CH.html*