IN THE HIGH COURT OF JUSTICE **Claim No. CO/1052/2017**
QUEEN'S BENCH DIVISION
DIVISIONAL COURT

B E T W E E N:

THE QUEEN
on the application of
THE NATIONAL COUNCIL FOR CIVIL LIBERTIES
("LIBERTY")

Claimant

-and-

(1) SECRETARY OF STATE FOR THE HOME DEPARTMENT
(2) SECRETARY OF STATE FOR FOREIGN AND COMMOMWEALTH AFFAIRS

Defendants

-and-

NATIONAL UNION OF JOURNALISTS

Intervener

SKELETON ARGUMENT ON BEHALF OF THE DEFENDANTS
FOR HEARING ON 17 – 21 JUNE 2019

Suggested reading list: *as suggested by the Claimant, together with:*

- *the second w/s of James Dix ("Dix 2")* ***TB/2/661-684***
- *the Claimant's and Defendants' skeleton arguments*
- *10 December 2018 letter from the Defendants to the Investigatory Powers Commissioner* ***TB/2/345-350***
- *Lord Anderson QC's Report of the Bulk Powers Review* ***TB/4/473-676***
- *The judgments in Privacy International v SSFCO and ors* [2016] UKIPTrib15_110-CH. ***AB/2/17-19***
- *Greennet Limited and ors v SSFCO and ors* [2016] UKIPTrib14_85-CH ***AB/2/16***
- *Liberty and ors v SSFCO and ors* [2014] UKIPTrib 13_77-H (2015) HRLR 3 ***AB/2/12***
- *Weber and Saravia v Germany* (2008) 46 EHRR SE5 ***AB/2/6***

Bundle references

References to the trial bundles are in the form "TB/x/y", where "x" is the bundle number, and "y" the page number. References to the authorities are in the form "AB/x/y", where "x" is the bundle number, and "y" the tab number.

(I) INTRODUCTION AND SUMMARY OF THE CASE ADVANCED BY THE SECRETARIES OF STATE

1. This is the Defendants' ("Ds'") skeleton argument for the substantive hearing of those aspects of the Claimant's ("C's") challenge to the Investigatory Powers Act 2016 (the "**Act**") that are based on the European Convention on Human Rights ("**ECHR**" or the "**Convention**")[1]. It also addresses the matters raised by the National Union of Journalists ("NUJ") in its intervention.

2. The powers under challenge are of critical importance to, and are effective in securing, the protection of the public from a range of serious and sophisticated threats arising in the context of terrorism, hostile state activity and serious / organised crime: see, in this regard, Dix 1 at §§8-32 [**TB/2/410]**. These powers were also the subject of an unprecedented degree of pre-legislative scrutiny, including a comprehensive assessment of the utility of existing bulk powers (which have been consolidated in the Act) by the then Independent Reviewer of Terrorism Legislation, Lord Anderson QC, who concluded:

   "*Having observed practical demonstrations, questioned a large number of analysts and checked what they said against contemporaneous intelligence reports, neither I nor others on the Review team was left in any doubt as to the important part played by the existing bulk powers in identifying, understanding and averting threats of a national security and/or serious criminal nature, whether in Great Britain, Northern Ireland or further afield*"[2].

3. The Act provides an updated framework for the use of a range of investigatory powers to obtain communications and information about communications; and for the retention and examination of bulk personal datasets by the security and intelligence agencies. It consolidates powers previously contained in a variety of enactments, and provides an updated legal framework for their use. That framework contains more extensive statutory protections against unlawful interference with individuals' rights, including under Article 8 and 10 ECHR. The powers in the Act are also supported by a more far-reaching and detailed system of safeguards, contained in updated statutory Codes of Practice for the exercise of the powers in the Act, and new and strengthened systems of oversight, as well as detailed handling arrangements maintained by the agencies who regularly utilise the powers in the Act.

4. It is submitted that the powers in the Act, when considered alongside the statutory and non-statutory safeguards, strike an appropriate balance between security and individual privacy. Assessing that balance involves a series of legislative, security and political judgments. The leeway or respect to be accorded by the Court to those

[1] The Court has ordered, by paragraph 7 of its Order of 27 April 2018 [**TB/2/81**], that C's challenge based on EU law to those parts of the Act other than Part 4 be stayed until 14 days after the day on which a judgment of the CJEU is handed down in the preliminary reference made in *Privacy International v SSFCO and ors* [2016] UKIPTrib15_110-CH. The reference remains pending before the CJEU.
[2] See the Bulk Powers Review at §9.13, [**TB/4/598**] and Dix 1, §45 [**TB/2/425**]

judgments is significant, in the light of both the subject matter of the powers (which concern national security, the prevention of serious crime and ultimately the protection of the public) and the exhaustive process of democratic scrutiny to which the powers were subjected in Parliament: see e.g. *Bank Mellat v HM Treasury (no.2)* [2014] AC 700 at [21] [**AB/4/38**]; *Lord Carlile of Berriew v Home Secretary* [2015] AC 954 at [19]-[34] per Lord Sumption [**AB/4/41**]. While the ECtHR has treated the systematic storage of personal data as engaging Article 8 and requiring justification, it has also consistently recognised that public safety and the prevention and detection of crime will justify such interferences with Article 8 provided that sufficient and proportionate safeguards exist: see e.g. *R(Catt) v Association of Chief Police Officers of England, Wales and Northern Ireland* [2015] AC 1065, per Lord Sumption at [33] and the ECtHR cases there cited [**AB/4/43**].

5. Ds' basic submission is that taken individually and in combination those powers are both in accordance with the law, and proportionate to the pressing social needs that the Act seeks to secure.

6. C has served a Re-Amended Statement of Facts and Grounds ("SFG") running to 162 pages [**TB/2/7**], a 19-page Response to Summary Grounds of Resistance [**TB/2/321**] and a 72-page skeleton argument. The length of those documents should not obscure the basic position, which is as follows:

   (1) C's ECHR challenges closely mirror arguments which have already been considered in detail, and in many cases rejected in terms, by the Investigatory Powers Tribunal ("**IPT**") or the European Court of Human Rights ("**ECtHR**"), and indeed (in the context of C's EU law challenge to Part 4 of the Act) this Court. Ds' Detailed Grounds of Resistance ("**DGR**") set out at §3 the extensive, recent judicial consideration which has been given to the precursor regimes to the Act governing the exercise of surveillance powers. Arguments similar to those advanced by C in these proceedings have largely been dismissed on the basis that the "*in accordance with the law*" and "*necessity*" requirements for justification of interferences with Convention rights were met by the legal regimes under challenge. To the extent that previous challenges were dismissed, the position under the Act is *a fortiori*, since the current regime offers significantly greater safeguards and more extensive protection for individuals' rights.

   (2) To the limited extent that recent judicial consideration has found precursor surveillance powers were not ECHR compliant, this has been remedied by the scheme of the Act, taken as a whole (including amendments to the Act made by the Data Retention and Acquisition Regulations 2018 with effect from 1 November 2018).

   (3) In the limited ways in which C's challenge raises points that have not previously been the subject of detailed judicial consideration in Strasbourg and/or the domestic

courts, those points are wrong, and should be rejected by this Court, for the reasons given in the DGR and below.

7. C's ECHR claim is directed at five aspects of the Act, namely:

   (1) The equipment interference powers in Part 6 Chapter 3 and Part 5 of the Act, which C describes as powers to engage in "bulk and thematic hacking[3]". This skeleton argument uses the statutory language.

   (2) The provisions relating to bulk personal datasets ("**BPD**") in Part 7 of the Act. C wrongly characterises these provisions as if they created a free-standing power to obtain BPD, but that is wrong for the reasons explained below.

   (3) The bulk interception powers in Part 6 Chapter 1 of the Act.

   (4) The acquisition and retention powers in respect of communications data in Part 6 Chapter 2 and Parts 3 – 4 of the Act.

   (5) The protections in and under the Act for journalists and lawyer-client communications.

8. As summarised at §4 of its skeleton argument, C's essential case is that the powers are unlawful because, in its submission, they are (i) too wide (in the case of the equipment interference powers in Part 6 Chapter 3 and Part 5, the BPD provisions in Part 7, and the bulk interception and acquisition powers in Part 6 Chapters 1 and 2) and because (ii) taken together, the powers lack sufficient safeguards to comply with C's characterisation of the 'minimum requirements' laid down in the Strasbourg jurisprudence. C also raises specific arguments in relation to journalistic materials and lawyer-client materials, and contends that the continued operation of Part 1 Chapter 2 of the Regulation of Investigatory Powers Act 2000 ("**RIPA**") in relation to the acquisition of communications data is not in accordance with the law[4].

9. Taking those points in turn, and leaving aside the observations made above about prior judicial rejection of equivalent arguments to those now advanced by C, Ds' position can be summarised as follows:

   (1) In relation to the equipment interference powers in Part 6 Chapter 3 and Part 5, and the BPD provisions in Part 7, these are not "*too wide*" as C alleges. They fully comply

[3] C does not challenge Part 5 insofar as it relates only to a targeted equipment warrant relating to equipment belonging to, used by or in the possession of a particular person or organization under s.101(1)(a) of the Act.

[4] C's challenge to certain of the powers in the Act on Article 14 discrimination grounds is no longer pursued: see Reply to Summary Grounds of Resistance, para 30 [**TB/2/336**]

with the requirements of the Convention case law. C's allegations as to the breadth of these powers are redolent of its contention that the communications data retention powers in Part 4 of the Act contravened EU law because of their allegedly "*general and indiscriminate*" nature. That contention was rejected by the Divisional Court in its judgment of 27 April 2018[5] (the "**April 2018 Divisional Court Judgment**"): see [118]-[138][6] [**AB/4/45**]. The Divisional Court's conclusion at [137] was that the "*overall amount of data which is retained under Part 4 of the 2016 Act will be the outcome of applying a statutory regime which requires the contents of each retention notice to be necessary and proportionate*" and that the "*rigorous approach required by the 2016 Act will be reinforced when the provisions for judicial scrutiny are brought into force*" (as has now occurred). This observation applies, *mutatis mutandis*, with equal force to other provisions that are impugned in these proceedings, and the fact that considerations of necessity and proportionality permeate the various powers in the Act is plainly of relevance to C's broad claim under the Convention just as it was to the narrower EU law-based challenge to Part 4 of the Act.

(2) As to the bulk interception and acquisition powers in Part 6 Chapter 1 and Chapter 2, C accepts that it cannot presently maintain the submission that these powers are too wide in the light of the decision of the First Section of the ECtHR in *Big Brother Watch and ors v United Kingdom* apps. 58170/13, 62322/14 and 24960/15 ("***BBW***")[7] [**AB/2/20**].

(3) As to safeguards, the Act is infused with concern for the protection of privacy and sensitive information, and contains a variety of statutory safeguards that are underpinned by Codes of Practice and internal handling arrangements maintained by the relevant agencies. Many of these safeguards are new innovations of the Act.

(4) In relation to the treatment of journalistic materials, the applicable powers in the Act, and the associated Codes of Practice, together contain a variety of strong safeguards for such material that fully satisfy the requirements of Articles 8 and 10 ECHR.

(5) C's application for a declaration that Part 1 Chapter 2 of RIPA is not in accordance with the law is unpleaded, and Ds object to its late introduction in a skeleton argument. In any event, and as explained in detail in the witness statements that they have adduced in these proceedings, Ds have acted responsibly, and as promptly as has been practicable, in bringing forward substantial legislative and operational changes to reflect the Divisional Court's Order on EU law issues in April

[5] [2018] EWHC 975 (Admin)

[6] See in particular the eight considerations set out at [127]-[136] of the April 2018 Divisional Court Judgment.

[7] App No 58170/13, 13 September 2018, First Section. C says that it wishes to reserve consideration of this point until the Grand Chamber, to which the First section's decision in *BBW* has now been referred, gives judgment on the referral. Subject to the Court's preference as to how this matter ought to be dealt with, Ds will respond to any submissions made by C at that stage.

2018. The continued operation of Part 1 Chapter 2 RIPA as a temporary reserve power is consistent with the Divisional Court's Order and reasons. In the circumstances, there is no good purpose to be served in considering and ruling on the compatibility of the provisions of Part 1 Chapter 2 RIPA with the Convention.

10. At §§5-7 of its skeleton argument, C makes certain remarks on questions of procedure. The points raised have largely now been overtaken by the directions given at the case management hearing on 20 May 2019, but insofar as they remain "live":

(1) C refers (skeleton, §5) to the Government's proposal to introduce a new scheme for the approval of the use of the "non-content" data of people in the British Islands, as referred to in the Government's Written Observations for the Grand Chamber of the ECtHR in *BBW*. The position is as explained in Dix 2 at §§45-56 [**TB/2/679**], and in §§18-25 of Ds' skeleton argument for the case management hearing on 20 May 2019[8] [**TB/2/751**]. In particular, the Government was able to confirm in its Observations to the Grand Chamber on 2 May 2019 that it intended to amend relevant Codes[9] to provide for a "thematic" certification regime, following a Cabinet decision to that effect on 1 May 2019. In the interim, the Intelligence Services have been working with the Investigatory Powers Commissioner (**"IPC"**) to strengthen his oversight of selectors used to effect selection for examination, and of the examination of secondary data relating to persons believed to be in the British Islands, under his existing powers[10].

(2) C refers to Ds' requests for a closed material procedure ("**CMP**") under s. 6 of the Justice and Security Act 2013, concerning compliance risks identified by MI5, and subsequently considered by the IPC, in relation to certain MI5 technology environments for the storage and analysis of data: see Ds' OPEN application dated 9 May 2019 [**TB/5/733**]. The subject matter of the CMP application concerns a detailed operational issue that is at the most of marginal relevance to the Convention challenge to the provisions of the Act, and has been properly brought to C's and the Court's attention under the continuing duty of candour. The Court has now ordered a procedure by which a gist of the relevant information can be prepared (with the input of Special Advocates and the Court) and, if it can be agreed, provided to C in advance of the June hearing. It is hoped that this process will obviate the need for a determination of the CMP application, and will minimise disruption to preparations for the June hearing.

[8] See further the letter to the IPC dated 10 December 2018 [**TB/2/345**], which was annexed to the Defendants' skeleton argument for the case management hearing that took place on 20 May 2019.
[9] It is intended that the "thematic" certification regime should apply to the exercise of bulk interception powers under Chapter 1 Part 6 of the Act, and to the exercise of bulk equipment interference powers under Chapter 3 Part 6 of the Act. Accordingly, the relevant Codes will be the Interception of Communications Code and the Equipment Interference Code.
[10] See Ds' skeleton argument for the case management hearing, §§20-22, **TB/2/751**.

11. Next, C raises three overarching issues of substance (skeleton, §§8-13).

12. First, C refers at §8 to what it describes as the "*startling*" observation at §78(7) of the DGR to the effect that "*[a]ny meaningful intrusion into privacy rights only occurs at the stage when content or secondary data is selected for examination*". C says that this is "*contrary to decades of ECtHR authority, which hold that the existence of a secret surveillance regime in itself interferes with private life*".

13. Ds have never suggested that the bulk interception of, or acquisition of, data under a regime such as that set out in the Act involves no interference with Convention rights. On the contrary, Ds accept that there is a technical interference with Article 8(1) ECHR when data is intercepted or retained (as the case may be) under the various impugned powers in the Act. The important point, however, is that any meaningful interference does not occur until a later stage, when an individual's communications data, or the content of an individual's communications, are selected for potential examination, if not actually examined by a human being. The fact that material is held for a short period of time in a 'soup' of data before being discarded, without any possibility that it may be selected for potential examination, let alone examined, cannot sensibly be regarded as a meaningful – still less, serious - interference with the right to privacy. This analysis and distinction is supported by *BBW*. In relation to the bulk interception powers as formerly set out in section 8(4) of RIPA, the ECtHR accepted that there will be a "*significantly greater*" interference (calling for "*more rigorous safeguards*") with Article 8 ECHR when material is selected for examination or actually examined by an analyst, even if earlier stages (the interception of 'bearers' and the automatic filtering and discarding by computer of the intercepted material) involve a technical interference with Article 8: see [329] and [338] of *BBW* (**AB/2/20**). The same point applies, *mutatis mutandis*, to all the bulk powers under the Act that are challenged by C in these proceedings.

14. The suggestion at §9(2) of C's skeleton argument that the mere interception, storage and filtering[11] of information involves a "*significant*" interference with privacy also ignores the periods of time for which individuals' information can be retained. Taking the bulk interception powers under Part 6 Chapter 1 of the Act by way of example, (i) s. 150(5) of the Act requires the Secretary of State to ensure in relation to every bulk interception warrant that arrangements exist to ensure that any copy made of material obtained under the warrant (if not destroyed earlier) is destroyed as soon as there are no longer any relevant grounds for retaining it; and (ii) the Interception Code requires intercepting authorities to "*specify maximum retention periods for different categories of data which reflect its nature and intrusiveness*", which should normally be no longer than

[11] C also refers at §9(2) of its skeleton to "searching and collating information about individuals". Where this involves selection for examination, Ds accept (and always have accepted) that there is a meaningful interference with privacy rights: that is precisely why rigorous safeguards apply at that stage. As further explained below, C's terminology here seems to reflect a misunderstanding of what "selection for examination" consists in.

2 years, and should be agreed with the IPC[12]. Further, as a matter of operational reality, the vast bulk of intercepted communications (which are themselves collected from only a small percentage of Internet 'bearers', selected as being the most likely to carry external communications of intelligence value) will be automatically discarded in near-real time, or within a short period of time following the application of 'selectors': see the description at *BBW*, [329], which aptly describes the process of bulk interception under the Act as well as under the predecessor provision in s. 8(4) of RIPA (cf. Dix 2, §22, **TB/2/668**). Similar statutory and operational limits apply to all the impugned powers. The powers therefore stand in stark contrast to the facts of cases such as *Catt* [2015] AC 1065 (**AB/4/43**), which concerned the potentially indefinite retention of information by electronic data about individuals by the police (although even in that case, Lord Sumption (giving the leading judgment) considered that the relevant interference with Article 8 was "*minor*": [26]).

15. C's contention at §9(3) of its skeleton argument that it is "*dangerous and artificial*" for Ds to suggest that interferences with privacy occurring before the point of selection for examination are less significant rests on a misunderstanding of what selection for examination entails. The sorts of processes to which C refers in §9(3)(b), insofar as they determine the content of information that analysts are potentially able to examine, themselves constitute selection for examination. So under the Act, they would need to be justified as necessary and proportionate, and would be subject to the extensive internal and external oversight that is a feature of the Act and its associated statutory codes and internal handling arrangements[13].

16. In the circumstances, C is quite wrong to characterise the assertion at DGR §78(7) as a "*false premise for much of the Defendants' argument*" and that "*[o]nce it is recognised, many of the assertions of sufficient safeguards fall away*". On the contrary, it is essential to a properly-informed consideration of proportionality in this case to appreciate that the overwhelming majority of information that is retained or acquired pursuant to the impugned bulk powers will never be selected for examination, let alone actually examined by a human being, and where selection for examination (properly understood) does occur, it will be subject to all the myriad safeguards in the Act.

17. By way of a **second** overarching issue of substance, C contends (skeleton, §§10-11) that the DGR fail to deal separately with each of the impugned powers in the Act, and fail to consider the cumulative impact of the powers at issue. The thematic approach taken in the DGR is simply a reflection of the fact that C's SFG advances essentially the same complaints under the Convention in relation to each of the powers concerned. Further, the cumulative impact of the impugned powers depends on the detailed system of safeguards under the Act and the associated regime, which are extensively described

[12] See the Interception Code, §9.24 [**AB/3/24**]. This includes both communications and communications data.

[13] See further Dix 2, §§21-22 [**TB/2/668**], responding to an identical misconception in Danezis 2 at §§43-44 [**TB/2/526**].

in both the DGR and Ds' witness evidence. If the individual powers are each justified for ECHR purposes, as Ds contend, then it is hard to see how their cumulative impact could give rise to a violation of the Convention. That is particularly so, because the statutory premise for the use of powers under the Act is that both the *type* of surveillance power used in any particular case, and the *way* in which it is used, will be chosen on the basis that they involve the least possible intrusion into individuals' privacy rights[14]. In that regard, it is also not accepted that equipment interference (which C refers to as "bulk hacking") is a uniquely invasive power: but even if that were the case, the relevant question for the Court is whether the applicable safeguards are adequate to ensure Convention compliance (which they plainly are).

18. As to the two specific points raised at §11 of C's skeleton argument:

(1) It is correct that the equipment interference power provides an important additional tool (although not a new power) to tackle sophisticated forms of terrorism, hostile state activity and serious or organised crime: see e.g. Dix 2, §7 [**TB/2/663**]. It does not follow from the fact that different powers may be needed for different purposes and in different situations that any particular power is unjustifiable, or that any particular power requires a different variety of safeguards. Again, the question for the Court is simply whether safeguards applicable to the impugned powers are adequate.

(2) C's point concerning s. 225 of Part 7 is, in fact, fully answered at DGR §79 [**TB/2/382]**. Part 7 of the Act does not create a new power to obtain information at all. In effect, it constitutes a new statutory scheme of safeguards in respect of BPD that did not exist previously. C simply misses the point that the designation of information as a BPD under Part 7 does not mean that no safeguards apply. Part 7 contains a range of robust safeguards of its own, including prohibitions on the disapplication of certain requirements under other Parts of the Act: see ss. 200, 202, 203, 206, 207, 212, 220, 221, 224. The justification for this approach is clearly explained at Dix 1 §243 (**TB/2/486**): in short, the designation of material as BPD enables the Ds (subject to Judicial Commissioner approval) to design appropriate retention/examination safeguards depending on the nature of the material, rather than the nature of the power used to obtain it. Part 7 is thus an important additional bulwark against unjustified interferences with privacy, rather than constituting some new and invasive power that cannot be justified.

19. The **third** and final overarching issue raised by C (skeleton, §§12-13) concerns the provisions relating to bulk interception in Part 6 Chapter 1 of the Act. Contrary to C's submission, those provisions (in the context of the safeguards applicable under the Act as a whole) do indeed remedy the defect identified by the First Section in *BBW* at [387]

[14] See s.2 of the Act.

(**AB/2/20**) in relation to the predecessor statutory provisions on bulk interception in Part 1 RIPA:

(1) C's points about "*operational purpose*" at §12(1)(a)(i) and (ii) are incorrect. Pursuant to s. 142(7) of the Act, the Secretary of State may only approve a bulk interception warrant if satisfied that the operational purpose is "*specified in a greater level of detail*" than the general purposes for which such a warrant may be obtained under s. 138(1)(b) or (2). That requirement is reinforced by relevant provisions of the Interception Code and by the requirement for a central list of operational purposes to be maintained, regularly shared with the ISC, and reviewed by the Prime Minister (see DGR, §§72(1) - (4), [**TB/2/376**]). These are plainly significant safeguards. They are bolstered by the underlying requirement for Judicial Commissioner approval of bulk interception warrants (s. 140) and go well beyond the safeguards in the system that was found (in certain limited respects) to be defective in *BBW*.

(2) As to §12(1)(b) of C's skeleton:

a. Any application for a warrant will be directed at a particular telecommunications operator, and will need to explain why it is necessary to intercept communications on bearers owned, operated by or accessible to that operator: see the Interception Code §6.20 [**AB/3/24**]. A Judicial Commissioner will see the same information put before the Secretary of State: Code, §6.28. As to the ongoing choice of bearers to intercept from among the particular bearers used by an operator, this is a dynamic process which it would be wholly impracticable to expect a Judicial Commissioner to micro-manage. See Code, §6.10[15].

b. The choice of bearers, and the choice of selectors/search terms to effect selection for examination, is a matter which lies directly within the oversight functions of the IPC, whose supervisory powers include "end to end" audit of the whole process of dealing with intercept material, from initial interception to destruction[16].

(3) As to §12(2) of C's skeleton argument, C relies on certain concluding remarks of the First Section in *BBW* at [387] [**AB/2/20**] in relation to "*the absence of any real safeguards applicable to the selection of related communications data for examination*".

[15] *"When conducting bulk interception, an intercepting authority must use its knowledge of the way in which international communications are routed, combined with regular surveys of relevant communications links, to identify those individual communications links that are most likely to contain overseas-related communications, which will be relevant to the operational purposes specified on a warrant. This is likely to be a dynamic process due to regular fluctuations in the way data routes across the internet."*

[16] This is a point explicitly made in relation to selectors in Ds' letter of 10 December 2018 to the IPC (see **TB/2/345**), which records Ds' commitment to work with the IPC to enhance his oversight of selectors.

Those remarks need to be read in the context of the specific and limited vice identified by the First Section at [355]-[357] of *BBW*, namely that the exemption of related communications data from the safeguards identified in section 16 of RIPA is not limited to the extent necessary to determine whether an individual is, for the time being, in the British Islands (the intelligence importance of which the First Section recognised at [353]). It does not follow from those remarks that the safeguards for content and non-content data must be the same: that would be impracticable and would prejudice national security, for the reasons given in Dix 2 at §§49-53 [**TB/2/680**]. That said, as referred to above and explained in Dix 2 at §§54-56, the Government is now taking steps (in light of *BBW*) to ensure that where non-content data obtained pursuant to Part 6 Chapter 1 or 3 of the Act is to be selected for examination by reference to a factor referable to a person who is believed to be in the British Islands, that must be certified as necessary and proportionate by the Secretary of State on a specific thematic basis. When that is considered in addition to the range of safeguards that apply under the Act to bulk interception warrants authorising the obtaining of 'secondary data' (i.e. non-content data), it cannot be said that the overall regime relating to the obtaining of such data is insufficiently foreseeable or proportionate for the purposes of Articles 8 or 10.

(II) BACKGROUND TO THE ACT AND OVERVIEW OF ITS KEY PROVISIONS

The introduction of the Act and current status of the relevant provisions

20. A detailed exposition of the background to the Act and the exceptionally extensive process of scrutiny that resulted in its enactment is set out in Dix 1 at §§33-47 [**TB/2/421**]. The Court is asked to read Mr Dix's account in full.

21. As set out at §12 of the DGR, the impugned provisions of the Act have all been in force since 5 February 2019 (or earlier), although for reasons explained in the witness statement of Katie Gardiner[17] [**TB/2/489**], certain public authorities have not yet transitioned to utilising the regime in Part 3 of the Act, which involves requests for authorisation to access retained communications data being made to the new Office for Communications Data Authorisation ("**OCDA**"). Accordingly, for the limited purpose of providing a statutory basis for certain public authorities, where necessary, to continue to access retained communications data pending their transition to the new regime, RIPA Part 1 Chapter 2 remains on the statute book. This issue is considered further below in the context of C's (unpleaded) challenge to RIPA Part 1 Chapter 2.

The array of privacy safeguards in and under the Act – in outline

22. The Act itself contains a variety of statutory safeguards for the protection of privacy and sensitive information, as non-exhaustively summarised at DGR §§13-25 [**TB/2/360**], and further described at Dix 1 §§61-75 [**TB/2/431**]. These safeguards impose limits on the exercise of powers to obtain communications and information about communications, and to retain or retain and examine bulk personal datasets, which reflect concern for privacy and protection of sensitive communications.

23. They go substantially beyond those contained in previous enactments. A large number of them are new and are important. The new safeguards in the Act are set out (non-exhaustively) at DGR §16 [**TB/2/361**]. In outline, they include:

    (1) Judicial or other independent authorisation for the exercise of key powers under the Act, including judicial approval of warrants;
    (2) New statutory provisions increasing the level of detail required to be included in relevant warrants for the exercise of bulk powers;
    (3) New and powerful statutory safeguards for journalistic material;
    (4) New and powerful statutory safeguards for legally privileged material;
    (5) New statutory safeguards for Parliamentarians' communications;

[17] Ms Gardiner is the Head of the National Communications Data Service within the Office for Security and Counter Terrorism in the Home Office.

(6) New specific statutory safeguards for disclosure of material overseas;
(7) New statutory safeguards for health records held as part of a BPD;
(8) New safeguards in relation to the retention, or retention and examination, of bulk personal datasets containing protected data or a substantial proportion of sensitive personal data; and
(9) New offences related to the deliberate breach of safeguards imposed upon the selection of material for examination, and the unlawful obtaining of communications data.

24. Specific features of the new legal regime introduced by the Act which provide for protection of privacy include the following:

(1) Under s.2 of the Act, any public authority deciding whether to apply for, provide, modify, renew, approve or cancel a warrant, authorisation or notice in respect of any of the powers in the Act challenged by C must have regard to the "*general duties*" in relation to privacy in in s2(2) of the Act[18];

(2) The safeguards in the Act are further fleshed out and strengthened in the relevant statutory Codes (see Dix 1, §§76-81, **TB/2/436**);

(3) Part 8 of the Act ("*oversight arrangements")* significantly strengthens, updates and improves the machinery for the supervision of investigatory powers, including the creation, under s. 227 of the Act, of the new office of the IPC[19]. The IPC has a wide variety of oversight functions under s. 229 of the Act, including oversight of the exercise by public authorities of all the powers challenged by C in these proceedings. The IPC is supported by the Office of the Investigatory Powers Commissioner ("IPCO"), including a Deputy IPC (Sir John Goldring), 14 other Judicial Commissioners, and almost 50 official staff. In addition, section 246 of the Act provides for a new Technology Advisory Panel, to advise the IPC and Secretary of State on the impact of changing technology on the exercise of investigatory powers (see Dix 1, §§106-120);

[18] Under s.2 of the Act ("General duties in relation to privacy"), any public authority deciding whether to apply for, provide, modify, renew, approve or cancel a warrant, authorisation or notice in respect of any of the powers in the Act challenged by the Claimant must have regard to the following (see s.2(2)):
"*(a) whether what is sought to be achieved by the warrant, authorisation or notice could reasonably be achieved by other less intrusive means,*
(b) whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant, authorisation or notice is higher because of the particular sensitivity of that information,
(c) the public interest in the integrity and security of telecommunications systems and postal services, and
(d) any other aspects of the public interest in the protection of privacy."

[19] The Investigatory Powers Commissioner has replaced a variety of other offices, which are abolished, viz the Interception of Communications Commissioner; the Intelligence Services Commissioner; the Chief Surveillance Commissioner, and other Surveillance Commissioners; and the Scottish Chief Surveillance Commissioner and other Scottish Surveillance Commissioners. See s.240 of the Act.

(4) A 'double-lock' system has been introduced, whereby requests to use certain more intrusive powers under the Act must be authorised as necessary and proportionate not only by the Secretary of State, Scottish Minister or law enforcement chief (as the case may be) but also by an independent Judicial Commissioner. Bulk warrants subject to this double-lock procedure must also specify more detailed 'operational purposes' for which material acquired under such warrants may be selected for examination (see Dix 1, §§62-75, 12 and §§68-75, [**TB/2/432**]). The double-lock system was recently cited approvingly by the UN Special Rapporteur on the Right to Privacy as "*one of the most significant new safeguards introduced by the IPA*" (see DGR at §21 [**TB/2/364**]);

(5) The Intelligence and Security Committee of Parliament, chaired by Rt Hon Dominic Grieve QC MP, retains statutory responsibility for oversight of the security and intelligence agencies (see Dix 1, §§121-123, [**TB/2/448**]);

(6) The Act makes important changes to the jurisdiction of the Investigatory Powers Tribunal ("**IPT**"), including provision for a right of appeal to the Court of Appeal / Court of Session, brought into force on 31 December 2018[20]. In *BBW*, the ECtHR accepted that the IPT provides an effective remedy in relation to particular instances of unlawful interference with privacy (see generally Dix 1, §§124-127 [**TB/2/449**]).

(7) In relation to communications data specifically, OCDA, exercising functions delegated to it by the IPC under Part 3 of the Act as amended by the Data Retention and Acquisition Regulations 2018, will ensure that the UK's arrangements in relation to the retention and acquisition of communications data comply with EU law (see generally Dix 1, §§128-135 [**TB/2/450**]; and Gardiner 1 [**TB/2/489**]).

(8) The Act and the associated Codes of Practice also contain specific provision relating to warrants that are directed at legally privileged materials and journalistic sources (see Dix 1, §§82-105 [**TB/2/438**] and Dix 2, §§31-36 [**TB/2/672**]).

25. It can therefore be seen at the outset that, taken as a whole, the Act and the associated regime is pervaded by safeguards for the protection of individual privacy and freedom

[20] Section 242 of the Act introduces a new section 67A RIPA, providing for an appeal on a point of law to the Court of Appeal or Court of Session against certain decisions of the IPT. Section 242 was brought into force on 31 December 2018 by the Investigatory Powers Act (Commencement no. 10 and Transitional Provision) Regulations 2018/1397. The Supreme Court in *R(Privacy International) v Investigatory Powers Tribunal* [2019] UKSC 22 (15 May 2019) [**AB/4/46**] has very recently held that the ouster clause in s.67(8) RIPA, stating that determinations, awards and other decisions of the IPT should not be subject to appeal or liable to be questioned in any court, did not exclude the supervisory jurisdiction of the High Court on judicial review to quash a judgment of the IPT for error of law. So in fact, even prior to the changes effected by the Act, the Courts have now held that decisions of the IPT were not immune from challenge.

of expression. C's Article 8 / 10 ECHR complaints need to be considered in the light of that essential context.

(III) LEGAL FRAMEWORK

26. Section B of C's skeleton argument contains a detailed exposition of the legal framework for Convention claims in respect of investigatory powers. Some of it is common ground (cf. Section III of the DGR) but there are a number of important differences between the parties.

(1) Existence of an interference (C's skeleton, §§23-25)

27. It is common ground that the exercise of the impugned powers interferes with Article 8 and 10 rights. However, the extent of any interference depends on the precise stage of the exercise of the powers relating to the information concerned. Thus:

    (1) Where individual data is briefly held in a "soup" of bulk data and then discarded pursuant to an automated process in which it is never selected for potential examination by a human being (see Dix 2, §22, [**TB/2/668**]), any interference with privacy is minimal and consequently requires less by way of justification. In contrast, more will be required in order to justify the selection of material for examination, and any actual examination of material by an intelligence analyst.

    (2) Similarly, and as a general rule, the examination of communications data will be less intrusive than the examination of the content of communications, a point that has long been recognised by the ECtHR (see *Malone v. UK* (1984) 7 EHRR 14 at [84] [**AB/5/49**], *Uzun v Germany* app. no. 35623/05 at [52] [**AB/5/63**], *Ben Faiza v France* app. no. 31446/12 at [74] [**AB/5/69**]) and recently re-affirmed in *BBW* itself at [350] [**AB/2/20**]. This is not an absolute rule (there will be circumstances in which communications data may reveal sensitive information about an individual), but it is nevertheless an important contextual point when considering the justification and safeguards applicable to the various powers relating to content *vs.* those relating to communications data.

28. It is not common ground that the mere existence of all the impugned powers interferes with Convention rights in and of itself. Ds' position is that this is the case only for the "bulk" powers under challenge. However, no point is taken on this issue for the purposes of this challenge (only)[21].

[21] C's skeleton asserts at §§24 that "*the ECtHR has repeatedly held that the existence of a secret surveillance regime is a significant interference*" with Articles 8 and 10. That is a simplistic summary of the case law. The position under the ECHR, as explained by the Grand Chamber in *Zakharov v Russia* (2016) 63 EHRR 17 [**AB/2/13**], is that an applicant can claim before the ECtHR to be the victim of a violation occasioned

(2) **Accessibility / foreseeability (C's skeleton, §§26-37)**

29. It is common ground that:

(1) In order to be justified, a given interference with Convention rights must be both in accordance with the law and correspond to a pressing social need (and be proportionate to the pursuit of that need).

(2) At least in the context of investigatory powers, the "*in accordance with the law*" requirement refers not only to the need for a measure to have "*some basis in domestic law*" but also the quality of the domestic law in question, which must be "*accessible to the person concerned, who must, moreover, be able to foresee its consequences for him*": see *Weber and Saravia v Germany* (2008) 46 EHRR SE5 [**AB/2/6**].

(3) In assessing compliance with these requirements, statutory codes of practice and other non-legislative materials such as internal handling arrangements are relevant (see DGR §§33-34 [**TB/2/366**]; C's skeleton, §37).

30. It is important to note, as recognised in *BBW* at §326 [**AB/2/20**], that there is no obligation on States to make public all the details of the operation of a secret surveillance regime, provided that sufficient information is available in the public domain. In this context, it is inevitable, and permissible, that so-called 'below the waterline' arrangements will exist. Further, the existence of detailed internal handling arrangements, supervised by the IPC, is material to whether there exist sufficient safeguards against abuse, as the IPT rightly held in *Liberty and ors v SSFCO and ors* [2014] UKIPTrib 13_77-H, [2015] HRLR 2 ("*Liberty IPT*") at [120]-[121] [**AB/2/12**]. The fact that such arrangements exist, sufficiently signalled in public documents, is relevant to the sufficiency of oversight under the Act. In assessing compatibility with the Convention, regard must be had to the actual operation of a surveillance system, including the checks and balances on the

---

by the mere existence of secret surveillance measures if the two conditions set out at [171] of *Zakharov* are satisfied, those being (i) whether the applicant can possibly be affected by the scope of the legislation permitting secret surveillance measures, either because he or she belongs to a group of persons targeted by the legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted; and (ii) the availability of remedies at national level i.e. whether the domestic system affords an effective remedy to a person who suspects that he or she was subjected to secret surveillance. Point (ii) is, of course, an issue relevant to the ECtHR rather than the domestic courts. In this case:

(1) Ds accept that the nature of the bulk powers in the Act is such that users of communications services such as C can claim to be "*directly affected*" by them for the purposes of the *Zakharov* test; and

(2) No point is taken by Ds on whether C can claim to be the victim of a violation occasioned by the mere existence of the non-bulk powers under challenge, because it is accepted that it would be appropriate for this Court to deal with C's challenge in the round. That should not be taken as a concession that the mere existence of those powers "*directly affects all users of communication services*".

exercise of power and the existence or absence of any evidence of actual abuse: see *Ekimdzhiev v Bulgaria* app. 62540/00, 30 January 2008, at [92] [**AB/5/57**], *BBW* at [320].

31. The foreseeability requirement must always be read subject to the important and well-established principle that it 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: see *Malone* (supra) at [67] [**AB/5/49**]; *Leander v. Sweden* (1987) 9 EHRR 433, at [51] [**AB/5/50**]; *Weber* (supra) at [93] [**AB/2/6**]; *Zakharov v Russia* (2016) 63 EHRR 17 at [229] [**AB/2/13**]; and *BBW* at [306] [**AB/2/20**]. This critical point is not referred to in C's summary of the applicable legal framework.

32. There is also an important point of difference between the parties as to the requirement of foreseeability:

(1) It is common ground that, when considering whether domestic law providing for the interception of communications is sufficiently foreseeable, compliance with the six minimum safeguards known as the "*Weber*" criteria[22], which were recapitulated in *BBW* at [307], must be considered. Ds accept that the same minimum safeguards apply *mutatis mutandis* to the obtaining of the content of communications via surveillance methods analogous to interception (e.g. via equipment interference[23]): see DGR, §§30-31 [**TB/2/366**].

(2) However, Ds <u>dispute</u> the application of the *Weber* criteria in the context of communications data (as opposed to the content of communications), contrary to the suggestion at §36 of C's skeleton argument. The ECtHR has never applied the *Weber* criteria in the context of communications data. That is unsurprising given the generally less intrusive nature of the covert acquisition of such data (see above). On the contrary, the ECtHR has regularly reaffirmed the difference between obtaining the content of communications and other, less intrusive, forms of surveillance: see *BBW* at [350] and the jurisprudence there cited. In *BBW* itself, the First Section did not apply the *Weber* criteria when considering the adequacy of the safeguards pertaining to the interception of "related communications data" (albeit on the basis that it did not consider it necessary to decide the point): see [352] of *BBW*. It would not be for this Court to apply the *Weber* criteria in a context where the ECtHR has chosen not to do so. The principles in *R ota Ullah v Special Adjudicator* [2004] 2 AC 323 at [20] [**AB/4/30**],

[22] See *Weber* (supra) at [95]:
"In its case law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed…"
[23] That the *Weber* criteria applied in the context of computer network exploitation (a form of equipment interference) was common ground in *Greennet* [2016] UKIP Trib 15_85-CH at §67 [**AB/2/16**].

R ota Al-Skeini v Secretary of State for Defence [2008] 1 AC 153[24] [**AB/4/32**] and *Kennedy v Information Commissioner* [2015] AC 455[25] [**AB/4/42**] apply: the Court should not construe the Convention too generously in favour of an applicant, by going beyond principles clearly and consistently established in the Strasbourg case law.

(3) That is quite aside from the separate issue whether the *Weber* criteria (which relate to interception) can sensibly be applied in the context of the retention or acquisition of communications data, as opposed to the interception of communications.

(4) Further, as noted in the UK Government's Written Observations for the Grand Chamber in *BBW* at §§145-146 [**TB/2/574**] with regard to bulk interception under a s.8(4) RIPA warrant, applying exactly the same safeguards to the selection for examination/examination of intercepted communication data as to the content of intercepted communications would be thoroughly impracticable, and injurious to the protection of the public. The same point applies with equal force to material obtained pursuant to a bulk warrant under Part 6 Chapter 1 of the Act or Part 6 Chapter 3 of the Act[26]: see further Dix 2, §§49-53 [**TB/2/680**].

33. In Ds' submission, the relevant question when considering whether domestic law relating to the interception, acquisition or retention of communications data is sufficiently foreseeable is simply the general question of whether "*the law is sufficiently foreseeable to minimise the risk of abuses of power*" (cf. *BBW* at [326]), subject always to the caveat that the individual should not be enabled thereby to foresee when the authorities are likely to obtain, access and use his communications data so that he can adapt his conduct (see §31 above).

34. That said, even if the *Weber* criteria were (to the extent possible) to apply directly or by analogy, Ds' position is that those criteria would be sufficiently satisfied in respect of powers concerning communications data.

(3) <u>Disproportionate powers / absence of requirement for reasonable suspicion and individual targeting: Liberty's skeleton, §§38-41</u>

---

[24] See [105]-[106] per Lord Brown: "*There seems to me, indeed, a greater danger in the national court construing the Convention too generously in favour of an applicant than in construing it too narrowly. In the former event the mistake will necessarily stand; the member state cannot itself go to Strasbourg to have it corrected…*"

[25] See [100] per Lord Mance.

[26] Under Part 6 Chapter 1 of the Act (bulk interception) and Part 6 Chapter 3 of the Act (bulk equipment interference), it is in general necessary to obtain a targeted examination warrant, approved by a Judicial Commissioner, before undertaking any selection for examination of material obtained under a bulk warrant, if it is intended to select material for examination using criteria referable to an individual known to be in the British Islands at that time, where the purpose of using those criteria is to identify the content of their communications (or "protected material", as defined in s.193, in relation to equipment interference – "protected material" being a wide category that includes any private information). See sections 152 and 193 of the Act.

35. In light of the decision of the First Section in *BBW* as well as that in *Rättvisa v Sweden*[27] [**AB/5/70**] C no longer seeks to contend (at least at this stage) that bulk interception, or other bulk powers, are inherently disproportionate or that they require reasonable suspicion and individual targeting. C contends that it may seek to revive such arguments in further submissions or on any appeal, if the Convention jurisprudence develops. Ds will make any responsive submissions then.

36. Ds reject the submissions at §§41(1) and (2) of C's skeleton, and respond below to C's detailed submissions on Part 6 Chapter 3 and Part 5 (Equipment Interference); Part 7 (BPD); and Part 6 Chapter 1 (bulk interception).

(4) State databases of sensitive information: C's skeleton, §§42-44

37. The provisions in Pt 7 are confined to the retention or retention and examination of BPD, once designated as such, and not its initial acquisition. The authorities cited at §§42-44 are directed to the proportionality of the acquisition and storage of data pursuant to particular legal powers, and are therefore of limited relevance to the provisions of Part 7, which do not involve a legal power to acquire data at all. That is a critical point in appreciating the Convention compatibility of Part 7.

(5) Special protections for journalistic and watchdog sources and materials: C's skeleton, §§45-56

38. This section of C's skeleton does not accurately state the effect of the ECtHR's case law in relation to journalistic sources and materials. The points below also apply to the analysis in the NUJ's skeleton at §§10-22, which is to the same effect as C's own.

39. The ECtHR's case law establishes that where an order is sought requiring the divulging of a journalistic source, or the purpose of obtaining material is to discover a journalistic source, there must be prior review of the authorisation by an independent and impartial body, or at least prompt *post facto* review in urgent cases: see e.g. *Sanoma Uitgevers BV v The Netherlands* [2011] EMLR 4 at [90]-[92] [**AB/2/9**], *Telegraaf Media BV v The Netherlands* (app. 39315/06, 22 February 2013) at [98]-[102] [**AB/2/10**], *Nagla v Latvia* (app. no. 73469/10, 16 October 2013) at [89]-[90] [**AB/2/11**], *Tillack v Belgium* (2012) 55 EHRR 25 at [53] [**AB/5/64**], *Ernst v Belgium* (2004) 39 EHRR 35 at [103] [**AB/5/55**]. It also establishes that in such cases, there must be an "overriding public interest" outweighing the general public interest of source protection (see e.g. *Sanoma* at [91]).

40. The ECtHR does not require prior review by an independent or impartial body where surveillance is not targeted at journalists, but may result in the acquisition of

[27] App No 35252/08, Third Section, 19 June 2018.

journalistic material. See e.g. *Weber and Saravia* at [151]-152] [**AB/2/6**], *BBW* at [492]-[495] [**AB/2/20**]. In such cases, there will be an overriding requirement in the public interest justifying the selection for examination of journalists' communications only if the selection is "*accompanied by sufficient safeguards relating both to the circumstances in which they may be selected intentionally for examination, and to the protection of confidentiality where they have been selected, either intentionally or otherwise, for examination*": see *BBW* at [492][28]. But those safeguards need not consist of independent authorisation. Nothing in the ECtHR's case law suggests otherwise: including the cases most particularly relied upon by C (*Sanoma, Telegraaf Media, Nagla*).

41. *Sanoma* **[AB/2/9]** and *Telegraaf Media* **[AB/2/10]** specifically concerned orders which were made for the purpose of discovering the identity of a journalistic source (or which were treated by the ECtHR as tantamount to such orders[29]). It is in that context that they require "*the guarantee of review by a judge or other independent and impartial decision-making body*": see *Sanoma* at [49], [65]-[66], [72], [88]-[90], *Telegraaf Media* at [85]-[87], [97], [99]-[102][30].

42. *Nagla* **[AB/2/**11]was a case where a public prosecutor authorised an urgent search at the home of the applicant (a well-known journalist), in the course of which a personal

[28] The NUJ's skeleton accepts that *BBW* did not find that independent authorization was required when journalistic material obtained under a bulk warrant may be examined, but asserts that *BBW* "*did not reject this as a Convention requirement either*": see skeleton, §27. That assertion is not understood. *BBW* concerned circumstances in which no independent authorization was required for selecting journalistic material for examination, obtained pursuant to a warrant under s.8(4) RIPA. If that position had been unlawful because of the absence of independent authorization, *BBW* would have said so. The plain implication of [493] of the *BBW* judgment – and *BBW's* citation of *Weber* – is that the problem with the regime was not the absence of independent authorization at the stage of selection for examination. It was the lack of consideration given in the Interception of Communications Code under RIPA to safeguards circumscribing the intelligence services' power to search for confidential journalistic material. The example given by the Court in *BBW* of the type of provision that should have been contained in the Code was e.g. a requirement upon analysts, in selecting material for examination, to give "*particular consideration*" to whether confidential journalistic material is or may be involved: see [493].

[29] In *Sanoma,* the police suspected that a vehicle participating in a street race had been used as a getaway car following a ram raid. They contacted the editorial office of "Autoweek" (a magazine published by the applicant) to seek photos held by its editors concerning the race, and were told that the photos could not be surrendered, because the journalists had only been given permission to take photos on condition that the anonymity of the participants would be respected. The prosecutor then issued the editor-in-chief with a summons, ordering him to surrender the photographs. The applicant surrendered the material under protest: see [14]-[22]. The purpose of the order was thus source identification, albeit not identification of anonymous sources in connection with their participation in an illegal street race, but rather for another purpose. See [66]-[72]. The NUJ asserts that Ds *"wrongly interpret [Sanoma] as a case about an order to disclose sources"*: fn10. To the contrary, Ds' DGR at §40 correctly observed that *Sanoma* is a case about obtaining material in order to discover a source.

[30] The same point is equally true of most of the other cases cited by the NUJ at skeleton §10 i.e. *Tillack, Financial Times Ltd v United Kingdom* (2010) 50 EHRR 46 **[AB/5/64]**, and *Ernst* **[AB/5/55]**. The NUJ also cites *Weber* and *BBW,* but as explained above, neither *Weber* nor *BBW* supports their case.

laptop and other items were seized. The search was retrospectively approved, without reasons, by an investigating judge, and upheld with no hearing by the President of the first-instance court (see [22]-[25]). The Government argued that the purpose of the search was not to identify a source, because they already knew the identity of the source ("IP"); rather, the purpose of the search was to gather evidence in criminal proceedings against IP: [78]. The Court, however, found that the purpose of the search warrant in this case was an even more "*drastic measure*" than an order to divulge the identity of a source. That was because "*the search warrant was drafted in such vague terms as to allow the seizure of "any information" pertaining to the crime under investigation allegedly committed by the journalist's source, irrespective of whether or not his identity had already been known to the investigating authorities*": [95].

43. In that context, the ECtHR held as follows at [101] (which contains the nub of its reasoning):

"*The Court considers that any search involving the seizure of data storage devices such as laptops, external hard drives, memory cards and flash drives belonging to a journalist raises a question of the journalist's freedom of expression including source protection and that the access to the information contained therein must be protected by sufficient and adequate safeguards against abuse. In the present case, although the investigating judge's involvement in an immediate post factum review was provided for in the law, the Court finds that the investigating judge failed to establish that the interests of the investigation in securing evidence were sufficient to override the public interest in the protection of the journalist's freedom of expression, including source protection and protection against the handover of the research material*".

44. In short, *Nagla* was not a case addressing the need for independent authorisation at all: the search was judicially authorised. It was also a case where the interference at issue was held by the ECtHR to be even more serious than an order for source disclosure, because it concerned the wholesale and deliberate seizure of journalistic material, overriding any confidentiality in the applicant's sources. In that context, it cannot possibly be taken as authority for a proposition that <u>any</u> action that may result in the acquisition of journalistic material requires independent authorisation and/or an "*overriding public interest*".

45. Indeed, such a conclusion would be wholly at odds with the ECtHR's own case law. In *Weber* **[AB/2/6]**, one of the applicants (a journalist) complained that the state's practice of "strategic monitoring" of communications (i.e. bulk interception) interfered with her rights under Article 10 ECHR. That complaint was dismissed as manifestly ill-founded in the following terms (see [151]-[152]):

"The Court observes that in the instant case, strategic monitoring was carried out in order to prevent the offences listed in s.3(1). It was therefore not aimed at monitoring journalists; generally the authorities would know only when examining the intercepted telecommunications, if at all, that a journalist's conversation had been monitored. Surveillance measures were, in particular, not directed at uncovering journalistic sources. The interference with freedom of expression by means of strategic monitoring cannot, therefore, be characterised as particularly serious.

It is true that the impugned provisions of the amended G10 Act did not contain special rules safeguarding the protection of freedom of the press and, in particular, the non-disclosure of sources, once the authorities had become aware that they had intercepted a journalist's conversation. However, the Court, having regard to its findings under Art.8, observes that the impugned provisions contained numerous safeguards to keep the interference with the secrecy of telecommunications – and therefore with the freedom of the press – within the limits of what was necessary to achieve the legitimate aims pursued…"

46. All the above indicates that the protections for which C argues go far beyond principles clearly and consistently established by the ECtHR.

47. Nor does the judgment of the CoA in *R(Miranda) v Secretary of State for the Home Department* [2016] 1 WLR 1505 **[AB/2/15]**, upon which both C and the NUJ heavily rely, hold otherwise. As to *Miranda*:

(1) *Miranda* concerned the deliberate exercise of the power under Sch 7 to the Terrorism Act 2000 to stop, question and detain the claimant, who was travelling on behalf of a journalist to collect computer drives containing encrypted data stolen from a foreign security agency; and to retain the hard drives in question. In other words, this was a deliberate exercise of a power for the purpose of seizing journalistic material.

(2) The essential reasoning of the case is at [114]-[115], where Dyson LJ stated:

"Laws LJ may be right in saying that the ECtHR has not developed an "absolute" rule of judicial scrutiny for cases involving state interference with journalistic freedom. But prior judicial or other independent and impartial oversight (or immediate post factum oversight in urgent cases) is the natural and obvious adequate safeguard against the unlawful exercise of the Schedule 7 powers in cases involving journalistic freedom. For the reasons that I have given, the other safeguards relied on by Laws LJ provide inadequate protection. The 2000 Act, therefore, contains no adequate safeguards relating to journalistic material simpliciter or to journalistic material the disclosure of which may identify a journalistic source."

(3) *Miranda* thus holds that in the circumstances addressed (the deliberate exercise of a stop and search power to seize journalistic material), the Sch 7 power contained inadequate safeguards, and that the "*obvious*" safeguard would be prior independent authorisation.

(4) *Miranda* is clearly not authority for the proposition that the ECtHR jurisprudence establishes the need for independent prior authorisation in any case involving retention of journalistic material. Indeed, Dyson LJ explicitly stated apropos *Nagla* that *"it would be wrong to make too much of this decision of one section of the ECtHR"*: see [106]; and did not dissent from Laws LJ's analysis that the ECtHR has <u>not</u> developed an absolute rule of judicial scrutiny for cases involving state interference with journalistic freedom: see [114].

48. Finally, C's assertion at skeleton §§50 and 56 (mirrored by the NUJ at §10 of its skeleton) that *BBW* supports its case on the required scope of special protections for journalistic material misunderstands the reasoning in the *BBW* judgment. The ECtHR did not suggest, still less state, that prior independent approval would be required as a matter of Convention law whenever there was a request for a journalist's communications data, or where such collateral intrusion was likely:
    (1) The ECtHR's reasoning on the compatibility with the ECHR of the power to acquire communications data in Chapter II Part 1 RIPA was premised on the basis that (i) the power was incompatible with EU law, inter alia because access to retained data was not subject to prior review by an independent body, as a result of the CJEU's judgment in *Tele2 Sverige AB v Post-ochtelestyrelsen C-203/15* and *Watson C-698/15* [2017] QB 771 ("***Watson CJEU***"): see [466] [**AB/5/73**]; (ii) this Court in the April 2018 Divisional Court Judgment had found that the power was incompatible with domestic law on the same basis, following the Government's concession to that effect; and (iii) for that reason the power was not "in accordance with the law": see *BBW* at [466]-[468] [**AB/2/20**].

    (2) That was also the starting point for the ECtHR's consideration of the claim for breach of Article 10 in respect of Chapter II Part 1 RIPA: see [497]. It followed that save where the regime under Chapter II Part 1 RIPA provided for independent authorisation (viz, where data was sought for the purpose of identifying a journalist's source), it was not compatible with Article 10: see [498]-[499]. But the ECtHR's reasoning simply did not address (nor was it based on) the ECtHR jurisprudence on when prior independent authorisation is required by reason of the inherent demands of Article 10.

    (3) Indeed, if the ECtHR's reasoning on the acquisition of communications data under Chapter II Part 1 RIPA had the effect for which C and the NUJ contend, it would be completely inconsistent with the ECtHR's reasoning on the (inherently more intrusive) selection for examination of communications themselves. As explained above, the ECtHR did not find that selection for examination of journalistic material required prior independent authorisation under Article 10: see *BBW* at [492]-[495].

(6) Special protections for lawyer-client communications: C's skeleton, §§57-59

49. The ECtHR authorities on communications between lawyers and their clients, including all those relied upon by C are simply authority for the general principle applying to all the ECtHR's case law in this area, which is that the extent of safeguards required will depend on the level of interference with an individual's right to respect for private life. They indicate that it will be relevant (indeed, highly relevant) that surveillance concerns a lawyer and their client, because of the importance of

maintaining the confidentiality of lawyer/client exchanges. But they do not establish a lexicon of specific rules for all lawyer/client surveillance, let alone make the application of any such rules dependent upon whether material so obtained is defined as subject to LPP under the domestic law of any particular State.

50. Thus, addressing the case law cited at C's skeleton §§57-59, and the principles which C asserts that case law establishes:

(1) *McE v Prison Service of Northern Ireland* [2009] 1 AC 908[31] **[AB/4/33]** concerned covert surveillance in a police station of the content of conversations between detainees and their solicitors. The majority of the House of Lords held that in principle such surveillance was permitted under RIPA; but authorisation of such surveillance under s.28 RIPA and the relevant code of practice for "directed surveillance" did not provide sufficient safeguards under Article 8 ECHR. The majority also either stated or implied that if such surveillance had been duly authorised under the intrusive surveillance provisions of s.32 RIPA (and the associated code), it would have been lawful: see [66] per Lord Hope, [75] per Lady Hale, [94] per Lord Carswell, [113] per Lord Neuberger. The question of what rules should generally apply to any surveillance connected with lawyer/client exchanges was not addressed, save that they should be "*clear and stringent*" ([111], Lord Neuberger).

(2) *RE v United Kingdom* (2016) 63 EHRR 2 **[AB/5/67]** was another case about targeted surveillance of the content of lawyer/client communications in a police station. By the time this surveillance took place, the regime at issue in *McE* had been modified so that covert directed surveillance of legal consultations was to be treated as "intrusive surveillance" under RIPA[32]. The ECtHR stated at [118] that "*the decisive factor [when determining what safeguards should apply] will be the level of interference with an individual's right to respect for his or her private life and not the technical definition of the interference*". It stated for obvious reasons that the surveillance here entailed a very high degree of intrusion into Article 8 rights, and held that in the circumstances the relevant provisions of Part II RIPA and the relevant code did not comply with Article 8 ECHR. That was because they did not contain safeguards concerning the examination, use, handling and destruction of material obtained, equivalent to those applying in the context of the interception of communications[33]. No lexicon of rules applicable to all lawyer/client exchanges was laid down, though the ECtHR observed that generally "*strengthened protection*" should be afforded to such exchanges: [131].

[31] See SFG §71 [**TB/2/162**] and fn 102.
[32] See [75] at p.76
[33] See [139]-[142]. This problem was remedied on 22 June 2010, after the surveillance complained of, when the applicable safeguards were brought into line with those applying in the interception context: [140].

(3) *Kopp v Switzerland* (1998) 27 EHRR 91 **[AB/2/5]** concerned interception of the content of telephone conversations, and laid down no lexicon of rules applicable to all surveillance relating to lawyer/client exchanges. It is addressed further below.

(4) *Szabo and Vissy v Hungary* (2016) 63 EHRR 3 **[AB/2/14]** was not a case about lawyer-client communications at all, and [77] of *Szabo* does no more than purport to summarise principles from *Telegraaf Media* and *Kopp*.

(5) *Michaud v France* (2014) 59 EHRR 9 **[AB/2/8]** was not a case about surveillance. It concerned a regulatory requirement that members of the French Bar should report money laundering suspicions to the National Bar Council. The ECtHR (fifth section) observed that Article 8 ECHR conferred "*strengthened protection*" for the confidentiality of lawyer/client exchanges, in view of the importance of the repercussions for the proper administration of justice ([117]-[120]): but held that the obligation for lawyers to report suspicions did not constitute a disproportionate interference with professional privilege ([131]). No lexicon of general conditions applicable to all surveillance relating to lawyer/client exchanges was laid down.

51. Thus, insofar as the case law (and the law of the ECtHR generally in this area) establishes any principles which can be said to apply to all surveillance concerning lawyer/client exchanges, they are simply that: (i) the importance of lawyer/client confidentiality requires specific recognition, and strengthened protection accordingly; but (ii) in accordance with the ECtHR's customary approach, the question what protection is required will depend on the degree of interference in any particular case, not its technical classification.

52. C is wrong to claim at skeleton §57(2) that a decision about whether information is a lawyer-client communication must be taken (or supervised by) an independent body before surveillance commences. That assertion relies upon an obviously decontextualized reading of *Kopp*. In this, as in other, areas, C ignores the feature of the ECtHR's jurisprudence referred to by Laws LJ at [88] of *Miranda* in the Divisional Court[34] ([2014] 1 WLR 3140) **[AB/4/39]**, namely that "*although the court's reasoning is sometimes expressed in very general terms…in this area as in others its method and its practice is to concentrate on the facts of the particular case*".

53. *Kopp* was a case where the Federal public prosecutor ordered monitoring of the private and professional phone lines of the applicant (a lawyer) and his wife (the ex-Head of the Federal Department of Justice and Police) over a 3-week period between 21

[34] The CA allowed Mr Miranda's appeal against the Divisional Court's judgment: but nothing in the reasoning on appeal casts doubt on the principle addressed here.

November and 11 December 1989, in order to identify a person working at the Federal Department of Justice and Police who might have disclosed official secrets. The President of the Indictment Division of the Federal Court authorised an application for monitoring only after it had started (on 23 November 1989). The monitoring required officials of the Swiss Postal Services to listen to conversations of the applicant and other lawyers in his office over that period (all the telephone lines of the office being monitored), though the applicant himself was neither suspected nor accused. In that capacity, the officials were inevitably required to listen to a multitude of privileged conversations, even though the President's Order of 23 November stated "*the lawyers' conversations are not to be taken into account*". In that context, the ECtHR expressed astonishment that the task of distinguishing between (privileged) matters connected with a lawyer's work and those relating to other activity should be left to an official of the Post Office's legal department, "*with no supervision by an independent judge*": see [73]-[74]. *Kopp* did not purport to lay down any general principle that any decision about whether material is covered by LPP (or is a communication between a lawyer and a client) should be supervised by an independent judge (let alone, authorised on an *ex ante* basis). C seeks to draw a general principle from a case on extreme facts, which is not authority for the principle.

(IV) RESPONSE TO C'S DETAILED SUBMISSIONS

A. C's position in its skeleton

55. C's approach has substantially shifted in a number of respects from that set out in the Re-Amended SFG. Various aspects of its claim that were prominent in the SFG are now either not pursued or barely elaborated, presumably in light of the points raised in the DGR.

56. In that regard, the structure of C's basic - and essentially homogeneous - approach in respect of each of the various powers under challenge in the SFG was as follows:

    (1) **First**, C contended that each of the impugned powers were unlawful on the basis (in each case) of an absence of individual targeting and a requirement for reasonable suspicion. Ds responded to the relevant allegations, taken together, at DGR §§51-58 **[TB/2/370]**. However, as noted above, C now does not in its skeleton argument pursue these points (see skeleton §40) in relation to any of the impugned powers. This issue is therefore not considered further below.

    (2) **Secondly**, C contended that the scope of application of the various powers was too wide to comply with the Convention, regardless of the nature of the applicable safeguards. Ds responded to those allegations, by reference to each power in turn, at DGR §§60-87 **[TB/2/373]**. With the exception of the bulk equipment interference power in Part 6 Chapter 3 of the Act and the BPD provisions in Part 7 of the Act, C's skeleton argument does not pursue the point that the impugned powers are unlawful (without more) because their scope of application is too wide. Save in relation to Part 6 Chapter 3 and Part 7 of the Act, therefore, this issue is again not considered further below.

    (3) **Thirdly**, C contended that each of the impugned powers failed to comply with five further "*critical factors*" that C said were to be derived from the Strasbourg jurisprudence[35] relating to (i) duration, (ii) procedure for authorisation, (iii) procedure for use/examination/storage/precautions when communicating, (iv) circumstances of destruction and (v) notification and remedies. Ds responded to those essentially homogeneous allegations at DGR §§88-89 **[TB/392 et seq]** (duration), 90-95 (procedure for authorisation), 96-101 (procedure for use, etc.), 102-107 (circumstances of destruction), 108-114 (notification and remedies). In its skeleton argument, C (with some limited exceptions) does not make any further submissions about the "*critical factors*" in its SFG, and does not respond to the

[35] See SFG §59 **[TB/2/59]**. These so-called "critical features" are partly, but not completely, reflected in the *Weber* criteria, as to which see above.

detailed points at DGR §§89-114.[36] Instead, its typical approach is to raise <u>further</u> (and largely unpleaded) alleged defects in the applicable safeguards for each power. Ds' approach below is to respond to the <u>additional</u> points raised, without repeating the points at DGR §§89-114 where C has not addressed those points in its skeleton argument. For the avoidance of doubt, however, Ds fully maintain those points, and indeed rely on the more-or-less total absence of any answer to them in C's skeleton argument.

(4) **<u>Fourthly</u>**, C raised a number of Article 14 discrimination arguments, but confirmed in its Reply that these would not be pursued, no doubt following the rejection of equivalent arguments in *BBW*. Although the SFG has not been formally amended to confirm that the discrimination claims have been withdrawn, Article 14 is not considered in C's skeleton argument, and is therefore not considered further below.

<u>B. Challenge to the equipment interference powers – Part 6 Chapter 3 and Part 5</u>

(1) Nature of the interference

57. Ds accept that the ability to interfere with equipment in bulk is capable of resulting in substantial interferences with individual privacy rights. That is precisely why the bulk equipment interference power in Part 6 Chapter 3 is tightly controlled and subject to robust safeguards: see DGR, §81(1) **[TB/2/384]**. However, it is not accepted – and not "common ground" - that bulk equipment interference is necessarily wider or more intrusive than the other impugned bulk powers, still less that it gives rise to "*an extremely severe intrusion into privacy and freedom of expression, more so than any other power under the Act*" (C's skeleton, §64).

58. Moreover, here, as in the context of the other impugned bulk powers, no meaningful interference with privacy occurs until material is actually examined by an analyst, or at least selected for examination (albeit that the latter is ordinarily an automated process) (see Dix 2, §§21-22 **[TB/2/668]**), at which point the array of safeguards in s. 193 of the Act kicks in.

59. As to the various points raised at §63 of C's skeleton argument by reference to Danezis 2, Professor Danezis's evidence on the alleged risks associated with bulk equipment interference is overstated and in some cases wrong for the reasons given at Dix 2 §§10-18 **[TB/2/664]**. To take one example, Professor Danezis makes a range of points at §§28-

[36] See, for instance, §§85-89 of C's skeleton argument, in which it maintains (but does not elaborate on) its pleaded case in relation to the critical features concerning Pt 6 Ch 3, and then goes on to describe "*additional absences of sufficient safeguards*". The same point arises at skeleton §162.

33 of Danezis 2 **[TB/2/522]** that are based on an online article by two technical directors from GCHQ. However, having consulted with the authors of the article, Mr Dix explains that Professor Danezis has failed properly to appreciate the subject matter of the article, which concerned targeted interception (effected by a communications services provider) and not bulk equipment interference at all: see Dix 2, §§11-16 **[TB/2/664]**.

(2) C's contention that the Pt 6 Ch 3 power is too wide to be compatible with Articles 8 and 10

60. The essential contention advanced by C at §§66-75 of its skeleton argument is that the bulk equipment interference power in Part 6 Chapter 3 is too wide to be justified for Article 8 / Article 10 purposes, regardless of the adequacy of the safeguards attached to it.

61. C's contention that the Part 6 Chapter 3 power contravenes the Convention without more (and without any consideration of the applicable safeguards: cf. C's skeleton, §70) comes close to a submission that it is not permissible for a bulk equipment interference regime to be operated at all. If that is what is contended, it is untenable. In *BBW* **[AB/2/20]**, the ECtHR held that "*the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States' margin of appreciation*" ([314]). The same must equally be true of a system of bulk equipment interference. The compatibility of such a system with the ECHR cannot be addressed in isolation, by reference to a reading of the powers that is divorced from a consideration of the applicable safeguards.

62. The recognised width of the categories of persons liable to have their communications intercepted or selected for examination (the second and third questions identified in *BBW* at [330]) did not lead the ECtHR in *BBW* to conclude that the s. 8(4) RIPA power was itself too wide, having regard to the fact that "*by its very nature a bulk interception regime will allow the authorities a broad discretion to intercept communications and, as such, [the Court] does not consider* ***this fact alone*** *to be fatal to the Article 8 compliance of the section 8(4) regime*" ([338]; emphasis added).

63. Further, the scope of application of bulk equipment interference warrants under Part 6 Chapter 3 is in a number of respects less wide than the bulk interception power in s. 8(4) that was not considered to be too wide or of insufficiently clear scope by the First Section in *BBW*. Thus:

    (1) Not only must a warrant under s. 178 of the Act be necessary for one of the specified purposes (which are worded in equivalent terms to the provisions of s. 5(3) of RIPA considered to be sufficiently clear in *BBW*; see [335]) and proportionate, it must also specify the operational purpose for which any material

obtained under the warrant may be selected for examination. The specified operational purposes must be included in a list made by the Heads of the Intelligence Services, and be subject to review by the Prime Minister and (at regular 3-month intervals) provided to the ISC: see s. 183 of the Act. This is an important additional constraint which was not a feature of the s. 8(4) RIPA regime. C's contention that the 'operational purposes' requirement adds "*little by way of constraint*" (skeleton, §69(2)) again misses the point that an operational purpose may be specified in the list of operational purposes only with the approval of the Secretary of State (s.183(7)), and the Secretary of State may give such approval only if satisfied that the operational purpose is specified in "*a greater level of detail than the descriptions contained in section 178(1)(b) or (2)*": see s. 183(8) of the Act.

(2) Overall, while the First Section noted that it would be desirable for there to be certain additional safeguards at the selection for interception stage and the selection for examination stage (*BBW*, §347), it did not find that the width of the s. 8(4) RIPA power itself contravened the ECHR on the grounds of insufficient clarity or excessive breadth.

64. Precisely the same considerations apply, *mutatis mutandis*, to the bulk equipment interference power in Part 6 Chapter 3 of the Act. The grounds on which that power can be exercised are sufficiently clear. Accordingly, the width of those powers and the extent of the communications to which they may attach cannot, in and of itself, mean that the powers are unjustified, having regard to the State's wide margin of appreciation in this context: everything turns on the adequacy of the safeguards.

65. Ds also draw attention in this context, as relevant to the issue of necessity, to the observations of Lord Anderson QC in the Bulk Powers Review, §7.1-7.38 [**TB/4/579**], on the utility of the power; the reasons why it is needed; the way in which GCHQ (only) proposes to use it; and the fact that no alternatives may exist to its use. Specifically:
    (1) The operational case for EI lies in the context of diminishing returns from interception owing to developments including end-to-end encryption (100% of emails from major email providers, and 50% of internet traffic, being encrypted by the time of the review) and the increasing anonymization of network devices, making it harder to distinguish between target and non-target devices without at least some initial analysis of the data held on them;
    (2) The fact that bulk EI operations will be designed to bring back the minimum amount of information required to rule out devices not of intelligence interest, which would often imply a "light touch" operation targeted in the first instance on equipment data (this is, of course, required under s.2 of the Act);
    (3) The fact that a targeted EI warrant may not be feasible because of the trend towards anonymization of devices;
    (4) The non-viability of CHIS as an alternative in certain scenarios;

(5) Lord Anderson's conclusion at §7.36 **[TB/4/585]** (albeit expressing an appropriate degree of caution, in circumstances where the power had not yet been used) that "*an operational case for bulk EI has been made out in principle, and there are likely to be real-world instances in which no effective alternative is available*".

(3) Alleged defects in relation to the absence of a British Islands safeguard in Part 6 Chapter 3

66. At §§76-83 of its skeleton argument, C advances the argument that the (limited) flaws identified by the First Section in *BBW* **[AB/2/20]** in relation to the s. 8(4) RIPA regime can be 'read across' into Part 6 Chapter 3. This ignores the point (which is common ground[37]) that, when considering Convention compliance, it is essential to consider the entire panoply of safeguards relating to the power concerned.

67. *BBW* identified certain limited defects in the s. 8(4) RIPA regime due to what it considered to be two principal areas of concern: (i) lack of oversight of the selection process, including selection of bearers for interception and selectors used[38]; and (ii) the absence of "*any real safeguards applicable to the selection of related communications data for examination*" : see [387].

68. However, Part 6 Chapter 3 contains extensive and additional safeguards which were not a feature of the s. 8(4) RIPA regime, and which mean that the limited defects identified in *BBW* cannot and should not be transposed to a finding that the safeguards in Part 6 Chapter 3 are insufficient. The relevant safeguards are set out at DGR §81(1)(a)-(k), and are not repeated here.

69. As noted above, a specific defect was identified by the First Section in *BBW* in relation to the fact that the intelligence services could search and examine "related communications data" (**RCD**) intercepted pursuant to a s. 8(4) RIPA warrant without the restriction on the selection for examination of material obtained using criteria referable to persons known to be in the British Islands: *BBW* at [355]-[357]. C calls this the "British Islands Safeguard". It contends that it is unlawful for "non-protected" material to be excluded from the equivalent safeguard that is built into s. 193(1)(c) of the Act in relation to material obtained under the bulk equipment interference power.

[37] cf. C's Reply, §6 [**TB/2/324**].

[38] The Court stated that it did not consider the absence of safeguards governing the selection of bearers to be fatal to the Convention compatibility of the regime, but what was of "most concern" was the absence of oversight of selectors. The Government's position is that the Court misunderstood in certain important respects the oversight functions of the IPC's predecessor as regards oversight of the bulk interception regime (the Interception of Communications Commissioner), but in any event, the IPC plainly does have proper oversight of the selection of bearers and the choice of selectors. See inter alia Ds' letter of 10 December 2018 to the IPC **[TB/2/345]**.

70. However, C's apparent contention that the "British Islands Safeguard" requires a targeted examination warrant whenever it is wished to select for examination the RCD of a person in the British Islands, using criteria referable to that person, is clearly wrong (and would be deeply damaging to the capabilities of the Intelligence Services, if correct). In other words, the contention is wrong on its own terms, leaving aside the fact that it cannot be read across the bulk EI regime under Part 6 Chapter 3 of the Act:

(1) The ECtHR's judgment in *BBW* cannot be taken as meaning that, whatever the protections applied to the content of the communications of persons in the British Islands, and irrespective whether they go above and beyond what Articles 8/10 ECHR require, exactly the same protections must always be applied to RCD. There would be no obvious principle for that conclusion, and the likely consequence of such a requirement would simply be the watering-down of any protections applied to content itself. Council of Europe states should not be discouraged from applying more stringent safeguards to content, on the basis that they always require "reading across" to RCD as well.

(2) As explained in Dix 2 at §§49-53 [**TB/2/679]**, it would be wholly impracticable for there to be a certification regime for RCD, equivalent to the certification regime in place under s.16(2) RIPA. The Secretary of State could not possibly consider personally the necessity and proportionality of targeting individuals based in the British Islands, on an individualised basis, for the reasons set out in Dix 2 §§49-51 (i.e. the fact that RCD is used to a great extent to discover unknown threats; the diversity of communications data types, and intelligence targets' use of technologies; the invaluable utility of RCD in discounting individuals from further intelligence interest, including individuals in the UK; and the resulting operational reality that many thousand such searches are undertaken every week in relation to individuals known or believed to be in the UK alone). The result of applying such a system would be a change of operational tradecraft which would almost inevitably lessen the utility of RCD, thus prejudicing national security and putting lives at risk.

(3) The same points about impracticality must be all the more true, now that the "British Islands safeguard" (under the Act) requires not simply certification by the Secretary of State, but a targeted examination warrant, issued by a Judicial Commissioner.

(4) Moreover, as set out in Dix 2 at §54 **[TB/2/681]**, the Government is taking steps in light of the *BBW* judgment to ensure that where non-content data is to be selected for examination by reference to a factor referable to a person who is believed to be in the British Islands, that must be certified as necessary and proportionate by the Secretary of State on a properly specific "thematic" basis (i.e. not individual by individual, but by reference to specified groups of individuals). It is intended to change the Interception of Communications Code to that effect. This would meet

the defect identified by the First Section in *BBW* in relation to the RIPA regime, were it still in place. *A fortiori,* to the extent (which is not accepted) that such defect could be "read across" to the bulk interception regime under Part 6 Chapter 1 RIPA, it will meet the defect in that context too.

71. Further, it should be noted that although no "read across" of the "British Islands Safeguard" findings in *BBW* to the bulk EI regime is appropriate in the first place in light of the extensive safeguards in the bulk EI regime (as set out above), the Government also proposes to apply the new "thematic certification" safeguard to "non-protected" material obtained under a bulk EI warrant; and proposes to alter the Equipment Interference Code to that effect. (See e.g. Ds' letter to C of 24 May 2019 in relation to disclosure, at [**TB/2/889**]).

72. Taken as a whole, therefore, there is no basis for the contention that the findings in *BBW* relating to RCD can be read across so as to establish a contravention of the ECHR in relation to Part 6 Chapter 3 and non-protected material. Moreover, if such a "read across" were appropriate, the Government is already taking steps to make amendments to the bulk EI regime which would address any such contravention: so any relief in that respect would be unnecessary and inappropriate.

(4) Alleged failure to comply with minimum safeguards

73. At §85 of its skeleton argument, C refers, without elaboration, to its pleaded case at SFG §§142-147 **[TB/2/224]** and Reply §§19-20 **[TB/2/329]** as to the alleged non-compliance of Part 6 Chapter 3 with the further "*critical factors*". However, in the main, it does not go on to address Ds' detailed response in the DGR to the allegations from the SFG and the Reply in relation to those factors. Ds do not reiterate their (largely unanswered) response to these points from the DGR.

74. As to the alleged "*additional absences of sufficient safeguards*" set out at §§86-89 of C's skeleton argument:

(1) As to the effect of s. 225 of the Act, this is addressed above at §18(2) above and is considered further below in the context of Part 7 (where the provision appears). The short point is that while s. 225 disapplies the safeguards applicable under Part 6 Chapter3 itself, it replaces them with a separate system of safeguards under Part 7 that can be appropriately tailored by reference to the material rather than the power under which it was obtained, which C omits to mention.

(2) As to the addition of operational purposes, C's point at §87(b) is not understood. Where an additional operational purpose is to be added to a warrant, this will be subject to all the safeguards applicable to the inclusion of an operational purpose in a warrant at the initial approval stage, including the 'double-lock' approval process (or *post hoc* approval by a Judicial Commissioner in cases of urgency): see

DGR, §§92(3) and (4) **[TB/2/393]**. It is therefore true, in one sense, that "*information may be used other than for purposes in existence when it was collected*", but only subject to the same strict safeguards as apply in relation to the initial warrant. The point therefore takes C nowhere.

(3) C's point at §88 concerning the allegedly weak Judicial Commissioner ("JC") approval process is similarly hard to follow. On the one hand, C contends that the JC's status as an 'approver', applying a judicial review standard, gives only "*limited additional protection*", but it then goes on to note that a JC must decide for himself the question of fair balance in relation to the proportionality of a warrant. Given that the JC must do so, and will have access to the same material as the Secretary of State, this 'double-lock' process is patently a very strong safeguard which differentiates the regime under Part 6 Chapter 3 (and other aspects of the Act) from predecessor legislation concerning investigatory powers. C's contention that the requirement for JC approval still does not pass muster for Convention purposes is impossible to reconcile with the fact that, in *BBW*, the First Section of the ECtHR considered that the power to issue a warrant in s. 8(4) RIPA was Convention-compliant without any form of independent authorisation at all (although limited other aspects of the system of oversight were held to be defective): see *BBW*, [381] **[AB/2/20]**.

(4) As to C's points at §89 of its skeleton argument concerning the IPC and the IPT:

i. C fails to explain why a system under which only errors causing significant prejudice or harm may be the subject of error reporting by the IPC is inadequate. The logical implication is that insignificant errors ought to be reported, but that is manifestly unsustainable.

ii. C similarly fails to explain why it is problematic for there to be a jurisdictional requirement for an applicant to have some basis (as opposed to no basis) for a suspicion that they are under surveillance before bringing a case to the IPT.

iii. C simply ignores the approving findings in *BBW* as to the extensive post-authorisation scrutiny provided by the IPC and the IPT: [377]-[381] (and see further [255]-[265] in relation to the effectiveness of the IPT as a remedy). In circumstances where the IPC has become substantially better resourced, and the IPT has an expanded jurisdiction and a new right of appeal (cf. DGR, §§18-24 **[TB/2/363]**) under the new regime introduced by the Act[39], the contention that

[39] And further, as explained above, the Supreme Court has now held in *R(Privacy International) v Investigatory Powers Tribunal* [2019] UKSC 22 (15 May 2019) **[AB/4/46]** that decisions of the IPT even prior to the introduction of the right of appeal may be subject to the judicial review jurisdiction of the High Court.

these systems of oversight are somehow too limited to be adequate lacks credibility.

(5) C's challenge to Part 5 of the Act

75. C does not now pursue the point that thematic and targeted equipment interference provisions in Part 5 of the Act are unlawful due to an absence of reasonable suspicion / individual targeting requirements: skeleton, §92.

Greennet

76. C's submissions instead focus on the contention that the "*thematic*" provisions in s. 101 (1)(b)-(h) of the Act (but not the "*targeted*" provisions in s. 101(1)(a)) do not comply with the Convention minimum requirements. However, *pace* C's skeleton argument at §93(4), the *Greennet* case **[AB/2/16]** does indeed effectively conclude this aspect of the claim against C, for the reasons given at DGR §82 **[TB/2/386]**. The fact that Part 5 of the Act includes certain limited additional purposes to those under s. 5 of the Intelligence Services Act 1994 is not a material point of distinction, especially when in every other meaningful respect the thematic equipment interference power in the Act is much narrower than the provision at issue in *Greennet*, due to the addition of the variety of safeguards under the Act. The fact that permission to apply judicial review has been granted in respect of *Greennet* in respect of a different issue is nothing to the point. Similarly, the fact that there have been further developments in the Strasbourg jurisprudence since *Greennet* is nothing to the point, given that C does not suggest that those developments affect the basic legal principles that the IPT applied in that case.

77. Whether or not the Administrative Court is bound (or ought as a matter of judicial comity) to follow the decision in *Greennet*, Ds contend that the IPT was correct to hold that the power at issue in that case was Convention-compliant, and that the position is *a fortiori* in relation to the thematic equipment interference power in Part 5 of the Act, given the array of stricter safeguards that apply to the latter.

Other points in C's skeleton argument concerning Part 5

78. The contentions at C's skeleton §§95(1)-(3) amount in substance to a submission that the permitted scope of thematic equipment interference warrants is, without more, too wide to be ECHR compliant[40]. For all the reasons given above in relation to Part 6 Chapter 3,

[40] Save that Liberty has (rightly, in light of DGR §82(2)) withdrawn the contention at SFG §156(2) **[TB/2/237]** that thematic equipment interference warrants are not required to describe the information that it is their purpose to retrieve.

that is wrong: in the absence of any basis for suggesting that the thematic equipment interference power is insufficiently clear to be "*accessible*" (as to which see the clear description of the grounds on which a warrant may be obtained in s. 101(1)(b)-(h) and 102 of the Act), the compatibility of that power with the Convention depends on the adequacy of the safeguards. In that regard, Ds repeat §74 above, *mutatis mutandis*.

79. In any event, the following should be noted in regard to the specific points made at §§95(1)-(3) of C's skeleton:

(1) C is wrong to assert at §95(1) that the purposes for which a warrant may be issued under Part 5 of the Act are "wider" than the applicable purposes under the targeted interception warrant regime at issue *Kennedy* **[TB/5/62]**. The grounds upon which a Part 5 warrant may be issued to the Intelligence Services are narrower than those applicable to interception warrants under s.5 RIPA, at issue in *Kennedy* [41]. The Act also permits law enforcement chiefs to seek warrants for the purposes of preventing or detecting serious crime, or preventing death or injury. It is true that "*preventing death or injury*" is not a purpose in s.5 RIPA; but that cannot realistically be a meaningful distinction. As to the observation that the Part 5 power can be used to alter equipment or information, the Act provides that a warrant may authorise conduct ancillary to obtaining information only to the extent that it is "*necessary to undertake in order to do what is expressly authorised or required by the warrant, including conduct for securing the obtaining of communications, equipment data or other information*": s.99(5)(a) of the Act.

(2) §95(2) of the skeleton overlooks the provisions as to specificity of warrants, contained in the EI Code **[AB/3/22]** and s.115 of the Act (most particularly, the details of warrants set out in the tables forming part of s.115(3) and 115(4), which C does not acknowledge). See in particular Code §5.15:

"The Act requires that certain additional details must be included in the warrant dependent on the subject-matter(s) of the warrant. For example, a thematic warrant that relates to equipment used by a group which shares a common purpose must include a description of that purpose as well as the name or description of as many of the persons who form that group as it is reasonably practicable to name or describe. An equipment interference authority must, when section 115 requires, name or describe as many of the persons, organisations or locations as is reasonably practicable. The descriptions of persons, organisations or locations must be as granular as reasonably practicable in order to

[41] *Kennedy v UK* concerned targeted interception warrants. Under s.5 RIPA, such warrants could be issued for the purposes of national security, the prevention or detection of serious crime, the safeguarding of the economic well-being of the United Kingdom, or giving effect to any international mutual assistance agreement. Under s.102(5) of the Act, a warrant can only be issued to the Intelligence Services for national security, the prevention or detection of serious crime, or in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security. Section 106 of the Act permits applications for targeted warrants by law enforcement chiefs (as defined), and such applications may be both for the prevention or detection of serious crime, or the purpose of preventing death or injury.

sufficiently enable proper assessment of the proportionality and intrusion involved in the interference."

(3) The same point equally applies to skeleton, §95(3).

C. Challenge to the bulk personal dataset provisions – Part 7 of the Act: C's skeleton, §§99-120

(1) Nature of the interference

80. The BPD provisions in Part 7 of the Act are of a fundamentally different character to the other provisions under challenge in these judicial review proceedings. In particular, and critically, Part 7 does not give the State any power to obtain information at all. Nor does it confer any new power to retain information that could not otherwise be held. Rather, Part 7 applies a series of safeguards to information obtained under other powers[42]:

(1) Where a set of information already obtained by an intelligence agency other than under the Act[43] possesses a certain quality – that is, where the information satisfies the definition of a BPD in s. 199(1) of the Act[44] – then the information must be treated as a BPD under Part 7. That means the continued retention, or retention and examination, of that material is subject to a series of robust safeguards, including a requirement for judicial authorisation: see further DGR, §87(2) **[TB/2/390]**. Importantly, this is not a matter of discretion for the intelligence agencies. If an intelligence agency retains a BPD that has been acquired under other powers, then it must obtain a warrant under Pt 7 if it wishes to continue retaining the set of information concerned: s. 200(1). Such a warrant may either be a "specific" BPD warrant or a "class" BPD warrant: s. 200(3)(a) and (b). In both cases, Judicial Commissioner approval is required before the Secretary of State may grant a warrant: s. 208.

---

[42] This point is made very clear in the BPD Code, at numerous places. See e.g. §3.1 of the Code **[AB/3/23]**: *"The Act does not create any new power to obtain BPDs. Rather it requires that the retention and use of BPDs must be subject to an authorisation scheme and a comprehensive set of robust and transparent safeguards."*

[43] Including pursuant to powers under the Intelligence Services Act ("**ISA**") 1994 **[AB/6/79]** and the Security Service Act ("**SSA**") 1989 **[AB/6/78]**.

[44] That is, it is a set of information including personal data relating to a number of individuals; the nature of the set is such that the majority of the individuals are not, and are unlikely to become, of intelligence interest; after any initial examination, the intelligence service retains the set of information for the exercise of its functions; and the set is held, or to be held, electronically for analysis in the exercise of those functions.

(2) Where a BPD has already been acquired and retained by an intelligence agency pursuant to a warrant obtained under a different Part of the Act, then the starting point is that no further warrant under Part 7 authorising its continued retention, or retention and examination, is necessary: s. 201 of the Act. However, under s. 225 of the Act, the head of the intelligence service concerned may apply to the Secretary of State for a direction that a BPD obtained pursuant to a warrant obtained under a different Part of the Act (with the exception of Part 6 Chapter 2) should be treated as subject to the regime in Part 7, whereupon the power under which the BPD was originally retained ceases to apply (though some of the associated regulatory provisions that applied under the acquiring regime will still apply[45]): s. 225(3). If such a direction is given, the intelligence service concerned may only exercise its power to retain or retain and examine the BPD by virtue of the direction, if authorised to do so by either a specific BPD warrant or a class BPD warrant under Part 7: s. 225(4). Importantly, a direction under s. 225(3) may itself only be given with the approval of a Judicial Commissioner: s. 225(7).

81. The arguments at §§99-101 of C's skeleton argument start from a false premise, that Part 7 itself authorises the obtaining, retention (etc.) of personal data. This is not the correct analysis, for the reasons just given. In the absence of a separate power to obtain / retain personal data, Part 7 can never apply.

(2) C's contention that the "Part 7 power" is too wide to be compatible with Articles 8 and 10

82. At §§102-113 of its skeleton argument, C advances the argument that the "*Part 7 power*" (sic) is too wide to be compatible with the Convention. As just noted, Part 7 simply provides a detailed statutory framework and safeguards for the retention, or retention and examination, of BPDs obtained under other powers. For this reason, the analogy with the cases of *S & Marper* (2009) 48 EHRR 50 **[AB/2/7]** and *MK v France* (app. 19522/09) **[AB/5/66]** is inapt. For instance, *Marper* concerned a blanket power to obtain and retain DNA and fingerprint samples, and not a system of safeguards for samples obtained pursuant to different statutory powers. That is quite apart from the fact that there is no sensible comparison to be drawn between the blanket, indiscriminate and indefinite retention of data in *Marper,* and the carefully calibrated safeguards governing retention put in place under Part 7 of the Act.

83. In the circumstances, it is not by the light of Part 7 that the 'width' of any power to retain BPDs should be assessed by the Court, but by reference to the powers under which BPDs are actually obtained, or retained, in the first place. But in that regard:

[45] See s.225(6) of the Act as regards the continued application of the safeguards in ss.56-59 of the Act concerning disclosure of material in legal proceedings, and the duty not to make unauthorized disclosures.

(1) There is no challenge to the regime in ISA 1994 **[AB/6/79]** and SSA 1989 [**AB/6/78]**. Such a challenge would have been hopeless, in the light of the finding in *Privacy International v SSFCO and ors* [2016] UKIPTrib15_110-CH ("***Privacy IPT***") **[AB/2/17]** that the scope of application of that regime was compatible with the Convention even without the safeguards in Part 7.

(2) As to the scope of application of the various other powers by which BPD might be obtained under the Act itself:

i. By virtue of s. 225(2), a direction under s. 225(3) cannot be given in respect of a BPD obtained under the bulk acquisition powers in Part 6 Chapter 2, so that there is no question of the Part 7 regime applying in respect of BPD under those powers.

ii. As to the various other powers under the Act, the only power in respect of which C now pursues a challenge as to the scope of its application is the bulk equipment interference power in Part 6 Chapter 3. For the reasons given at §§60-65 above, however, the contention that the Part 6 Chapter 3 power is too wide to be compatible with the Convention is wrong.

84. In the circumstances, the contention that "the Part 7 power" itself is too wide is incoherent: the scope of application of the powers that do permit the obtaining and retaining of BPD in the first place are either unchallenged in these proceedings, not pursued at this stage, or (in the sole case of Part 6 Chapter 3) compliant with the Convention for the reasons given elsewhere in this skeleton argument.

85. It follows that the potential applicability of Part 7 to a wide variety of different information, provided that the information satisfies the statutory definition of a BPD in s.199 of the Act (which is common ground) is not a reason for impugning Part 7, but the exact opposite. It means that the safeguards within Part 7 will be widely applied. For that reason, C's skeleton at §§108-109 is misdirected. Most particularly, the contention at §108 of C's skeleton that Part 7 "*is an enabling power*" is a basic misunderstanding.

86. C's argument shifts at §110 to an alternative contention that the Part 7 regime is insufficiently foreseeable, because it contains insufficient safeguards.

87. The question for the Court in this context is the general one identified in *Malone* at [68] **[AB/5/49]**, namely whether domestic law indicates the scope of any discretion and the manner of its exercise with sufficient clarity "*to give the individual adequate protection against arbitrary interference*" (cf. *Zakharov* at [230] **[AB/2/13]**). The more detailed *Weber* criteria are inapplicable in this context, since (taken at their highest) they pertain to the lawfulness of powers to gather information, as opposed to the lawfulness of

safeguards imposed in relation to information already gathered under a different power or powers.

88. Applying that general test, the IPT held in *Privacy IPT* [**AB/2/17**] that the regime governing the obtaining, retention and examination of BPDs following the publication of the ISC's report on their use on 12 March 2015 **[TB/3/193]** was sufficiently foreseeable to comply with Article 8 ECHR, before the panoply of protections in Part 7 of the Act came into effect. See its October 2016 judgment, [100]. *A fortiori,* the Part 7 regime is clearly sufficiently foreseeable.

89. In answer to C's criticisms of the various additional statutory requirements at §110 of its skeleton argument:

(1) As to §110(1) of C's skeleton argument:

i. it is correct that the requirement for examination to be necessary for operational purposes does not constrain the power to retain information. But there are other statutory safeguards on the power to retain a BPD pursuant to either a class or a specific BPD warrant i.e. all the requirements of the Part 7 warrantry regime, including the need for a detailed application for a warrant to be made to the Secretary of State, containing the information in s.204 or 205 of the Act, as the case may be, as expanded upon by Chapter 5 of the BPD Code; the requirement for the Secretary of State to approve such a warrant only where satisfied that it is proportionate and necessary on the grounds in ss.204/205 of the Act; and notably, the requirement that a Judicial Commissioner approve such a warrant (s.208 of the Act).

ii. The '*operational purposes'* requirement is a substantial safeguard on the power to examine, and it is not the case that operational purposes will be identical to the statutory bases for the issue of a warrant. That is because, as in other Parts of the Act, the operational purposes which may be included in a BPD warrant must be specified in a "list of operational purposes" maintained by the heads of the intelligence services, which require the Secretary of State's approval, and to which approval may only be given where the operational purposes are specified "*in a greater level of detail*" than the descriptions given in s.204(3)(a) or 205(6)(a) as to the bases on which a warrant may be obtained generally (i.e. national security etc): see s. 212(5)-(8). The list of operational purposes is subject to regular review by the ISC and the Prime Minister: ss. 212(9) and (11).

(2) As to §110(2) of Liberty's skeleton argument, concerning the absence of a British Islands safeguard:

i. Where the Secretary of State considers that such a safeguard should be imposed in the case of the selection for examination of protected data in a dataset

retained pursuant to a specific BPD warrant, he may do so: s. 207[46]. The presence or absence of such a safeguard is a matter that falls to be considered by a Judicial Commissioner in deciding whether to approve a given request for a warrant.

ii. In the case of a class BPD warrant, an intelligence service may not retain, or retain and examine, a BPD pursuant to a class BPD warrant at all if the head of the intelligence service considers that the BPD consists of, or includes, "protected data" (defined in s. 203[47]) or health records (defined in s. 206), or if a substantial proportion of it consists of sensitive personal data (defined in s. 202(4) by reference to s.86(7)(a)-(e) Data Protection Act 2018[48]). See s. 202 of the Act. The inevitable effect of that limitation is that no content retained pursuant to a class BPD warrant could be selected for examination on the basis of criteria referable to an individual known to be in the British Islands in the first place, because that would involve retaining and examining "protected data" for the purposes of s.203 of the Act[49].

---

[46] Section 207 must also be read with s.221(3), which states: *"The Secretary of State must also ensure, in relation to every specific BPD warrant which specifies conditions imposed under section 207, that arrangements are in force for securing that any selection for examination of protected data on the basis of criteria which are referable to an individual known to be in the British Islands at the time of the selection is in accordance with the conditions specified in the warrant."*

[47] "Protected data" is defined by s.203(1) as *"any data contained in a bulk personal dataset other than data which is one or more of the following: (a) systems data; (b) data which falls within subsection (2); (c) data which is not private information"*.
Data which falls within subsection (2) is: "*identifying data which- (a) is contained within the bulk personal dataset, (b) is capable of being logically separated from the bulk personal dataset, and (c) if it were so separated, would not reveal anything of what might reasonably be considered to be the meaning (if any) of any of the data which would remain in the bulk personal dataset or of the bulk personal dataset itself, disregarding any meaning arising from the existence of that data or (as the case may be) the existence of the bulk personal dataset or from any data relating to that fact*".
"Systems data" is defined in s.263(4) of the Act.

[48] Section 202(4) of the Act (as of 29 March 2019, pursuant to amendments made by SI 2019/419) defines "sensitive personal data" as *"personal data consisting of information about an individual (whether living or deceased) the processing of which would be sensitive processing for the purposes of section 86(7)(a)-(e) of the Data Protection Act 2018"*. "Sensitive processing" under s.86(7)(a)-(e) of the 2018 Act is defined as:
"(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
(b) the processing of genetic data for the purpose of uniquely identifying an individual;
(c) the processing of biometric data for the purpose of uniquely identifying an individual;
(d) the processing of data concerning health;
(e) the processing of data concerning an individual's sex life or sexual orientation"

[49] There are other restrictions on the grant of a class BPD warrant as well: for instance, a statutory restriction in s.202(3) that an intelligence service may not retain, or retain and examine, a BPD in reliance on a class BPD warrant *"if the head of the intelligence service considers that the nature of the bulk personal dataset, or the circumstances in which it was created, is or are such that its retention, or retention and examination, by the intelligence service raises novel or contentious issues which ought to be considered by the Secretary of State and a Judicial Commissioner on an application by the head of the intelligence service for a specific BPD warrant."*

iii. Given the strict statutory restrictions on the kind of material that may be retained and examined pursuant to a BPD warrant, in addition to the safeguards attached to BPD warrants generally, the absence of a mandatory British Islands safeguard cannot be regarded as a factor that renders the Part 7 provisions incompatible with the Convention. The ECtHR's conclusions in *BBW* concerning the treatment of a different kind of information (related communications data) in a different statutory context (s. 8(4) RIPA) cannot sensibly or fairly be read across in this way, *pace* §110(2)(c) of C's skeleton argument.

(3) As to §110(3) of C's skeleton argument, DGR §87(7)(c) **[TB/2/391]** does not amount to an admission that class BPD warrants are unnecessary / unjustifiable in all cases. The point at DGR §87(7)(c) is simply that a class BPD warrant may only be issued where it is necessary and proportionate. If, on a given set of facts, it is not considered by the Secretary of State to be necessary and proportionate to approve a class BPD warrant (because a specific BPD warrant is available as a less intrusive means of achieving the same intelligence objective) then the Secretary of State will not be able to give such approval. It simply does not follow that, in all cases, a BPD class warrant will be unnecessary or disproportionate. It will – unsurprisingly - depend on the circumstances. Most particularly, it would be unworkable and unnecessary to obtain individual specific BPD warrants for individual datasets of the same class, where the underlying data is subject to exactly the same necessity and proportionality considerations.

(4) The assertion at §110(4) of C's skeleton argument is not understood. The matters pleaded at DGR §87 plainly do constitute real restrictions on the exercise of the various provisions of Part 7, i.e. that its scope is indeed narrower than C pleads.

90. At §111 of its skeleton argument, C wrongly characterises Ds' position. Ds do not contend that Articles 8 and 10 require nothing more than the express conferral of a power. Leaving aside that C has misunderstood the nature of Part 7 in approaching the provision as though it confers a power to obtain information, Ds accept that the requirements of accessibility and foreseeability must be satisfied by the power at issue. They are so satisfied.

(3) "Part 7 does not otherwise satisfy the minimum safeguards": C's skeleton, §§114-120

91. §115 of C's skeleton essentially repeats contentions advanced at §194(3B) of C's SFG **[TB/2/267]**. Ds answered those contentions at DGR§87(7) **[TB/2/391]**. In particular:
(1) The issue of either a class or a specific BPD warrant requires the approval of a Judicial Commissioner, who will assess the necessity and proportionality of issuing a warrant of the type in question, with the benefit of detailed information inter alia as to the nature of the BPDs to which the warrant relates; the extent of personal data within them and any other factors relevant to their intrusiveness;

and the operational justification for retaining and examining them. *Pace* §115(1), it is thus clearly wrong that class BPD warrants create a "*sub-discretion, exercised entirely in secret and without Judicial Commissioner oversight*", as to (a) whether a dataset falls within a class; and (b) whether to retain a dataset. Given that a class BPD warrant must be authorised by a Judicial Commissioner, and given that the Judicial Commissioner will have all the detailed information in the warrant application when he makes that determination, a Judicial Commissioner will precisely have oversight as to whether a class is sufficiently clearly defined, and what sort of datasets will fall within it.

(2) Indeed, the Secretary of State can only issue a class BPD warrant, where he is satisfied that it will be possible for the Secretary of State and Judicial Commissioner to exercise effective oversight of the operation of the class BPD warrant and of the retention and use of individual BPDs authorised by that warrant: Code, §5.2 **[AB/3/23]**.

(3) It is inherent within the whole scheme of the Act that a class BPD warrant can be issued only where it is necessary and proportionate to do so, because no less intrusive means would be capable of achieving the aims in question. See s.2 of the Act. In other words, where a less intrusive specific BPD warrant or warrants are capable of achieving the ends in question, it is not open to the Secretary of State to issue a class warrant (and a Judicial Commissioner will not approve it). Still further, where it is proposed to apply for a class BPD warrant, the Secretary of State (and Judicial Commissioner) is obliged to consider whether the proposed warrant should be split into smaller classes and revised applications submitted for a smaller class BPD warrant or warrants, in order to ensure effective oversight. See Code, §§5.4[50] and 5.5 **[AB/3/23]**.

(4) Further, s.202 of the Act contains important statutory restrictions on the use of class BPD warrants, viz. (i) an Intelligence Service may not retain or retain and examine a bulk personal dataset in reliance on a class BPD warrant, if the head of the Intelligence Service considers that it consists of, or includes, "protected data", as defined in s.203; (ii) "protected data" itself consists of a wide class of information: see above; (iii) in addition, an Intelligence Service may not retain, or retain and examine, a BPD in reliance on a class BPD warrant if the head of the service considers that it consists of, or includes health records, or that a substantial proportion of the BPD consists of sensitive personal data: see above; and (iv) an Intelligence Service may not retain, or retain and examine, a BPD in reliance on a class BPD warrant if the head of the Intelligence Service considers that the nature

[50] §5.4 of the Code illustrates the above point, stating *"Where the Secretary of State refuses to issue the warrant, he or she may instead invite the relevant intelligence service to split the class into smaller classes and submit revised applications for a smaller class BPD warrant or smaller class BPD warrants and (where appropriate) specific BPD warrants for any individual BPDs."*

of the BPD, or the circumstances in which it was created, is or are such that its retention, or retention and examination, raises novel or contentious issue which ought to be considered by the Secretary of State and a Judicial Commissioner on an application for a specific BPD warrant. See s.202(3) of the Act.

(5) The above position clearly provides sufficient safeguards against abuse for the purposes of Articles 8 and 10 ECHR.

92. As to "*duration and cancellation provisions*", the basic premise of C's skeleton at §§116-117 is wrong. Section 219 of the Act contains "bridging" provisions to ensure that any retention and examination of material within a BPD remains lawful for a limited period following the non-renewal or cancellation of a warrant, pending authorisation via a new warrant. If an Intelligence Service were to use those bridging provisions so as to avoid the need for selection for examination to be only for "operational purposes", it would be acting unlawfully as a matter of basic public law (i.e. it would be acting for an improper purpose, and/or acting contrary to the *Padfield* principle). Further, examination of material is <u>always</u> constrained by principles of necessity and proportionality under the Intelligence Service's own internal safeguards and s.6 HRA 1998[51].

93. At §118 of its skeleton, C complains that there is "*no (or at least no clear) provision requiring destruction*" of a BPD, or copies of material derived from it, once the BPD warrant has expired. But this again is wrong. §7.55 of the BPD Code is precisely such a provision. It states:

"Where the continued retention of any [BPD retained under a class warrant] no longer meets the tests of necessity and proportionality, all copies, extracts and summaries of it held within the relevant intelligence service must be scheduled for destruction as soon as possible once it is no longer needed for any of the authorised purposes".

That is sufficiently clear.

94. C's skeleton at §119 (*"weak Judicial Commissioner approval regime"*) and §120 (*"very limited notification [of errors]"*) repeat points addressed elsewhere.

[51] C also fails to note important safeguards within the bridging provisions themselves. For instance, where the Head of an Intelligence Service has not applied for a further warrant within 5 working days of the ending of the previous warrant, but wishes to consider further whether to apply for another BPD warrant, they must apply to the Secretary of State for authorization to retain, or retain and examine, the BPD in the meantime; that authorization may only be granted for a maximum period of 3 months; and importantly, the Secretary of State's authorization must <u>itself</u> be approved by a Judicial Commissioner (see s.219(3)(b)).

D. Challenge to the bulk interception powers – Part 6 Chapter 1

(1) Nature of the interference

95. The ability to effect interception in bulk is a critical capability for the Intelligence Services. It will often be the only way by which they can establish links between known subjects of interest, search for traces of activity by individuals who may not yet be known, and (more generally) identify patterns of activity that might indicate a threat to the United Kingdom: Dix 1, §190 **[TB/2/468]**. It is precisely its bulk nature that makes material acquired and retained pursuant to bulk interception powers so useful for the purposes of protecting national security and enabling the effective investigation of serious crime.

96. Bulk interception is not a new power. Its previous incarnation, in s. 8(4) RIPA, was the subject of detailed judicial consideration in *Liberty IPT* **[AB/2/12]**, in which the IPT held that "*the law gives individuals an adequate indication as to the circumstances in which and the conditions upon which the Intelligence Services are entitled to resort to interception, or to make use of intercept*" ([159]) and found no breach of Article 8 or Article 10 ([161]). In *BBW* **[AB/2/20]**, the First Section emphasised that the bulk interception of communications was within the margin of appreciation available to Member States ([314][52]) and affirmed that, save in some limited respects (see below), the s. 8(4) regime was compliant with the ECHR.

97. Critically, and in relation to §122 of Liberty's skeleton argument, it has never been held that bulk interception *per se* violates the Convention, notwithstanding the (inherent) breadth of the material that can be obtained via such a regime. To the contrary, *BBW* rejected the contention that the s. 8 (4) RIPA power was too wide, stating: "*by its very nature a bulk interception regime will allow the authorities a broad discretion to intercept communications and, as such, [the Court] does not consider* ***this fact alone*** *to be fatal to the Article 8 compliance of the section 8(4) regime*" ([338]; emphasis added).

98. Further, the utility of bulk interception powers was the subject of detailed scrutiny by Lord Anderson QC as part of the Bulk Powers Review, who found that there was a proven operational case for the power, which had shown itself to be of "*vital utility*" in various operational contexts, in relation to both "*target discovery*" and "*target development, the triaging of leads and as a basis for disruptive action*". Lord Anderson gave the example of the bulk interception playing an "*important part…in the prevention of*

[52] In this context, the First Section specifically emphasised the role of bulk interception powers in addressing "*the current threats facing many Contracting States (including the scourge of global terrorism and other serious crime, such as drug trafficking, human trafficking, the sexual exploitation of children and cybercrime), advancements in technology which have made it easier for terrorists and criminals to evade detection on the Internet, and the unpredictability of the routes via which electronic communications are transmitted*": [314].

bomb attacks, the rescue of a hostage and the thwarting of numerous cyber-attacks". Crucially, Lord Anderson considered that various suggested alternatives to bulk interception "*fall short of matching the results that can be achieved using the bulk interception capability*" and "*may also be slower, more expensive, **more intrusive** or riskier to life*" (emphasis added): see the extract at Dix 1, §190 **[TB/2/468,** original report at **TB/4/567]**. *BBW* expressly relied on Lord Anderson's QC review[53] in support of its conclusion that the bulk interception regime in s. 8(4) RIPA satisfied the requirements of proportionality: see [384]-[386] **[AB/2/20]**. This is the context against which C's allegations concerning the nature of the interference involved in bulk interception must be analysed: cf. C's skeleton argument, §§121-124.

99. C variously characterises bulk interception *per se* as a "*serious*" interference with private life, correspondence and freedom of expression (skeleton, §121), as interfering "*deeply upon private life*" (ibid, §123) and as involving a "*significant chilling in communications and expression*". However, this fails properly to distinguish between the various stages involved in the process of bulk interception. As the IPT observed in *Liberty IPT* at [62], "*interception can simply comprise the obtaining and recording of a communication (as it is being transmitted), so as to make it available subsequently to be read, looked at or listened to by a person: no one in fact needs actually to have read, looked at or listened to the communication for interception to occur*." And as already noted, the First Section in *BBW* accepted that there will be a "*significantly greater*" interference when material obtained through bulk interception is selected for examination or actually examined by an analyst, even if earlier stages involve an interference with Article 8 rights: see [329] and [338] of *BBW* **[AB/2/20]**.

100. Further, as noted above in relation to bulk equipment interference, it is important to understand the likely duration of the retention of information pursuant to Part 6 Chapter 1 when considering the extent to which there has been any meaningful interference with Convention rights. In that regard, where an individual's information is either discarded in real-time under the 'strong selector' process, or held for a few days at most in a general 'soup' of data as part of the 'complex query' process, and never otherwise examined or used, any interference with Convention rights is – at most – a technical one: see Dix 2, §22 **[TB/2/667]**, and the quotation from §6.6 the Interception of Communications Code **[AB/3/24]**.

101. As with all the other powers under challenge, the question of Convention-compliance will be determined by reference to the adequacy of the safeguards applicable to the various stages of the bulk interception process, and not by reference to high-level considerations of the potential breadth of the information that could in principle be retained under the Part 6 Chapter 1 power.

[53] as well as broadly similar findings made by the 'Venice Commission' on the Democratic Oversight of Signals Intelligence Agencies, as summarised at [211]-[216] of *BBW*. **[AB/2/20]**.

102. It should also be added that C's assertions about the chilling effect of the bulk interception regime on communications and expression (e.g. personal web-browsing habits) are essentially hypothetical and unevidenced (cf. C's skeleton argument, §123). Ds' core submission is that, in the light of the array of safeguards applicable to the Pt 6 Ch 1 regime, any 'chilling' effect of the mere existence of bulk interception powers is likely to be negligible, and in any event vastly outweighed by the proven operational case for such a regime, clearly evidenced in Lord Anderson QC's Bulk Powers Review.

(2) Allegation that the defects found to exist in BBW apply to bulk interception under Part 6 Chapter 1

103. The answer to this part of C's case, in summary, is as follows:

(1) It is against the totality of the safeguards within the scheme (and Article 6), that compatibility with Arts 8 and 10 ECHR falls to be assessed. For that reason, it is not possible simply to transpose the ECtHR's findings in *BBW* across to the new statutory scheme in the Act, as C seeks to do. The new scheme under the Act has features which address the defects found in *BBW*.

(2) The ECtHR's findings in *BBW* concerning oversight of the selection process were based on factual misunderstandings about the nature of the oversight provided (at that time) by the Interception of Communications Commissioner; but more importantly, the oversight of the selection process now provided by the IPC is clearly sufficient to address the ECtHR's concerns in *BBW* (quite aside from the features of the new regime under the Act, alluded to above).

(3) The ECtHR's findings in *BBW* concerning safeguards applicable to the selection of RCD under the s.8(4) Regime cannot be read across to Part 6 Chapter 1 of the Act; and in any event, even if it were possible to read them across as C seeks to do, the Government has committed to putting in place a scheme of thematic certification for the selection of RCD of persons in the British Islands which would address those findings. See the points made at §§69-71 above in relation to Part 6 Chapter 3 of the Act.

(a) Oversight of selection of bearers and selectors / search criteria

Selection of bearers

104. C contends that Part 6 Chapter 1 "*does not regulate the selection of bearers at all*" (skeleton, §129). This is plainly wrong, given the requirement for a bulk interception warrant under s. 136 of the Act, the applicable provisions of the Interception Code **[AB/3/24]** (including a requirement that the warrant application must contain "*a*

description of the communications to be intercepted")[54], and the oversight of both the Judicial Commissioner and the IPC.

105. C's case then moves to the contention that the selection of bearers is subject to the same regulation as it was under RIPA "*save for Judicial Commissioner approval*", and "*this did not prevent a finding of incompatibility due to the absence of oversight of selection of bearers*" (skeleton, §129(1)). As to that argument:

(1) C misreads the judgment in *BBW* [**AB/2/20**]. The ECtHR found that it would be "*desirable for the criteria for selecting the bearers to be subject to greater oversight by the [IPC]*" ([338]). But it did not consider "*this fact alone*" to be fatal to the compliance of the regime, having regard to the lesser seriousness of the interference with ECHR rights that occurs at the 'selection of bearers' stage, as opposed to selection for examination.

(2) C's passing reference to "Judicial Commissioner approval" fails to afford proper significance to one of the key features of the bulk interception regime in Part 6 Chapter 1 of the Act which distinguishes it from the s. 8(4) regime, and which renders it impossible to transpose the ECtHR's conclusions in relation to the latter into equivalent conclusions in relation to the former. The fact that Judicial Commissioner approval is required for a warrant under Part 6 Chapter 1, and that the Judicial Commissioner must be provided with the same material as the Secretary of State issuing the warrant, means that the Judicial Commissioner will be provided with information about what communications service provider's bearers it is intended to intercept, and why. That is, precisely, independent oversight of bearer selection.

(3) The selection of bearers is also subject to the provisions of §6.10 of the Interception Code, which requires the Intelligence Services to select them for interception on the basis of regular surveys of those bearers most likely to contain overseas-related communications, relevant to the operational purposes specified in the warrant[55].

(4) The First Section in *BBW* did not appear to appreciate that the Interception of Communications Commissioner's powers and functions gave him "end to end" oversight of the entire process of interception, from selection of bearers to destruction of intercept material (see e.g. the 2014 Annual Report of the

[54] See Interception Code of Practice, §6.20(b) [**AB/3/24**]

[55] *"When conducting bulk interception, an intercepting authority must use its knowledge of the way in which international communications are routed, combined with regular surveys of relevant communications links, to identify those individual communications links that are most likely to contain overseas-related communications, which will be relevant to the operational purposes specified on a warrant. This is likely to be a dynamic process due to regular fluctuations in the way data routes across the internet. The intercepting authority must also conduct the interception in ways that limit the interception of communications or secondary data that are not overseas-related to the minimum level compatible with the objective of intercepting the required overseas-related content."*

Interception of Communications Commissioner at §§6.54-6.59 **[TB/3/381]**, and the Interception of Communications Commissioner's own description of his role in overseeing bearer selection at §6.80 of his 2015 Annual Report.) In any event, however, it is clear not only that the IPC's functions under s.229 of the Act give him oversight of bearer selection; but also that his greater resources and powers give him an advantage in this respect over the oversight abilities of the bodies he replaced, including the Interception of Communications Commissioner.

106. As to §129(2) of C's skeleton argument, the contention that the position under the Act is worse than under RIPA (because s. 136(2) requires only that the "*main purpose*" of a bulk interception warrant is the "*interception of overseas-related communications*" or the obtaining of secondary data therefrom, in contrast to the restriction of bulk interception to "*external communications*" under a RIPA warrant) is wrong. Under s. 5(6)(a) of RIPA, the conduct authorised by an interception warrant in relation to "*external communications*" expressly includes "*all such conduct (including interception of communications not identified by the warrant) as it is necessary to undertake in order to do what is expressly authorised or required by the warrant*". Thus, <u>where necessary</u>, non-external communications could be obtained pursuant to a RIPA warrant. This did not trouble the First Section in *BBW* **[AB/2/20]**. Similarly, a warrant under s. 136 of the Act <u>may</u> cover communications that are not overseas-related, but only in the context of the <u>main</u> purpose of the warrant being confined to obtaining overseas-related communications. The position in this limited respect is, therefore, in substance no different under Part 6 Chapter 1 of the Act as under RIPA. Moreover, the fact that the position is exactly the same under RIPA and the Act in this regard is made explicit by the Interception Code. The Interception Code states at §6.9 **[AB/3/24]** that "*a bulk warrant authorises the interception of communications that are not overseas-related <u>to the extent that it is necessary in order to intercept the overseas-related communications to which the warrant relates</u>*" (emphasis added). It also states at §6.20 (addressing warrant applications) that each application must contain "*(c) [a] description of the conduct to be authorised, which must be restricted to the interception of overseas-related communications, the obtaining of secondary data from such communications, and the conduct (including the interception of other communications not specifically identified by the warrant as set out at section 136(5)) it is necessary to undertake in order to carry out what is authorised or required by the warrant*".

107. When that position is put together with the fact that the definition of "*overseas-related communications*" is narrower than the definition of "*external communications*" in RIPA[56], the true position is that the Act is in this respect too <u>more</u> protective of

[56] Under RIPA, an "*external communication*" was defined by s.20 as "*a communication sent or received outside the British Islands*". Under Part 6 Chapter 1 of the Act **[AB/1/2]**, by s.136(3) of the Act, "*overseas-related communications*" means "*(a) communications sent by individuals who are outside the British Islands, or (b) communications received by individuals who are outside the British Islands.*"
The use of the phrases "*sent by individuals*" and "*received by individuals*" in s.136(3) represents a deliberate narrowing of the definition of communications that a bulk warrant is intended to capture. In the course of *Liberty IPT* **[AB/2/12]**, the Government's witness Charles Farr explained that "*external*

individuals' rights than RIPA. In any event, it is by reference to the entire system of safeguards applicable to the selection of bearers under Part 6 Chapter 1 of the Act that its Convention-compliance must be ascertained. Any definitional change in relation to the permissible subject matter of a warrant would not mean that the very substantial additional new safeguards, not least independent Judicial Commissioner approval, should be ignored: see further DGR §73 **[TB/2/378]**.

108. Finally, C is wrong to say (skeleton, §129(3)) that the new "*operational purposes*" requirement under the Act – which was not present in RIPA - is a safeguard irrelevant to the first stage of selection of bearers. A bulk interception warrant "*must specify the operational purposes for which any intercepted content or secondary data obtained under the warrant may be selected for examination*" (s. 142(3)). Those operational purposes must be specified, in the central list of such purposes, "*in a greater level of detail than the descriptions contained in section 138(1)(b) or (2)*". This plainly constrains the circumstances in which a warrant in respect of the interception of content / secondary data carried by given bearers may be approved: if there are no operational purposes in respect of which the Secretary of State is satisfied that intercept material may proportionately be obtained from bearers carrying communications of the CSP to whom the warrant is addressed, then a warrant cannot be issued at all.

Selectors / search criteria

109. Several of the same points made above in relation to the selection of bearers also apply to C's arguments under this head:

(1) The ECtHR's findings at [340] and [347] of *BBW* were based on its understanding that the Interception of Communications Commissioner did not, in practice, provide meaningful independent oversight of selectors and search criteria. That conclusion, which was based on the findings of the ISC in its 2015 Report ("*Privacy and Security: A Modern and Transparent Legal Framework*") **[TB/3/193]**, did not properly appreciate the Interception of Communications Commissioner's changes to his own practice, to provide such oversight, as referred to in his 2013 Annual Report at p.58 (**[TB/3/112]**), and his summary of his own oversight processes at

communications" would include a communication between a person and a thing (for example, a server located outside the UK). So where a person in the British Islands, for example, undertook a Google search, which was in substance a communication between their device and Google's servers located in the USA, that was an "*external communication*" for the purposes of Chapter 1 Part 1 RIPA. The breadth of the definition of "*external communication*" was one of the matters about which C most particularly complained in *Liberty IPT*, albeit that the IPT rejected that complaint: see the 5 December 2014 Judgment at [93]-[102]. The position has now been changed by s.136(3) of the Act. The fact that an "*overseas-related communication*" must be sent or received by an individual outside the British Islands means that a communication between an individual in the British Islands and a server outside the British Islands would not fall within the definition – Google searches and the like by persons within the British Islands are not "*overseas-related communications*".

§6.37 of his 2014 Report[57] **[TB/3/375]**. But in any case, it is plain that the IPC does have such oversight. That follows not only from his power to oversee the whole interception process under s.229 of the Act, and from his increased powers and resources by comparison to the oversight bodies he replaced, but also from the specific terms of Ds' letter of 10 December 2018 to the IPC ([**TB/2/345**])[58].

(2) As indicated in Ds' letter of 10 December 2018, the new statutory requirement of operational purposes is an important constraint on selectors/search criteria. It means that selectors/search criteria must be justified not only by reference to their necessity and proportionality for the statutory purposes in s.138 of the Act, but also by reference to the specificity of the operational purposes on the list maintained by the heads of the Intelligence Services under s.142 of the Act.

(3) Further, the compatibility of the system needs to be assessed as a whole, by reference to all its applicable safeguards, including those not in place under RIPA, such as the requirement for Judicial Commissioner approval of interception warrants, and the increased role played by the Courts in post hoc oversight (given the new statutory route of appeal from the IPT).

---

[57] The Edward Snowden allegations, which prompted the ISC's 2015 Review, also prompted the Interception of Communications Commissioner (at that time, Sir Peter May) to investigate the operation of the bulk interception regime under s.8(4) RIPA in detail, which he did in his 2013 Annual Report, published on 4 May 2014. As may be seen from p.58 of his 2013 Report **[TB/3/112]**, one of the matters that the Commissioner wished to investigate further was precisely the operation of selectors/search terms. He stated:
"(3) I need to undertake further detailed investigation into the actual application of individual selection criteria from stored selected material initially derived from section 8(4) interception. I have had this fully explained and even demonstrated to me. But I am currently short of sufficient detailed material necessary to make a full structural analysis and assessment of the internal process. Time has not permitted me to undertake this inquiry before writing this report."
That inquiry was subsequently built into the Commissioner's processes. The Commissioner stated in his 2014 Annual Report, published in May 2015, that he had conducted the full structural analysis to which the 2013 Annual Report referred, and said at §6.37 **[TB/3/375]**:
"In 2014 my office carried out the further investigations into the actual application of individual selection criteria…and in particular reviewed the breadth and depth of the internal procedures for the selection of material to ensure that they were sufficiently strong in all respects. These investigations, which focused on GCHQ as the interception agency that makes the most use of section 8(4) warrants and selection criteria, addressed in good detail the selection criteria and related matters."

[58] In that letter the Ds began by observing that the new requirement in the Act that selection for examination be limited by reference to "operational purposes" was an important additional safeguard, and continued:
"*In relation to the oversight of selectors specifically, this now sits within scope of your main oversight functions in the IP Act: as part of the requirement that you keep under review the exercise by public authorities of statutory functions relating to the interception of communications. Furthermore, the investigation and information powers that you have been granted under the IP Act enable you to require the provision of any information from public authorities that you may require in exercising your functions, including in relation to selectors.*
These factors, taken together, respond substantively to this violation. Nevertheless, in order to assist your oversight in this area our officials and those from the intelligence services, GCHQ in particular, have committed to work with your office to establish how the oversight of selectors could be enhanced and how this would be best taken forward in practice."

110. As to §131(3) of C's skeleton argument, there is indeed no meaningful substantive difference between s. 16(4)(a) of RIPA and s. 152(3)(b) of the Act, notwithstanding the removal of the language of "*reasonable grounds*". What is required under s. 152(3)(b) is that the person to whom the warrant is addressed considers that the selection of intercepted content for examination does not breach the prohibition in s. 152(4) of the Act on selection criteria that are referable to an individual known to be in the British Islands at that time. In public law, there must be a reasonable basis for the belief of the person to whom the warrant is addressed that the prohibition in s. 152(4) would not be breached by selection for examination, whether or not the statute expressly so provides. C's counter-example at §131(3)(a) of its skeleton argument (a case in which there is a complete absence of information about an individual) does not demonstrate that the protections under this aspect of the Act are less exacting than under the equivalent provisions of RIPA. If the addressee of the warrant had no information at all about an individual, it is not understood how s/he could rationally form the view that the criteria used for the selection of the relevant intercepted content are not "*referable to an individual known to be in the British Islands at the time*": s. 152(4)(a) of the Act.

111. As to §131(3)(c) of C's skeleton argument, which reiterates a contention from SFG §113, the Secretary of State is required by the Act to ensure that, to such extent as he considers appropriate (i) arrangements are in force for securing that any material is handed to overseas authorities only where it appears to the Secretary of State that safeguards corresponding to those in the Act will apply, to the extent that the Secretary of State considers appropriate; and (ii) restrictions are in place to prevent 'prohibited disclosures' taking place overseas (i.e. a disclosure that would breach the prohibition in s. 56(1) concerning the exclusion of evidence from legal proceedings): see s. 151(2)(a) of the Act and §§9.26-9.29 of the Interception Code of Practice **[AB/3/24]**. This is not a wider discretion to disapply arrangements relating to disclosure/copying and retention than applied under RIPA, but a narrower one. Nothing in RIPA empowered the Secretary of State to ensure that any overseas authority to which material was disclosed applied the safeguards in s.16 RIPA (or their equivalent). By contrast, under the Act, the Secretary of State may, where he considers it appropriate, make authorisation of disclosure to an overseas authority conditional on the "British Islands" safeguard being in place and persisting thereafter.

112. As to §131(3)(d) of C's skeleton argument, concerning the effect of s. 225 of the Act in permitting disapplication of the safeguards in ss.150 and 152 of the Act, see above at §§18(2), 74 and 80.

113. As to §131(4) of C's skeleton argument, C simply ignores the description at DGR §73(2) **[TB/2/378]** of the greatly increased resources of the IPC, which plainly facilitate greater oversight, including of the selectors / search criteria stage; and ignores, too, the fact that he heads a cadre of Judicial Commissioners whose

independent prior approval is required for the exercise of various powers under the Act. Importantly, and at the risk of over-repetition, this is again just one aspect of the overall system of applicable safeguards: but the compliance of Part 6 Chapter 1 with the Convention needs to be considered holistically. The fact that a particular aspect of the statutory regime is broadly equivalent to that under RIPA is by the by: it is the adequacy of the regime as a whole that needs to be considered.

114. Finally, as to §§133-135 of C's skeleton argument, Ds do not repeat the points already made in relation to the effect of s. 225 of the Act: see §18(2) above. The critical point is that while s. 225 does indeed give a discretion to disapply safeguards that apply under Part 6 Chapter 1 (and other Parts of the Act which give a power to obtain content or communications data), the effect of such disapplication is that a <u>different</u> set of safeguards under Part 7 applies. Further, a critical safeguard applies right at the outset of the disapplication process, with the requirement for Judicial Commissioner approval where the Secretary of State wishes to give a direction under s. 225(3): see s. 225(7). C's skeleton argument ignores this safeguard, and maintains its earlier, and wrong, contention that the Secretary of State has a "*near complete discretion*" when giving a direction under s. 225 of the Act.

115. For the reasons given above, C is wrong to suggest that the Part 6 Chapter 1 regime is vitiated by the same defects in relation to the various stages of the bulk interception regime as identified by the First Section of the ECtHR in *BBW*. Considered as a whole, the regime affords very substantially increased protection to individual privacy and free expression rights, and there is no basis for a finding of a violation of the ECHR on the grounds that the regime is not "*in accordance with the law*".[59]

<u>(b) Power to derive and use secondary data</u>

116. C's second argument by reference to the decision in *BBW* is that the findings of the First Section in relation to related communications data ("**RCD**") can similarly be read across to a finding that the provisions of Pt 6 Ch 1 on "secondary data" are not in accordance with the law.

117. It is accepted that the safeguard on selection for examination of communications of persons outside the British Islands in s. 153(5) of the Act applies only to content, and not secondary data. However, *contra* the suggestion at §137 of C's skeleton argument, it does not follow that the argument in respect of the Act is "*a fortiori that which succeeded in BBW in respect of RIPA*". Again, it is essential to bear in mind that Convention compliance is a matter that must be addressed by a reference to the overall schema of safeguards that applies to secondary data, and not merely by taking a single deficiency identified by the ECtHR in relation to the earlier bulk

[59] Unsurprisingly, given the findings of the First Section in *BBW* at §§384-386 **[AB/2/20]** in relation to the proportionality of the bulk interception regime, Liberty advances no free-standing proportionality argument in relation to Pt 6 Ch 1.

interception regime and assuming that the same issue renders the new regime unlawful.

118. Ds' basic position on this aspect of the case is set out at DGR §§78(5)-(7) **[TB/2/381]**. C seeks to answer Ds' arguments at §§140 *et seq* of its skeleton argument. In response:

(1) C seeks to downplay the significance of the operational purposes requirement as a constraint on the selection for examination of secondary data. But, for reasons explained elsewhere in this skeleton argument and in the DGR and supporting evidence filed by Ds, this is indeed an important and robust new safeguard. The breadth of the definition of secondary data does not detract from the significance of the safeguard, since it is only where selection for examination is carried out pursuant to the specified operational purposes that any secondary data may actually be examined.

(2) C seeks to address Ds' contention (DGR §78(5)) that the examination of secondary data is, in general, less invasive of privacy than the examination of content. It does so in two stages:

i. C contends, first, that the definition of secondary data in s. 137(4)-(5) of the Act does not exclude content. This is a mistake, and ignores DGR §78(6) at which this point is addressed.[60] Pursuant to s. 137(4)-(6) of the Act, secondary data must be either "*systems data which is comprised in, included as part of, attached to or logically associated with the communication (whether by the sender or otherwise)*" or "*identifying data*" which is (inter alia) capable of being logically separated from the remainder of the communication with which it is associated and, if it were so separated, "*would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication*". But in that regard: (a) as C itself recognises (at footnote 62 of its skeleton), "*systems data*" cannot be content, given the express exclusion of systems data from the definition of content in s. 261(6)(b); and (b) since "*identifying data*" can only be "*secondary data*" if, when separated from the associated communication, it would not reveal anything of what might reasonably be considered to be the meaning of that communication, it is inconceivable that this variety of secondary data could include content, let alone "*the most sensitive content*" (*pace* C's skeleton, §141(1)). To the contrary, this definition of secondary data is deliberately designed to mesh with, and mutually to exclude, the definition of "*content*" in s. 261(6) of the Act. It is therefore not understood why C has formed the view that secondary data may include content. As a matter of deliberate statutory design, content is precisely what secondary data is not.

[60] It also ignores Dix 1 §203 **[TB/2/473]**, in which an equivalent error by Liberty's witness, Professor Danezis is corrected.

ii. Next, C notes the recognition in *BBW* at [356] that the acquisition of RCD is not necessarily less intrusive than the acquisition of content. But Ds have always accepted that the acquisition of secondary data (the broad equivalent of RCD under the Act) is not necessarily less intrusive than the acquisition of content. Their point has always been rather that this is "*a general rule*", and that the examination of the most sensitive content will always raise greater privacy concerns than the examination of any secondary data: DGR, §78(5). This has been recognised by the ECtHR itself (e.g. in *Malone* at [84] **[AB/5/49]**), and is an important factor when considering the adequacy of the safeguards relating to the bulk interception of secondary data. See further §§120-125 below. None of which is to suggest that, in particular cases, secondary data may not reveal sensitive information about an individual.

(3) At §142 of its skeleton argument, C addresses DGR §78(7) **[TB/2/381]**. In response

i. The various points at §142(1) of C's skeleton argument are hard to follow. The short point is that, if content needs to be examined in order to extract secondary data, then the full safeguards applicable to the examination of content will apply. Accordingly, the width of the definition of secondary data, the possibility of automated analysis, and so on, are of limited relevance. See generally Dix 1, §§203-205 **[TB/2/473]**.

ii. As to §142(2) of C's skeleton argument, it is true that the requirement of being separable from meaning does not apply to systems data under s. 137(4). But systems data has a constrictive statutory definition of its own in s. 263(4) of the Act, and moreover (as set out above, and as C itself recognises at footnote 62) content is defined so as expressly to exclude systems data: s. 261(6)(b) of the Act.

iii. As to §142(3) of its skeleton argument, C simply omits to refer to all the safeguards that do apply at the 'pre-examination' stages of the process, i.e. the warrantry provisions (including the requirement for Judicial Commissioner authorisation), and the need to specify operational purposes in a warrant, as well as the *ex post* safeguards of IPC and IPT oversight. Taken as a whole, there is patently an adequate array of safeguards in relation to the acquisition, retention and examination of secondary data.

119. The concluding remarks at §143 of C's skeleton argument in relation to bulk interception – which draw an implicit comparison between the provisions of Part 6 Chapter 1 and the placing of a continuously recording camera and microphone in everyone's home – represent precisely the kind of inaccurate and hyperbolic submission rejected in *Privacy IPT* at [72] **[AB/2/17]**, where the Government's approach

was described as an attempt to "*obtain data wholesale from every living human being with a working internet connection*".

E. Challenge to the powers relating to communications data – Part 6 Chapter 2 and Parts 3 - 4

(1) Nature of the interference

120. Communications data ("**CD**") is to be distinguished from the content of a communication. While it is defined in precise terms in s. 261(5) of the Act, CD essentially constitutes data that enables the intelligence agencies to understand matters such as "*who has been communicating with whom, and where from, as [opposed to] what the parties actually said to one another*"[61].

121. The ability of the intelligence agencies to acquire CD in bulk under Part 6, Chapter 2, and then select data for examination for a specified operational purposes, is an important intelligence-gathering tool, allowing the agencies to work at pace to detect and disrupt threats to the UK. It is used to identify subjects of interest within the UK and overseas, and to understand relationships between suspects, in a way that would not be possible using 'targeted' methods. In the Bulk Powers Review, Lord Anderson QC found that there was a "*proven operational case*" for the bulk acquisition of CD and concluded that **[TB/4/578]**:

> "*(a) Bulk acquisition has been demonstrated to be crucial in a variety of fields, including counter-terrorism, counter-espionage and counter-proliferation. The case studies provide examples in which bulk acquisition has contributed significantly to the disruption of terrorist operations and, [through] that disruption, almost certainly the saving of lives.*
>
> *(b) Bulk acquisition is valuable as a basis for action in the face of imminent threat, though its principal utility lies in swift target identification and development.*
>
> *(c) The SIAs' ability to interrogate the aggregated data obtained through bulk acquisition cannot, at least with currently available technology, be matched through the use of data obtained by targeted means.*
>
> *(d) Even where alternatives might be available, they are frequently more intrusive than the use of bulk acquisition*."

122. That is the essential context against which the proportionality of any interference with privacy arising from the acquisition, and subsequent retention / examination, of CD must be analysed.

[61] See A Question of Trust, §5.26 [**TB/3/528**]

123. More generally, and in relation both to Part 6 Chapter 2 and Parts 3 and 4 of the Act, the acquisition of (and subsequent examination of) CD can involve an interference with the privacy of users of communications services (although it will never reveal the content of users' communications). It is, however, important to note that CD is generally less intrusive than the content of communications: other things being equal, an intelligence analyst seeing information as to the telephone number from which a text message was sent will involve a lesser interference with privacy than the same analyst reading the text message itself.

124. C contends that this analysis of the distinction between CD and content is "*flawed*" (skeleton, §147). However, none of the reasons advanced by C undermines the contention that CD is as a general rule less intrusive than content:

(1) C contends that the claim is contrary to "*high authority*" (skeleton, §147(1)). However, the authorities cited (*Digital Rights Ireland* **[AB/5/72]** and *BBW* **[AB/2/20]**) do not cast doubt on, let alone dismiss, the general proposition advanced by Ds as to the relative intrusiveness of CD and content:

i. As is apparent from the quotation from *Digital Rights Ireland* at §147(1) of C's skeleton argument, the CJEU simply recognised that, in particular cases, CD "*may*" allow a greater understanding of individuals' private lives. Ds do not suggest otherwise. In particular cases, CD may indeed facilitate such an understanding, which is part of the reason why CD is of such value for the intelligence agencies[62].

ii. The reference to [356] of *BBW* is misleading. There, the ECtHR did not accept that the acquisition of "related" CD is "***necessarily*** *less intrusive than the acquisition of content*" (emphasis added), e.g. because the content of an electronic communication might be encrypted whereas the related CD might reveal the identity and location of the sender. Again, Ds do not suggest otherwise. It does not follow – and the First Section did not suggest – that CD is not *generally* less intrusive than content, even if that is not "*necessarily*" the case.

(2) C contends that the general proposition is "*contrary to the careful findings of the ISC*" in its March 2015 report *Privacy and Security: A modern and transparent legal framework*. However, C's quotation from that report (see skeleton, §147(2)) is incomplete:

i. C omits the immediately preceding quotation from the report, where the ISC expressly recognised that "*while the volume of Communications Data available has*

[62] More recently, in *Ministerio Fiscal C-207/16* [2019] 1 WLR 3121 **[AB/5/74]**, the Grand Chamber of the CJEU has confirmed that the threshold that acquisition of communications data should be for "serious crime" does not even apply to the acquisition of the least intrusive communications data (which can properly be justified on grounds of "crime", whether or not it is serious).

made it possible to build a richer picture of an individual, this remains ***considerably less intrusive than content***" (emphasis added) **[TB/3/250]**.

ii. The ISC did indeed recognise that "*certain categories*" of CD do have the potential to reveal more intrusive information about a person's private life, as the quotation extracted by C from its report shows. But C does not provide the complete quotation, the final sentence of which reads (in full): "This category of information requires greater safeguards ***than the basic 'who, when and where' of a communication***" (words omitted by C emphasised) **[TB/3/250]**. In other words, the ISC was not suggesting that CD generally requires "*greater safeguards*" than content. It was making a narrower point, that certain types of CD require more protection than CD generally, given that (as the ISC observes immediately beforehand) the latter is "*considerably less intrusive than content*".

(3) C refers to differences in the speed and ease with which information from CD can be extracted (skeleton, §147(3)). This is a matter that is relevant to the operational utility of CD. But, in and of itself, it tells one nothing about the intrusiveness of the information concerned.

125. Accordingly, and *contra* the suggestion at §148 of C's skeleton argument, the distinction between the content of the most personal communications and CD generally is not illusory. It reflects a view shared by the ISC. Nor is the distinction "*irrelevant*". When considering the proportionality of the system of safeguards that applies to CD, it is plainly relevant to have regard to the lesser overall degree of intrusion into individual privacy that will likely result from the acquisition (and retention / examination) of such data.

126. In any event, as set out in the DGR and further below, a robust system of safeguards applies to the bulk acquisition of CD under the Act, which in its essential respects is identical to the system of safeguards that applies to powers concerning the bulk acquisition of content. Accordingly, even if successful, C's attempt to equate the intrusiveness resulting from the bulk acquisition of CD with that resulting from the bulk acquisition of content, gets C nowhere.

(2) Allegedly disproportionate power / failure to require reasonable suspicion and individual targeting at all stages

127. In light of the decision in *BBW*, C no longer pursues the claim that bulk acquisition is incompatible with the ECHR per se, or that the Part 6 Chapter 2 regime is unlawful in the absence of provision for reasonable suspicion and individual targeting: see C's skeleton argument, §149.

(3) Allegation that the defects found to exist in BBW apply to bulk acquisition under Part 6 Ch 2

Alleged absence of oversight of search criteria

128. As to §151 of C's skeleton argument, the starting point in assessing the alleged absence of oversight relating to search criteria is that Convention compliance needs to be considered in the round, by reference the full plethora of safeguards that apply to the bulk acquisition of CD under Part 6 Chapter 2 of the Act. C's narrow focus on the oversight of search criteria should not obscure the very substantial protections that apply to CD more generally, e.g. the 'double-lock' process for the authorisation of bulk acquisition warrants, and the provisions relating to operational purposes (which provide a real constraint on selection for examination, i.e. the point at which CD may actually be looked at by an analyst).

129. In any event, the points at §§151(1)-(5) of C's skeleton argument, which are effectively recycled from allegations made earlier in C's skeleton argument in relation to other provisions of the Act, are without foundation. Taking them in turn:

(1) As to §151(1) of C's skeleton, §109 above is repeated. The IPC does have effective independent oversight of search criteria; and in any event, the regime as a whole provides sufficient safeguards against abuse for the reasons set out above, which are repeated in this context *mutatis mutandis*.

(2) As to §151(2) of C's skeleton, which relates to protection for persons in the British Islands, see §§130-134 below.

(3) As to §151(3) of C's skeleton, which concerns the Secretary of State's alleged "*discretion*" to disapply safeguards when material[63] is provided to overseas authorities, see §111 above.

(4) As to §151(4) of C's skeleton, the requirement that selection for examination be for operational purposes only is indeed a real constraint in relation to CD, just as it is in relation to other information acquired under the Act. See §§87 and 108 above.

(5) As to §151(5) of Liberty's skeleton, concerning the IPC, see §§24 and 109 above.

Absence of British Islands safeguard

[63] §151(3) of Liberty's skeleton argument refers to intercept material, but this should presumably be a reference to CD.

130. It is correct that Part 6 Chapter 2 of the Act does not include any express provision restricting the exercise of the bulk acquisition power in the case of persons known to be in the British Islands. Indeed, Part 6 Chapter 2 explicitly authorises the obtaining of domestic CD in bulk: that is part of its purpose. But it simply does not follow that the findings in relation to RCD in *BBW* **[AB/2/20]**, relating to the absence of a "British Island safeguard" for RCD intercepted pursuant to the bulk interception regime under RIPA, can be read across to the different regime for bulk acquisition of CD under the Act[64].

131. *First,* the power under Part 6 Chapter 2 is not an analogue of the bulk interception power under s.8(4) RIPA at all. It replaces the (much less tightly defined and rigorous) previous regime for the bulk acquisition of communications data under s.94 Telecommunications Act 1984 **[AB/6/76]**, which itself included no "British Islands safeguard". The lawfulness of that regime was considered in detail by the IPT in *Privacy IPT* **AB/2/17]**, which found in its judgment of October 2016 that (subject to an issue of transfer of data) the regime was in accordance with the law after 4 November 2015 (see [85]-[101] of the judgment).

132. *Secondly,* the reasoning of the First Section in *BBW* concerning the need to apply a "British Islands safeguard" to RCD turned entirely upon the fact that such a protection was applied to content, but not to RCD, under the s.8(4) Regime. The Court's logic was not that any CD regime would necessarily require a "British Islands safeguard", or the equivalent; its reasoning was simply that it was unjustified to exempt RCD in its entirety from safeguards applied to the searching and examining of content under the same regime. See *BBW* [352]-[357]. For that reason, too, the reasoning in *BBW* cannot simply be transposed to CD under Part 6 Chapter 2, which is a self-contained regime for the acquisition of CD (only).

133. *Thirdly,* Part 6 Chapter 2 contains a panoply of protections, over and above those applicable to RCD under RIPA, including specific protections relating to the searching and examining of CD, which together ensure the compliance of the provisions concerned:

(1) A bulk acquisition warrant must now specify not only the statutory grounds for which the warrant is necessary (s. 158(1) of the Act), but also the operational purposes for which any CD acquired under the warrant may be selected for examination: s. 161(3) of the Act. As with the various other bulk powers, those operational purposes must appear in a central list maintained by the Heads of the Intelligence Services and approved by the Secretary of State, be specified in "*greater*

[64] This point is made without prejudice to the observations at §70 above as to (i) what the First Section in *BBW* actually meant by a "British Islands Safeguard", and (ii) the impossibility of applying exactly the same "British Islands Safeguard" to intercepted content, and to intercepted communications data.

detail" than the statutory purposes themselves, and that list is subject to regular review by the ISC and the Prime Minister: s. 161(4)-(10) of the Act.

(2) In distinction to the position relating to RCD under RIPA, a bulk acquisition warrant must now be approved by a Judicial Commissioner (a senior judge[65]): s. 159 of the Act. The Judicial Commissioner will have access to the same detailed information as the Secretary of State when considering a warrant application (including the information that the Code of Practice requires). (Further information as to the Judicial Commissioner approval process is set out at DGR §72(4) **[TB/2/377]**).

(3) Further detailed provision as to the content of an application for a bulk acquisition warrant is set out in the Bulk Acquisition Code at §§4.5(a)-(i) **[AB/3/25]**.

(4) The purposes for which a bulk acquisition warrant can be issued (see s. 158(1)(a) and (2) of the Act) are narrower than the purposes for which a s. 8 (4) warrant under RIPA could be issued. In this regard, the position under Part 6 Chapter 2 is equivalent to the position relating to bulk interception warrants under Part 6 Chapter 1: see DGR §72(3) **[TB/2/377]**.

(5) Importantly, selection for examination may only be carried out for one or more of the operational purposes specified on the warrant: s.172(1) and (2) of the Act. Further, the Code provides that in general, automated systems should wherever possible be used to effect selection for examination for those purposes: Code, §6.12 **[AB/3/25]**.

(6) The Bulk Acquisition Code requires arrangements to be put in place for the creation and retention (for the purposes of subsequent examination or audit) of documentation outlining why access to the data by authorised persons is necessary and proportionate, and what are the applicable operational purposes for which it is required. That documentation must be available for review by the IPC, in the exercise of his oversight powers under s.229 of the Act: see e.g. Code, §6.15. (It should be noted that there was no equivalent Code applicable to the exercise of the power under s.94 Telecommunications Act 1984 at all, and no statutory system of oversight: see e.g. *Privacy IPT* (October 2016) at [72]-[80] **[AB/2/17]**).

(7) The Bulk Acquisition Code, and s.2 of the Act, also require due regard to be given to whether the level of protection applied in relation both to the acquisition of CD and to its selection for examination is sufficient, in light of any circumstances that might lead to an unusual degree of intrusion or infringement of rights and freedoms, particularly regarding privacy and, where it might be engaged, freedom

[65] The requirements for appointment as a Judicial Commissioner are set out in s. 227(1) of the Act. The 16 currently appointed Judicial Commissioners are all current or recently retired High Court, Court of Appeal and Supreme Court judges.

of expression. See Code, §§6.20-6.32. Those protections include specific provisions in the Code concerning sources of journalistic information (see Code, §§6.24-6.32, and see further below as concerns journalistic information generally); but they are not limited to journalistic information. See in particular §§6.20-6.23 of the Code[66].

134. In the light of the substantial additional protection afforded to CD acquired in bulk under the Act, and for the other reasons set out above, the absence of a discrete British Islands safeguard does not give rise to a contravention of the ECHR.

(4) Alleged failure to comply with minimum safeguards

135. For the reasons given above at §32, the *Weber* minimum safeguards approach does not apply to CD. Ds' response to §§157-162 of C's skeleton argument is without prejudice to that submission.

136. As to §159(1)-(2) of C's skeleton argument, Ds rely on the reasoning in *Privacy IPT* **[AB/2/17]** and *Liberty IPT* **[AB/2/12]** and not solely their precedential value. The fact that those cases are concerned with predecessor regimes does not assist C: the relevant precursor regimes included substantially lesser safeguards than Part 6 Chapter 2, and yet they were held to pass muster for ECHR purposes.

137. As to §159(3) of C's skeleton and the "*sharing of datasets with foreign states*":

(1) The Intelligence Services have power to provide information to others in relation to their functions pursuant to the Security Service Act 1989 **[AB/6/78]**, the

[66] See for example §6.22-6.23:
"…officers, giving special consideration to necessity and proportionality, must take into account any such circumstances that might lead to an unusual degree of intrusion or infringement of rights and freedoms, particularly regarding privacy and, where it might be engaged, freedom of expression. Particular care must be taken when considering whether data should be selected for examination in such circumstances, including additional consideration of whether there might be unintended consequences of such examination and whether the public interest is best served by the data being selected for examination.
The nature of bulk data means that in many cases, the authorised person will not know who the communications data relates to at the pint of its selection for examination. However, authorised persons must consider any additional sensitivities in all cases where it is intended or known that the data being selected for examination includes communications data of those known to be in such professions, including medical doctors, lawyers, journalists, Members of Parliament, or ministers of religion."

Intelligence Services Act 1994 **[AB/6/79]**, and s.19 Counter-Terrorism Act 2008[67] **[AB/6/81]**. Section 158(6)(a)(iii) of the Act is not relevant to this issue[68].

(2) There are specific statutory safeguards governing the provision to overseas authorities of CD acquired under Part 6 Chapter 2. In particular, by s.171(9) of the Act, the Secretary of State must ensure that arrangements are in force for securing that CD is handed over or given to an overseas authority only if the Secretary of State considers that requirements corresponding to the requirements of s.171(2)[69], s.171(5)[70] and s.172[71] will apply to it, to such extent as he considers appropriate.

---

[67] See in particular:

(1) s.1 Intelligence Services Act 1994 in relation to the Secret Intelligence Service (*"(1) There shall continue to be a Secret Intelligence Service…under the authority of the Secretary of State; and, subject to subsection (2) below, its functions shall be – (a) to obtain and provide information relating to the actions or intentions of persons outside the British Islands…"* See also 2(2)(a) of the 1994 Act in relation to the responsibilities of the Director-General concerning disclosure of information.

(2) In relation to GCHQ, s.3(1)(a) Intelligence Services Act 1994 (*"(1) There shall continue to be a Government Communications Headquarters under the authority of the Secretary of State; and, subject to subsection (2) below, its functions shall be – (a) to monitor, make use of 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…"*. See also s.4(2)(a) of the 1994 Act in relation to the responsibilities of the Director-General concerning disclosure of information.

(3) In the case of the Security Service, see s.2(2)(a) in relation to the responsibilities of the Director-General concerning disclosure of information.

(4) In relation to all 3 of the Intelligence Services, subsections 19(3)-(5) Counter-Terrorism Act 2008: *"(3) Information obtained by the Security Service for the purposes of any of its functions may 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.

(4) Information obtained by the Secret Intelligence Service for the purposes of any of its functions may 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 purposes of the prevention or detection of serious crime, or
d. for the purposes of any criminal proceedings.

(5) Information obtained by GCHQ for the purposes of any of its functions may be disclosed by it -

a. for the purpose of the proper discharge of its functions, or
b. for the purpose of any criminal proceedings."

[68] Section 158(6)(a)(iii) of the Act essentially relates to the disclosure by the CSP obtaining information pursuant to the warrant to the Intelligence Service to whom the warrant is addressed. It does not concern disclosure by the Intelligence Services of material obtained under the warrant relating e.g. to the sharing of datasets with foreign states.

[69] S.171(2) requires that the number of persons to whom any of the data is disclosed or otherwise made available, the extent to which any of the data is disclosed or otherwise made available, the extent to which the data is copied, and the number of copies that are made are limited to the minimum necessary for the authorized purposes set out in s.171(3).

[70] S.171(5) requires that every copy made of data obtained under the warrant (if not destroyed earlier) is destroyed as soon as there are no longer any relevant grounds for retaining it (as defined in s.171(6)).

[71] Section 172 requires that any selection of data for examination is carried out only insofar as necessary for operational purposes specified in the warrant at the time of the selection of the data for examination, and is necessary and proportionate for those purposes.

Those safeguards are reflected in the various internal arrangements of the Intelligence Services.

(3) No equivalent statutory safeguards applied under s.94 Telecommunications Act 1984 **[AB/6/76]**, as considered in *Privacy IPT* at [61] et seq of its July 2018 judgment **[AB/2/19]** (albeit that consideration was given to whether data would receive substantially equivalent protection in the hands of an overseas recipient). Further, the previously divided responsibilities of the oversight bodies preceding the IPC meant that they did not have available all previous records and information considered by the IPT in *Privacy IPT* (see [70] of the judgment). Nevertheless, the IPT found by a majority that the previous regime was in accordance with the law for the purposes of Article 8 ECHR as respected data sharing with foreign states.

(4) In all the circumstances, it is clear that the regime for sharing data with overseas authorities under Part 6 Chapter 2 is in accordance with the law.

138. As to §161 of C's skeleton, concerning the scope of application of Part 6 Chapter 2:

(1) C's description of the breadth of the discretion conferred on the executive by Part 6 Chapter 2 gives insufficient weight to the constraints on the exercise of that discretion. The constraints to which C refers at §161(1) of its skeleton argument as the "*only constraints*" on that discretion are, in fact, very substantial, for reasons explained in the DGR and elsewhere herein. Further, the constraints to which C refers are strikingly incomplete, because they exclude the system of independent authorisation by Judicial Commissioners, which is one of the key new protections under the Act; and the need to specify in the warrant the operational purposes for which data may be selected for examination.

(2) C's reliance on the interrelationship between Part 6 Chapter 2 and Part 4 of the Act (skeleton, §161(2)) ignores the findings of this Court in the April 2018 Divisional Court Judgment [**AB/4/45]**, to the effect that that the Part 4 regime will not give rise to the 'general and indiscriminate' retention of CD. The Divisional Court's conclusion at [137] carries equal force in relation to the Convention as it does in relation to the EU law position:

"*Ultimately, the overall amount of data which is retained under Part 4 of the 2016 Act will be the outcome of applying a statutory regime which requires the contents of each retention notice to be necessary and proportionate. This rigorous approach required by the 2016 Act will be reinforced when the provisions for judicial scrutiny are brought into force.*"

139. As to §162(1)-(4) of C's skeleton argument, concerning the further procedural safeguards in relation to Part 6 Chapter 2 that are said to be "*insufficient*", C's various allegations reiterate points made earlier in its skeleton argument in relation to other powers. Ds' responses to those points above are not repeated here.

(5) Retention and acquisition of CD under Parts 3 – 4 of the Act / RIPA Part 1 Chapter 2

RIPA Part 1 Chapter 2

140. At §§163-166 of its skeleton argument, C advances – for the first time – the allegation that RIPA Part 1 Chapter 2 **[AB/1/3]** is not in accordance with the law. That allegation is unpleaded; C should not be permitted to advance it at this late stage; and the declaration C seeks in this respect would have no utility. C also inaccurately summarises the effect of RIPA Part 1 Chapter 2, as now amended by the Data Retention and Acquisition Regulations 2018. Further, C's suggestion that the continued operation of Part 1 Chapter 2 RIPA has *"emerged, in part in correspondence and evidence in this case"* is tendentious. The continued operation of Part 1 Chapter 2 of RIPA is a matter of public record; and the fact that Part 3 IPA does not govern all CD acquisition requests, and Part 1 Chapter 2 of RIPA is still on the statute books, is evident on the face of legislation. The good reasons for that are set out below.

141. As the Court will be aware:

(1) This Court declared in the April 2018 Divisional Court Judgment **[AB/4/45]**, following a concession from Ds, that Part 4 of the Act was incompatible with EU law in that in the area of criminal justice (i) access to retained data was not limited to the purpose of combating "serious crime"; and (ii) access to retained data was not subject to prior review by a court or independent administrative body: [186].

(2) The Court required Ds to amend the legislation by 1 November 2018 accordingly. It did not require public authorities to stop acquiring CD pending the coming into force of a new regime, and stated that it was not *"prepared to contemplate the grant of any remedy which would have the effect, whether expressly or implicitly, of causing chaos and which would damage the public interest"*: [92].

(3) Ds amended the legislation by means of the Data Retention and Acquisition Regulations 2018 ("the 2018 Regulations"), made on 31 October 2018.

(4) The 2018 Regulations amended Part 1 Chapter 2 RIPA with effect from 1 November 2018, so as to provide that a person designated for the purposes of Chapter 2 could acquire communications data falling within s.21(4)(a)-(b) RIPA[72]

[72] This consists (in broad terms) of (i) traffic data; and (ii) service use data. It does not include subscriber data (which would fall within s.21(4)(c) RIPA), on the basis that the CJEU's findings in *Watson CJEU* concerning compatibility with the e-Privacy Directive were not concerned with subscriber data. The Court will recall a parallel issue of the scope of the CJEU's findings in relation to CD arising in the April 2018 Divisional Court Judgment, with respect to whether the CJEU's judgment in *Watson CJEU* covered only "events data" as defined in s.261 of the Act, or both "events data" and "entity data". This Court found that the definition of "events data" under the Act embraced both "location data" and "traffic

for the purpose of preventing or detecting "serious crime" only (as defined in s.25(1) RIPA), and not "crime" per se. In other words, Part 1 Chapter 2 RIPA has fully reflected this aspect of the Court's judgment from 1 November 2018. C's skeleton argument wholly fails to recognise this.

(5) The 2018 Regulations also amended the Act to provide for a new system of independent authorisation for requests to acquire retained communication data under Part 3 of the Act (i.e. OCDA), covering all requests within the scope of the e-Privacy Directive (and indeed, some requests outside the scope of the e-Privacy Directive[73]).

(6) Part 3 of the Act came into force on 5 February 2019, pursuant to the Investigatory Powers Act 2016 (Commencement No.11) Regulations SI 2019/174. Public authorities have started transitioning to OCDA, and thus making acquisition requests pursuant to the Act, from April 2019.

(7) However, Part 1 Chapter 2 RIPA has not yet been repealed, because the practical complexities and difficulty of setting up a system of independent authorisation for a multitude of different public authorities and types of CD under the Act have meant that OCDA is not yet fully operational. So certain public authorities cannot yet use the system of independent authorisation provided for by Part 3 of the Act. Those difficulties have been explained *inter alia* in Dix 1, §§128-135 **[TB/2/450]** and Gardiner 1 **[TB/2/489]**, as well as in evidence before the Court at the hearing of C's EU law challenge to Part 4 of the Act. Part 1 Chapter 2 RIPA will be repealed when all relevant public authorities have transitioned to using OCDA, which is expected to be by the end of 2019.

(8) This Court indicated in the April 2018 Divisional Court Judgment [**AB/4/45]** that it understood the practical difficulties to which the evidence on OCDA before the Court referred, and the reasons why both the IPC and Ds did not wish to establish OCDA in a way which proved to be premature and therefore counter-productive in the public interest: [96].

(9) Thus, Part 1 Chapter 2 RIPA continues in existence only as a temporary residual power, to ensure that certain public authorities that remain unable to use the system of independent authorisation effected by OCDA are able to access the CD that they need, pending transition to OCDA.

---

data" in the e-Privacy Directive and so "entity data" did not fall within the scope of paragraph 2 of the dispositif in *Watson CJEU*: see [154] of the Judgment.

[73] For instance, the system of independent authorization covers both events and entity data. It does not cover requests from the Intelligence Services, on the basis that EU law does not apply in the field of national security.

142. The ECtHR in *BBW* found that Part 1 Chapter 2 RIPA was not in accordance with law for the purposes of Articles 8 and 10 EHCR, precisely because, and only insofar as, this Court declared it contrary to EU law in the April 2018 Divisional Court Judgment: see *BBW* at [465]-[468], [496]-[498][74] **[AB/2/20]**.

143. In the circumstances set out above, Ds submit that not only should the challenge to Part 1 Chapter 2 RIPA be dismissed on the basis that it is unpleaded, but the declaration sought would have no utility. This Court has made clear that it does not expect Ds immediately to cease operating the Part 1 Chapter 2 RIPA regime, before relevant public authorities are able to use OCDA. Ds have, for their part, amended the legislation as required, and are taking all practical steps to ensure that OCDA comes fully into operation as soon as reasonably possible. Part 1 Chapter 2 RIPA continues on the statute books only as a temporary, residual power. The ECtHR's findings on Article 8 and 10 do not go beyond those made by this Court in relation to EU law. In those circumstances, no useful purpose would be served by the declaration that C seeks.

Parts 3 and 4 of the Act

144. Ds' basic response to the submissions at §167 *et seq* of C's skeleton argument is that, in circumstances where the Divisional Court has already held that the Part 4 regime does not give rise to the general / indiscriminate retention of data and so does not contravene EU law in that respect, it would be a remarkable result if the regime were nevertheless incompatible with the Convention due to the wide scope of its application and the absence of sufficient safeguards. C does not address the April 2018 Divisional Court Judgment in the context of its submissions on Parts 3 - 4.

145. As to §170 of C's skeleton argument, Ds did indeed understand the various allegations made by C in relation to Part 4 as individual allegations of Convention incompatibility. But in any event, Ds' case is that, taken as a whole, the regime in Pt 4 of the Act is wholly compliant with the Convention.

146. As to the various allegations at §171 of C's skeleton argument, and without prejudice to Ds' primary argument that the *Weber* criteria area inapplicable in the context of CD:

(1) As to §171(1) of C's skeleton argument, the Defendants do indeed rely on the generally less intrusive nature of CD, as to which see above.

[74] The precise wording of the ECtHR's judgment is capable of causing confusion, because the ECtHR does not appear fully to have appreciated the limitations on this Court's declaration in the April 2018 Divisional Court Judgment to (i) events data only; and (ii) the area of criminal justice only. However, it is entirely clear that the ECtHR did not intend to go beyond the scope of this Court's judgment in April 2018, but rather to reflect it.

(2) As to the contention at §171(2) of C's skeleton argument that the statutory purposes for the retention of and access to CD remain "*wide*", those purposes have been substantially narrowed following the amendments introduced by the Data Retention and Acquisition Regulations 2018: see DGR §85(2) **[TB/2/388]**. Further, C has no answer to the point that the acquisition of data must be "*for the purposes of a specific investigation or specific operation*": see s. 61(1)(b) of the Act (and the related provisions of §3.13 of the Communications Data Code **[AB/3/28]**).

(3) §171(3) of C's skeleton argument confuses the question of which public authorities may from time to time need to access retained data with the question of whether access to retained data will be authorised in any particular case. The fact that a range of public authorities may in principle obtain CD under Part 3 cannot conceivably give rise, or contribute, to a breach of the Convention.

(4) §171(4) of C's skeleton argument misrepresents Ds' argument at DGR §85(5) **[TB/2/389]**. Ds observed that applying a geographical limitation, or an individual targeting limitation, to the retention power under Part 4 of the Act would be wholly impracticable, would emasculate its usefulness, and is not required under the Convention. Ds also observed that this point is *a fortiori,* since bulk interception (not limited by geography, or individual targeting) is in principle compatible with the Convention. C's skeleton argument does not address the substance of the point in the DGR; nor does it give any principled reason why the position should be different under Part 4, than for bulk interception.

(5) §171(5) of C's skeleton argument is not understood. A retention notice under Part 4 of the Act requires prior authorisation by a Judicial Commissioner (s. 89 of the Act), and a system of independent authorisation (by the OCDA) for access to retained CD is well on the way to being fully implemented. The reliance on *Zakharov* **[AB/2/13]** is therefore misplaced: that case concerned the direct interception by the State of communications (not CD), without obtaining prior judicial authorisation.

(6) As to §171(6) of C's skeleton argument, DGR §113 **[TB/2/399]** provides a complete answer. The argument advanced by C is based on a straightforward misreading of §24.24 of the Communications Code [**AB/3/28]** as if it provided an exhaustive definition of 'relevant' errors for the purposes of s. 231 of the Act. That is not what §24.24 does. It simply provides non-exhaustive examples of reportable errors (cf. §24.25). The key provision, however, is §24.21, which states in the clearest possible terms that where an error results in CD being acquired or disclosed wrongly, a report must be made to the IPC.

147. In conclusion, Part 6 Chapter 2 and Parts 3 – 4 of the Act together provide a comprehensive and robust set of safeguards that provide ample protection for individuals' Convention rights, even in those particular cases where CD does reveal private information. C's various complaints about these Parts of the Act should be dismissed.

F. Journalistic and watchdog protection

148. Ds answer below in turn the NUJ's contentions at §§24-41 of its skeleton concerning (i) independent authorisation; (ii) the need for an "*overriding requirement in the public interest*"; and (iii) the definition of "*journalistic material*" in the Act. Point (iii) also comprehends C's single substantive point in its skeleton on this part of the case, which is a complaint that the Act and Codes do not make specific reference to "*watchdog organisations*" as meriting protection under Article 10 ECHR (C's skeleton, §177).

(1) Independent authorisation: NUJ's skeleton, §§24-31

149. The core answer to all the NUJ's points on this part of the case is that they misunderstand the effect of the ECtHR's case law. For the reasons already explained above at §§38-48, that jurisprudence requires prior independent authorisation (save in urgent cases) where an order is sought requiring the divulging of a journalistic source, or where the purpose of obtaining material is to discover a journalistic source. It does not require prior independent authorisation in the wide range of other circumstances pleaded by the NUJ at skeleton §26.

150. Indeed, as explained above, it is plainly inconsistent with *BBW* and *Weber* to suggest that the ECtHR requires prior independent authorisation where information obtained in bulk is searched in order to identify a source, or to obtain journalistic material (let alone, where that is simply one possible consequence of the search). *BBW* and *Weber* explicitly indicate that such independent authorisation is not required.

151. Therefore, in answer to the various complaints about the statutory regime at §§30-31 of the NUJ's skeleton:

(1) As to §30(a), the NUJ's complaint about the absence of any need for independent approval for selection for examination under the bulk acquisition regime under Part 6 Chapter 2 of the Act misunderstands the ECtHR's reasoning at [499][75] of *BBW* **[AB/2/20]**. As explained at §48 above, the ECtHR's finding of unlawfulness at [499] of *BBW* was made on the premise that EU law required access to retained

[75] The NUJ's skeleton refers in this respect to [495] of *BBW*, but [495] is concerned with a different point: it appears that this is intended to be a reference to [499].

communications data to be subject to prior review by an independent body. It had nothing to do with the inherent requirements of Article 10 ECHR. The ECtHR's reasoning concerning Chapter 2 Part 1 RIPA cannot be read across to Part 6 Chapter 2 of the Act. Part 6 Chapter 2 concerns a bulk acquisition power available only to the Intelligence Services, for national security-related grounds: see s.158 of the Act. It is not within the scope of EU law at all.

(2) As to §30(b), exactly the same point also applies to selection for examination under Part 6 Chapter 1 (bulk interception) and Part 6 Chapter 3 (bulk equipment interference) of the Act. It should also be noted that there are very significant protections in place for journalistic material under Part 6 Chapters 1 and 3 (and the same applies to Part 6 Chapter 2), albeit that they do not involve prior independent approval before material is selected for examination, save where the "British Islands" safeguard applies. For instance, as regards bulk interception under Part 6 Chapter 1:

i. By s.154 of the Act, where a communication intercepted under a bulk warrant is retained, following examination, and is a communication containing journalistic material, the IPC must be informed as soon as reasonably practicable;
ii. By §9.84 of the Code, where an authorised person in an intercepting authority intends to select material for examination to identify or confirm a source of journalistic information (and a targeted examination warrant is not otherwise required), they must notify a senior official[76] in a different authority, who can only approve the selection if they consider the authority has arrangements in place for the handling, retention, use and destruction of communications that identify sources of journalistic information; and no selection for examination can take place prior to that approval.
iii. By §9.86 of the Code, where an authorised person in an intercepting authority intends to select content for examination which it is believed is confidential journalistic material (and a targeted examination warrant is not otherwise required), the same principle applies. They must notify a senior official in a different authority before selecting it, and the official can only approve the selection if they consider the authority has appropriate arrangements in place etc.
iv. By §9.87 of the Code, where either confidential journalistic material or material identifying a source is retained and disseminated to an outside body, reasonable steps should be taken to mark it as confidential, and where there is any doubt as to the lawfulness of its proposed handling or dissemination, legal advice must be sought.

[76] "Senior official" is defined by s.157 of the Act as "*a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service*".

v. By §9.88, where either confidential journalistic material or material identifying a source has been selected for examination and retained, the matter should be reported to the IPC as soon as reasonably practicable.

Parallel safeguards apply under Part 6 Chapter 3. Taken as a whole, these are precisely the type of safeguards that the ECtHR indicated at [492] of *BBW* that it would expect in a Convention-compliant regime.

(3) The same points apply in relation to §30(c) (BPD under Part 7 of the Act). No independent judicial authorisation is required, and the carefully calibrated protections in the BPD Code concerning selection for examination of confidential journalistic protected data and journalists' sources are well sufficient to comply with the Convention. See the BPD Code, §§7.38-7.48 **[AB/3/23]**.

(4) As to §30(d), this point adds nothing to the issues addressed in the April 2018 Divisional Court judgment in light of *Watson CJEU,* and any declaration in this respect would be otiose, in light of the Government's amendment of the relevant legislation and steps to establish OCDA.

(5) As to §30(e), it is a serious understatement to characterise the Codes as merely "*a relevant consideration*", and "*effectively policies*". They are statutory Codes, laid before both Houses of Parliament for approval, and subject to mandatory consultation with the IPC. By Schedule 7 to the Act:

i. Codes must include "*provision designed to protect the public interest in the confidentiality of sources of journalistic information*" (para 2(1)(a));
ii. Codes must include "*provision about particular considerations applicable to any data which relates to a member of a profession which routinely holds items subject to legal privilege or relevant confidential information*" (para 2(1)(b) – relevant confidential information including, by para 2(4), journalistic material);
iii. A Code must be taken into account by a person exercising any functions to which it relates (para 6(1));
iv. The Codes are admissible in evidence in criminal or civil proceedings (para 6(3)), and a court or tribunal determining any question in criminal or civil proceedings may take into account a person's failure to have regard to a Code (para 6(4));
v. A supervisory authority exercising functions by virtue of the Act (i.e. the IPC, any Judicial Commissioner, the Information Commissioner, or the IPT) may take into account a failure by a person to have regard to a Code in determining a question which arises in connection with the exercise of those functions (para 6(5)).

(6) Finally, §31 of the NUJ's skeleton is wrong for the reasons already set out above: there is no requirement that journalistic material discovered unexpectedly should be the subject of an independent determination whether it can be used.

(2) "Overriding requirement in the public interest": NUJ's skeleton, §§32-38

152. The NUJ's argument here mistakenly treats the phrase "*overriding requirement in the public interest*" as a special formula that requires repetition in the language of the statutory scheme. There is no magic in the phrase, which means that the language itself must be written into the applicable Codes (still less, the Act). Rather, the phrase simply reflects the weight to be afforded to journalistic source protection in the ECHR scheme.

153. The phrase "overriding interest" is derived from the Grand Chamber's judgment in *Goodwin v UK* (1996) 22 EHRR 123 **[AB/5/52]**. *Goodwin* was a case which concerned source disclosure (in that case, the question whether a High Court order requiring the applicant journalist to disclose his source constituted a violation of his rights under Article 10 ECHR). The ECtHR found that although the impugned measure was prescribed by law, and pursued a legitimate aim, the High Court's order was not "necessary in a democratic society". In that regard, it stated at [39]:

"The Court recalls that freedom of expression constitutes one of the essential foundations of a democratic society and that the safeguards to be afforded to the press are of particular importance…Protection of journalistic sources is one of the basic conditions for press freedom… Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public-watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected. Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society and the potentially chilling effect an order of source disclosure has on the exercise of that freedom, such a measure cannot be compatible with Article 10 of the Convention unless it is justified by an overriding requirement in the public interest. These considerations are to be taken into account in applying to the facts of the present case the test of necessity in a democratic society under paragraph 2 of Article 10 (art. 10-2)."

154. As the reasoning at [39] of *Goodwin* makes clear, the need for an "*overriding requirement in the public interest*" to provide sufficient justification under Article 10(2) reflects the importance of the protection of journalistic sources for press freedom. It does not represent some separate, freestanding, need for the language of "*overriding interest*" to be expressly written into any applicable statutory scheme. That sort of formalistic requirement would be inconsistent with the ECtHR's concentration upon substance, not linguistic niceties. Indeed, the outcome as well as the reasoning in *Goodwin* is flatly inconsistent with the application of any such formalistic condition. If such a condition existed, the absence of the language of "*overriding requirement*" from national law would inevitably have meant in *Goodwin* that any relevant interference with Article 10(1) was not "*prescribed by law*". But in *Goodwin,* the "*prescribed by law*"

test was met, because the law was reasonably foreseeable and provided adequate protection against arbitrary interference: see [29]-[34]. The problem, rather, was the measure's lack of proportionality: see [46].

155. That is not to say that the importance of source protection will not require national law to contain clearly defined rules concerning source disclosure, in order to provide sufficient safeguards against abuse. See e.g. *Sanoma* at [88] **[AB/2/9]**:

"Given the vital importance to press freedom of the protection of journalistic sources and of information that could lead to their identification any interference with the right to protection of such sources must be attended with legal procedural safeguards commensurate with the importance of the principle at stake".

The point, however, is that those safeguards do not need to take any specific form by reason of the "overriding public interest" needed to justify an interference with the right to protection of journalistic sources. They merely need to be sufficiently rigorous.

156. For completeness, there is nothing in the *BBW* judgment **[AB/2/20]** (or in the Government's response to the judgment) which suggests otherwise, contrary to §§32-35 of the NUJ's skeleton. The ECtHR found that, having regard to the need for an overriding requirement in the public interest to justify interfering with source protection, the lack of any "above the waterline" arrangements in the s.8(4) Regime limiting the Intelligence Services' ability to search and examine confidential journalistic material was not "prescribed by law": [495]. It emphatically did not find that the s.8(4) Regime was unlawful because it failed to refer explicitly to the need for an "*overriding requirement in the public interest*".

157. As to how those principles apply here:

(1) All the applicable Codes under the Act contain explicit, carefully calibrated protections for "*confidential journalistic material*" as defined in s.264 of the Act, including where it is contained in information obtained in bulk, and is subsequently selected for examination. The position, therefore, is that (by contrast to the s.8(4) Regime under consideration in *BBW*), exactly the type of "above the waterline" arrangements to which the First Section was alluding at [495] of *BBW* now exist.

(2) Specific protections apply under the Codes to such material, irrespective whether it is deliberately sought, or discovered unexpectedly (leaving aside the question whether this situation is subject to an "*overriding requirement*" for source protection in the first place).

(3) So the NUJ's only complaint can be that the language of *"overriding requirement in the public interest"* is not used throughout the Codes[77]; and that is not, on a proper analysis, a valid complaint for the reasons above.

(3) The definition of "journalistic material": NUJ's skeleton, §§39-41

158. The NUJ's final complaint at skeleton §§39-41 is that "journalistic material" is too narrowly defined in s.264 of the Act (and GCHQ's Compliance Guide **[TB/5/190]**) in various respects[78]. That contention is wrong, and the NUJ's various criticisms at §40(a)-(f) of its skeleton are not well founded. The Home Office consulted widely upon the definition, including meeting several times with journalist groups, and the difficulty of defining who is a "journalist" in the digital age was discussed extensively during the passage of the Bill through Parliament (see Dix 2, §42 **[TB/2/677]**). The resulting definition is sensible, workable, and consistent with the jurisprudence. Addressing the NUJ's criticisms in turn:

(1) As to skeleton §40(a)-(b), Mr Cobain asserts that the definition of "journalistic material" is problematic because there will be circumstances where a journalist

---

[77] In fact, a number of the Codes do refer to the need for there to be an "overriding requirement in the public interest" to outweigh source protection: see e.g. §9.76 of the EI Code of Practice **[AB/3/22]**, and similar language in the Communications Data **[AB/3/28]** and Bulk Acquisition Codes **[AB/3/25]**.

[78] For ease of reference, the definition of "journalistic material" in s.264(2)-(5) of the Act is as follows (and "confidential journalistic material is itself defined in s.264(6)-(7)):

"(2) "Journalistic material" means material created or acquired for the purposes of journalism.

(3) For the purposes of this section, where
- *a. a person ("R") receives material from another person ("S"), and*
- *b. S intends R to use the material for the purposes of journalism, R is to be taken to have acquired it for those purposes.*

Accordingly, a communication sent by S to R containing such material is to be regarded as a communication containing journalistic material.

(4) For the purposes of determining whether a communication contains material acquired for the purposes of journalism, it does not matter whether the material has been acquired for those purposes by the sender or recipient of the communication or by some other person.

(5) For the purposes of this section –
- *a. Material is not to be regarded as created or acquired for the purposes of journalism if it is created or acquired with the intention of furthering a criminal purpose, and*
- *b. Material which a person intends to be used to further such a purpose is not to be regarded as intended to be used for the purposes of journalism.*

(6) "Confidential journalistic material" means-
- *a. in the case of material contained in a communication, journalistic material which the sender of the communication-*
  - *i. holds in confidence, or*
  - *ii. intends the recipient, or intended recipient, of the communication to hold in confidence;*
- *b. in any other case, journalistic material which a person holds in confidence.*

(7) A person holds material in confidence for the purposes of this section if –
- *a. The person holds it subject to an express or implied undertaking to hold it in confidence, or*
- *b. The person holds it subject to a restriction on disclosure or an obligation of secrecy contained in an enactment."*

does not acquire information for the purposes of journalism, but later decides to use it for those purposes. But Mr Cobain's suggested approach is too wide, because it would mean in effect that any information ever provided to a journalist would always need to be treated as "journalistic material". So the protections for confidential journalistic sources in the Act would need to apply to every interchange between a journalist and anyone else at all (see Dix 2, §41 **[TB/2/675]**). That is not a realistic position. Information which is not given to a person in his capacity as a journalist does not realistically require the protections applicable to journalists. *Miranda* **[AB/2/15]** does not decide otherwise (contrary to the NUJ's skeleton, §40(b)). Lord Dyson MR did not hold in *Miranda* that "journalistic material" comprised any information received by a journalist for any purpose: *Miranda* was not concerned with the definition of "journalistic material", not least because the information at issue in *Miranda* was obviously information provided by a source, for the purposes of journalism.

(2) Further, it is not only consistent with the case law, but correct, to provide that the question whether someone is a journalist for the purposes of the Act should be assessed "*on all the facts and circumstances available at the time*"[79]. That is not a narrow, but a properly fact-sensitive, approach: particularly since all the Codes also provide that the assessment must "*take into account the purpose of the provisions contained within the Act which is to protect the proper exercise of free speech, and protect the role that journalists play in protecting the public interest*".

(3) As to skeleton §40(c), the NUJ's reading of the definition of "*confidential journalistic material*" in s.264 of the Act is much too narrow. The reference in s.264(7)(a) of the Act to "*an express or implied undertaking of confidentiality*" itself comprehends all the broad circumstances in which an obligation of confidence may arise either at law or equity. For instance, information obtained by improper or surreptitious means, or indeed by accident or mistake, which bore the necessary quality of confidentiality would itself be held subject to an equitable obligation of confidence – i.e. an implied undertaking - owed to the person from whom it was obtained. Mr Cobain's understanding of the significance of the word "undertaking" in these circumstances is unduly narrow (see Cobain 1 §47(3) **[TB/2/509]**). Further, the NUJ's argument fails to recognise that the definition of "confidential journalistic

[79] This is the approach in all the relevant Codes: see e.g. Interception of Communications Code, §9.81 **[AB/3/24]**; Equipment Interference Code **AB/3/22**, §9.77; BPD Code **[AB/3/23]**, §7.43; Communications Data Code **[AB/3/28]**, §8.15. The relevant paragraph, which is common across the various Codes, provides:
"An assessment of whether someone is a journalist (for the purposes of the Act) should be made on all the facts and circumstances available at the time. Consideration should be given, in particular, to the frequency of the individual's relevant activities, the level of personal rigour they seek to apply to their work, the type of information that they collect, the means by which they disseminate that information and whether they receive remuneration for their work. This approach will take into account the purpose of the provisions contained within the Act which is to protect the proper exercise of free speech, and reflect the role that journalists play in protecting the public interest."

material" also includes information which the sender of the communication intends the recipient to hold in confidence, irrespective whether the recipient believes themselves bound by an express or implied undertaking to that effect. So Mr Cobain's observation at §47(3) that he would not necessarily consider himself bound by an undertaking of confidence *"even when a source expects confidential treatment"* (emphasis as in the original) precisely reflects circumstances in which information would be treated as "confidential journalistic material" under the definition in s.264 of the Act.

(4) As to §40(d)-(e), the test whether a person is a "journalist" in the various Codes properly allows for journalists who "blog", or post online, to be treated as such. It is entirely justifiable that matters such as the frequency of a person's activities, the level of personal rigour that a person applies to their work, the type of information they collect, and whether they are remunerated for it, should be taken into account as relevant, albeit non-exhaustive, factors when determining whether a person is a "journalist". In appropriate cases, those factors are equally apt to apply to an online blogger as to a print journalist. The test, which is an open-textured one made on *"all the facts and circumstances available at the time"* also properly allows for "social watchdogs" to fall within the definition: not least, because it requires account to be taken of "*the role that journalists play in protecting the public interest*".

(5) The NUJ's skeleton at §40(f), and Cobain 1 §§48-54 **[TB/2/611]**, allude to a supposed difficulty which does not in fact arise. The effect of s.264(5) of the Act is to exclude from the definition of "journalistic material" for the purposes of that section material that is created or acquired with the intention of furthering a criminal purpose. So, to use the NUJ's example, it is correct to say that a paper authorising torture, written by a government official, would not be "journalistic material" for the purposes of s.264. Thus, the paper itself would not benefit from the protections for "*confidential journalistic material*" under the Act. However, the second government official who passed the unlawful paper on to a journalist would be a "*source of journalistic information*" for the purposes of s.263 of the Act, namely "*an individual who provides material intending the recipient to use it for the purposes of journalism or knowing that it is likely to be so used*". That definition is not disapplied, simply because the material in question is not "*journalistic material*" for the purposes of s.264 of the Act. So the official would benefit from the relevant protections for journalistic sources in the Codes and Act, as appropriate[80]. The

[80] See for example §9.74 of the Interception Code **[AB/3/24]**:
"There is a strong public interest in protecting a free press and freedom of expression in a democratic society, including the willingness of sources to provide information to journalists anonymously. Where a targeted interception warrant is sought or a targeted examination warrant to select for examination communications, to determine the source of journalistic information, the public interest requiring such selection must override any other public interest."
§6.25 of the Bulk Acquisition Code **[AB/3/25]**, §9.76 of the EI Code **[AB/3/22]**, and §7.45 of the BPD Code **AB/3/23]** are to similar effect.

protections within and under the Act for "*confidential journalistic material*" and the protections within and under the Act for "*sources of journalistic information*" overlap: but they do not depend upon each other. It is perfectly possible for a person to be a "*source of journalistic information*" under s.263 of the Act, even if the information they provide is not "*confidential journalistic material*" for the purposes of s.264.

H. Lawyer-client special protection: C's skeleton, §§179-202

159. In light of the legal principles set out above at §§49-53, none of C's complaints about the provisions of the Act and Codes as regards protection for lawyer-client communications disclose any breach of Articles 8 or 10 ECHR.

(1) Part 6 Chapter 2 and Parts 3-4 of the Act: Powers relating to communications data, C's skeleton §§183-191

160. In summary, there are three answers to this part of the challenge:

(1) The ECtHR case law upon which C relies is concerned with the targeted surveillance of the content of legally privileged communications. That case law cannot be "read across" as if it applied in unmodified form to communications data.

(2) The relevant Codes[81] expressly require *"special consideration"* to be given to necessity and proportionality when seeking access to communications data relating to a person who is a member of a profession handling privileged or otherwise confidential material. Such consideration, and the conditions attached to it, is sufficient to meet any requirement of Articles 8 and 10 ECHR in this context.

(3) C's skeleton appears to make a further, new, challenge to the system based on GCHQ's 2018 Compliance Guide **[TB/5/51 et seq]** (skeleton, §185). Any such challenge would need to be pleaded, so that it could be addressed in evidence; and in any event, in the absence of any indication that the lack of "technical measures" to which the Compliance Guide refers makes it difficult or impossible for GCHQ to identify confidential material, the challenge cannot succeed.

[81] I.e. the Communications Data Code of Practice **[AB/3/28]**, relating to the exercise of functions under Parts 3 and 4 of the Act (see §§8.8-8.11), and the Bulk Acquisition Code of Practice **[AB/3/25]**, relating to the exercise of functions under Chapter 6 Part 2 (see §§6.19-6.23).

The law as it applies to communications data

161. As set out above at §§49-53, the surveillance cases upon which C relies in this area (*Michaud* **[AB/2/8]**, *RE* **[AB/5/67]**, *Kopp* **[AB/2/5]**, *McE v PSNI* **[AB/4/33]**, *Szabo* **[AB/2/14]**) all address targeted surveillance of the content of lawyer-client communications, not the obtaining of communications data. They also make clear that the degree of any "strengthened protection" necessary for lawyer-client exchanges will depend upon the context.

162. Acquisition of communications data may reveal when a communication occurred; between what devices; and for how long it lasted. But communications data will very rarely itself disclose any advice given, because it will not reveal the content of the exchanges between a lawyer and their client[82]. So it will not touch upon (or will touch only indirectly upon) the central purpose of LPP, which is to enable a client to make full disclosure to his legal adviser for the purposes of seeking legal advice without apprehension that anything said by him in seeking advice, or to him in giving it, may be subject to disclosure against his will. This is a context where the difference in the degree of intrusiveness involved in obtaining communications data, and in obtaining the entire content of exchanges, is likely to be particularly marked.

The Codes and Act

163. The Communications Data Code and the Bulk Acquisition Code specifically confer additional protections upon communications data concerning lawyers. They state that (i) the degree of interference with rights may be higher where the communications data relates to a professional (such as a lawyer) handling privileged information; (ii) it may be possible to infer an issue of sensitivity from the fact that a

[82] There is a dispute between the parties as to the extent to which LPP is likely to apply to communications data. Ds' position is that communications data will very rarely be subject to LPP. LPP protects confidence in communications made between client and lawyer for the purpose of advice or assistance in a relevant legal context. It does not protect information that does not consist of a communication between client and lawyer. See e.g. *R v Manchester Crown Court ex p Rogers* [1999] 1 WLR 832 at 839 **[AB/4/29]** per Lord Bingham CJ (the record of time on a solicitor's attendance note, on a time sheet or fee record could not qualify for privilege if it were not in any sense a communication. Quite apart from the fact that it had nothing to do with obtaining legal advice, it recorded nothing which passed between solicitor and client). The cases cited in Passmore 1 at §27 **[TB/2/55]** address exceptional circumstances, in which information that would ordinarily not be subject to LPP (e.g. a name, location or phone number of a client, lawyer or witness) could in principle be treated as privileged. Those cases are both highly unusual, and are premised upon that information being the subject of a communication between client and lawyer for the purposes of giving or receiving legal advice. See e.g. *JSC Bank v Ablyazov* [2012] EWHC 1252 at [17]-[18] **[AB/4/36]** and [24]-[29]; *JSC Bank v Solodchenko (no.3)* [2011] EWHC 2163 **[AB/4/35]** at [27]-[29]; *SRJ v Persons Unknown* [2014] EWHC 2293 at [17] and [27] **[AB/4/37]**. However, it is unnecessary to resolve this dispute, because the degree of protection given by Strasbourg to lawyer/client exchanges does not depend upon whether they are classified as subject to LPP as a matter of domestic law: see e.g. *RE v UK* [**AB/5/67**].

person communicates with a lawyer; (iii) accordingly, special consideration must be given to issues of necessity and proportionality; (iv) applications must draw attention to any circumstances that might lead to an unusual degree of intrusion or infringement of rights; (v) particular care must be taken by individuals authorising such applications, including consideration of any unintended consequences and of the public interest; (vi) applications must note in all cases where an application is made for the communications data of a relevant professional (including a lawyer); (vii) the fact that such an application has been made should be recorded; and (viii) applications should be marked for the attention of the Investigatory Powers Commissioner. See §§8.8-8.11 of the Communications Data Code **[AB/3/28]** (and parallel provisions in §§3.72-3.75 of the Bulk Acquisition Code **[AB/3/25]**).

164. Further, by s.2 of the Act, public authorities deciding whether to issue, renew, cancel, modify, apply for, approve, or approve a decision to give or vary, a warrant under Part 6, an authorisation under Part 3 or a notice under Part 4 of the Act (as the case may be) must have regard to *"whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant, authorisation or notice is higher because of the particular sensitivity of that information"*: s.2(2)(b). Non-exhaustive examples of "sensitive information" given in s.2(5) of the Act include *"items subject to legal privilege"*: s.2(5)(a).

165. Those additional protections, and the specific recognition of the importance of lawyer/client confidentiality which they entail, are plainly sufficient to satisfy the demands of Articles 8 and 10 ECHR[83] in these circumstances.

GCHQ's Compliance Guide

166. Finally, C's skeleton at §185 complains that *"the erroneous view that communications data will only rarely be privileged has led GCHQ into not providing any technical measures to protect such information in its systems"*. As to this:
(1) The view is correct.
(2) In any case, the part of the Compliance Guide quoted by C **[TB/5/214]** makes clear that metadata systems must have procedural safeguards in place to ensure that confidential material (including LPP material) is appropriately handled if it is encountered, so the absence of "*technical measures*" would at least on the face of it appear irrelevant.
(3) If C were to make a challenge to GCHQ's practices on the basis that "*technical measures*" were needed, that challenge would need to have been pleaded so that it could be properly addressed in the evidence.

[83] There is nothing in the ECtHR 's case law to suggest that different or additional considerations arise here under Article 10 ECHR, to those arising under Article 8 ECHR.

(2) Part 6 Chapter 3, Part 5, Part 6 Chapter 1 and Part 7: C's skeleton, §§192-202

167. C's complaints under this head similarly rely upon the false proposition that the ECtHR authorities lay down a lexicon of legal rules, when in fact they only establish a general principle that strengthened protection should be accorded to lawyer-client exchanges, the amount of protection required depending upon the context. On a proper analysis, the relevant provisions of the regime under Part 6 Chapter 3, Part 5, Part 6 Chapter 1 and Part 7 provide strengthened protection for lawyer-client material; and the fact that they do so in a graduated way is simply a function of the fact that some contexts require more protection than others. Accordingly, none of C's complaints here discloses any breach of Article 8 or 10 ECHR.

"Particular weight not accorded to the interest of lawyer-client confidence in some cases": C's skeleton, §§192-197

168. The answer here is that strengthened protection is provided to lawyer-client confidence in all cases, but on an appropriately graduated basis, depending upon the circumstances. Viz:

(1) At the apex of the need for protection will be cases where it is intended to search material obtained in bulk in order to obtain the legally privileged communications of lawyers. Thus, where a targeted examination warrant must be obtained under Part 2 or Part 5, or where selection for examination otherwise occurs under Part 6 Chapter 1 or Part 6 Chapter 3, or where it is intended to select for examination protected data held in a BPD, the decision-maker must have regard to the public interest in the confidentiality of items subject to LPP; there must be *"exceptional and compelling circumstances"* that make it necessary to authorise the search; and such circumstances will not exist unless (i) the public interest in obtaining the information outweighs the public interest in maintaining the confidentiality of legally privileged material; (ii) there are no other reasonable means of obtaining the information; and (iii) the search is necessary for the purpose of preventing death or serious injury or in the interests of national security[84].

(2) A wide definition of legal privilege applies for these purposes: under section 263 of the Act, "*items subject to legal privilege*" bears the same wide meaning as in s.10

[84] See s.27, s.112, s.153, s.194 and s.222 of the Act. See also the Interception Code **[AB/3/24]** at §§9.54-9.56 and 9.60; the EI Code **AB/3/22]** at §§9.48-9.54 and 9.56, and the BPD Code **[AB/3/23]**at §§7.25-7.28.

Police and Criminal Evidence Act 1984[85] **[AB/6/77]**. Further, the effect of the Codes is to widen the ambit of material treated as legally privileged still further[86].

(3) Strong, albeit not identical, protections also apply where is it likely that items subject to LPP (again, applying the wide approach to LPP set out above) will be selected for examination, even if this is not the intention. In such cases, any application for a targeted examination warrant under Part 2 or Part 5 of the Act must state that the relevant material is likely to include items subject to LPP, and how likely this is[87]; and the person to whom the application is made (which will also, of course, be subject to approval by a Judicial Commissioner) may only issue the warrant if they consider that the protective safeguards in place include specific arrangements for the handling, retention, use and destruction of items subject to LPP. (Obviously, the application would also need to set out why it was necessary and proportionate to select such items for examination.) Again, where it is not necessary to obtain a targeted examination warrant (e.g. for the examination of the communications of persons outside the UK), parallel protections apply under the Codes: a senior official, who must not be a member of the same authority to whom the bulk warrant is addressed, must apply the same tests before approving the selection for examination of those items, and the authorised person is prohibited from accessing the items until he or she has received that approval.

---

[85] ***"Meaning of "items subject to legal privilege".***
(1)Subject to subsection (2) below, in this Act "items subject to legal privilege" means –
(a)communications between a professional legal adviser and his client or any person representing his client made in connection with the giving of legal advice to the client;
(b)communications between a professional legal adviser and his client or any person representing his client or between such an adviser or his client or any such representative and any other person made in connection with or in contemplation of legal proceedings and for the purposes of such proceedings; and
(c)items enclosed with or referred to in such communications and made –
(i)in connection with the giving of legal advice; or
(ii)in connection with or in contemplation of legal proceedings and for the purposes of such proceedings,
when they are in the possession of a person who is entitled to possession of them."

[86] As C rightly accepts, the applicable Codes provide here that:
(1) In the case of the Interception Code **AB/3/24]**, wherever it is intended to select for examination communications using criteria referable to a lawyer acting in a professional capacity under a targeted examination warrant, it should be assumed that the material is subject to LPP – see §9.62 of the Interception Code. Where no targeted examination warrant is required (i.e. where the target is not in the British Islands), the same considerations apply: see §§9.59-9.61 of the Code.
(2) In the case of the EI Code **[AB/3/22]**, wherever it is intended to select for examination material using criteria referable to a lawyer acting in his professional capacity under a targeted EI warrant or a targeted examination warrant, it should be assumed that the material is subject to LPP: see §9.58 of the EI Code. Where the individual whose material is to be selected from material obtained in bulk is outside the British Islands, so that no targeted examination warrant is required, similar considerations apply: see §§9.55-9.57 of the EI Code.
(3) In the case of the BPD Code [**AB/3/23]**, any communication between a lawyer and a client, or between a lawyer and another person for the purpose of actual or contemplated litigation (whether civil or criminal) must be presumed to be privileged unless the contrary is established: see §7.21 of the BPD Code.

[87] See s.27(8) and s.112(7) of the Act.

(4) Protections also apply where legally privileged items are inadvertently and unexpectedly selected for examination (so that the enhanced protections set out above have not been applied). Any such item must be handled strictly in accordance with the same protections under the Codes regarding handling, retention, use and destruction that would apply to any other LPP items[88].

(5) C complains that the above protections only apply to "*content*" under Chapter 6 Part 1, "*protected material*" under Chapter 6 Part 3, or "*protected data*" under Part 7. The basic answer is that it is very unlikely that any material which is not "content", "protected material", or "protected data" (as the case may be) will be legally privileged in the first place. So, in accordance with the hierarchy of protections set out above, it is unnecessary to apply the same protections to such material. However, it is incorrect to imply that special protections do not apply to this material as well. Under ss. 153, 194 and 223 of the Act, the IPC must be informed of "*items subject to legal privilege*" which have been retained following their examination for purposes other than their destruction under Part 6 Chapters 1 and 3 and Part 7. See s.153(9), 194(9) and 223(1) of the Act. Unless the IPC considers that the public interest in retaining the item outweighs the public interest in its confidentiality, and that its retention is necessary in the interests of national security or for the purpose of preventing death or significant injury, the IPC must order its destruction, or impose one or more conditions on its use or retention; and even if those conditions are met, the IPC may nevertheless impose such conditions as he considers necessary for the purpose of protecting the public interest in the confidentiality of items subject to legal privilege. See s.153(10)-(12), s.194(10)-(12) and s.223(2)-(4) of the Act. Importantly, such items are not confined to "*content*", "*protected material*", or "*protected data*".

(6) C also complains that the above safeguards apply only to material retained under a specific BPD warrant, and not a class BPD warrant (see skeleton, §194(4)). However, that is incorrect. The statutory provisions of s.222 and 223 of the Act apply only to material retained under a specific BPD warrant (see s.222(1) of the Act), but the equivalent paragraphs of the BPD Code at §§7.25-7.33 **[AB/3/23]** apply to BPDs generally, whether retained under a specific or class warrant. See in particular §7.1 of the BPD Code, which states that the chapter sets out the safeguards which each intelligence service should put in place in relation to storage of BPDs "*whether acquired under class BPD or specific BPD warrants*", and the absence of any limitation to specific warrants in §§7.25-7.33 of the Code[89]. Also, and more fundamentally, in the BPD context, LPP material would always amount to "*protected data*" for the purposes of s.203 of the Act. So pursuant to s.202 of the

[88] See Interception Code, §9.61 **[AB/3/24]**; EI Code, §9.57 **AB/3/22]**; BPD Code **[AB/3/23]**, §7.29.
[89] Other provisions of Chapter 7 of the BPD Code are restricted to material retained pursuant to a specific BPD warrant: see e.g. §7.15.

Act, no search for LPP material could be conducted in respect of material retained pursuant to a class BPD warrant. A specific BPD warrant would be required.

"No prior, independent determination of whether and how special lawyer-client protection applies": C's skeleton, §§198-201

169. The short answer to this complaint is that the Strasbourg case law does not require prior independent authorisation before legally privileged material is selected for examination from material obtained in bulk. Such a requirement cannot properly be derived from any of the cases set out at §§49-53 above.

"No clear rules": C's skeleton, §202

170. There is no reason of principle why a decision about whether the crime/iniquity exception to LPP applies requires independent determination, particular where (as here) it is attended with appropriate safeguards.

(V) CONCLUSION

171. In conclusion, for the reasons set out above, the Claimant's claim in reliance on Convention rights should be dismissed.

SIR JAMES EADIE QC
GERRY FACENNA QC
JULIAN MILFORD
MICHAEL ARMITAGE
IMOGEN PROUD

June 2019