Appeal Ref. CA-20220001019

IN THE COURT OF APPEAL (CIVIL DIVISION)
ON APPEAL FROM THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
DIVISIONAL COURT
[2019] EWHC 2057 (Admin)
Singh LJ and Holgate J

BETWEEN:

THE QUEEN
on the application of
THE NATIONAL COUNCIL FOR CIVIL LIBERTIES

Appellant/Claimant

– and –

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

Respondents/Defendants

-and-

NATIONAL UNION OF JOURNALISTS

Intervener

DEFENDANTS' SKELETON ARGUMENT

References to the Claimant's skeleton are in the form "CSkel§x", where "x" is the paragraph number.
References to the authorities bundle, core bundle and supplementary bundle are in the forms ***[AU/x/y], [CB/x/y]*** *and* ***[SB/x/y]*** *respectively, where "x" is the tab number and "y" is the page number.*
Suggested pre-reading:

- *The parties' skeleton arguments* **[CB/3], [CB/4]**
- *The ECHR and EU law appeal grounds* **[CB/1], [CB/2]**
- *The judgments of the Divisional Court from 2018 ([2019] QB 481), 2019 ([2020] 1 WLR 243) and 2022 ([2022] EWHC 1630 (Admin)* [**CB/29], [CB/30], [CB/31]**
- *The judgment of the ECtHR in Big Brother Watch v UK (2022) 74 EHRR 17* **[AU/56**]

A. INTRODUCTION AND SUMMARY

1. The Investigatory Powers Act 2016 ("**the Act**") replaced various surveillance powers in different enactments with a single, consolidated framework, containing substantially strengthened

safeguards and a guiding principle of the protection of privacy[1]. Among other matters, under the framework now in place:

(1) Warrants issued by the Secretary of State are now subject to the "double lock", under which (subject to limited and specific statutory exceptions) they are required to be approved by a Judicial Commissioner before they take effect. That applies to all warrants for targeted interception under Part 2; notices issued to telecommunications operators for the retention of communications data ("**CD**") under Part 4; warrants for targeted equipment interference ("**EI**") under Part 5; warrants for bulk interception of communications and secondary data, acquisition of communications data in bulk ("**BCD**"), and bulk EI under Part 6 Chapters 1, 2 and 3; and warrants for the retention and examination of bulk personal datasets ("**BPDs**") under Part 7.

(2) Information collected or retained under "bulk" powers in Parts 6 and 7 of the Act can be selected for examination only for specified "operational purposes", approved by the Secretary of State and overseen by the Intelligence and Security Committee of Parliament ("**ISC**") and Prime Minister.

(3) Most requests to acquire CD from telecommunications operators under Part 3 of the Act must be approved by an independent body (the Office of Communications Data Authorisations, "**OCDA**").

(4) Information held by the Security and Intelligence Agencies ("**SIAs**") about persons, the majority of whom are not likely to become of intelligence interest, is subject to an entirely new system of safeguards for BPDs, which requires their retention, handling and use to be authorised by warrant under Part 7 of the Act.

(5) The operation of each of the powers under the Act is subject to a new and comprehensive statutory code, which sets out revised and strengthened safeguards. There are also strengthened statutory safeguards for the protection (inter alia) of journalistic information and information subject to LPP. The Investigatory Powers Commissioner ("**IPC**") provides strengthened oversight over the powers under the Act, by comparison with the oversight bodies he has replaced.

[1] See s.2 of the Act **[AU/67/2644]**.

2. The overall conclusion of the UN Special Rapporteur on the Right to Privacy in relation to the Act was set out in observations following his 2018 mission to the UK:

"*While the new set-up may still contain a number of imperfections, the UK has now equipped itself with a legal framework and significant resources designed to protect privacy without compromising security. Given its history in the protection of civil liberties and the significant recent improvement in its privacy laws and mechanisms, the UK can now justifiably reclaim its leadership role in Europe as well as globally. For example, the UK is now co-leading with that tiny minority of EU states which have made a successful effort to update their legislative and oversight frameworks dealing with surveillance".*

3. The Claimant ("**C**") has mounted a "root and branch" challenge to Parts 3-4, 5, 6 and 7 of the Act as contrary to the European Convention on Human Rights ("**ECHR"**) and EU law. The Divisional Court ("**DC**") considered that challenge in great detail in three judgments from 2018 ([2019] QB 481, **"2018 J"**, [**CB/29]**), 2019 ([2020] 1 WLR 2043, **"2019 J**", [**CB/30**]), and 2022 ([2022] EWHC 1630 (Admin), **"2022 J"**, **[CB/31]**). The challenge was dismissed, save in limited respects which relate to EU law:

   (1) In 2018 J, the DC held that Part 4 of the Act was incompatible with EU law in two specific respects conceded by the Defendants ("**Ds**") following the judgment of the CJEU in *Tele2* and *Watson (Joined cases C-203/15 and C-698/15)* [2017] QB 771 (***"Watson CJEU"***) [**AU/15/477**]. Those were that in the area of criminal justice, access to retained data was not limited to the purpose of combating "serious crime", and was not subject to prior review by a court or independent administrative body. Otherwise, C's challenge to Parts 3 and 4 of the Act was dismissed. Parts 3 and 4 of the Act were subsequently amended following 2018 J. Parts of the EU law challenge were stayed, pending judgments of the CJEU in *Privacy International v SSFCO C-623/17* [2021] 1 WLR 4421 ("***Privacy International CJEU"***) [**AB/17/613**] and *La Quadrature du Net and ors v Premier Ministre and ors (C-511/18, C-512/18, C-520/18)* [2021] 1 WLR 4457 (***"La Quadrature CJEU"***) [**AU/18/649**].

   (2) In 2019 J, the DC dismissed Cs' ECHR challenge.

   (3) In 2022 J, the DC considered C's stayed EU law challenge following *Privacy International CJEU* and *La Quadrature CJEU,* and following the UK's exit from the EU. It held that the amendments to Parts 3 and 4 of the Act following 2018 J had not fully cured their incompatibility with (what was by then) retained EU law as set out in *Watson CJEU*. Specifically, the DC held that when the SIAs acquired CD under Part 3 not for national security purposes but for the purposes of preventing or detecting crime, they were required to

obtain prior independent authorisation in the same way as (for example) the police: §130. In all other respects, however, the EU law challenge failed.

4. In summary, Ds submit that the DC was clearly right to dismiss C's challenge save in the limited respects set out above, and these appeals should be dismissed accordingly, with one proviso. In 2019 J, the DC considered C's ECHR challenge against the principles set out in Strasbourg jurisprudence at that time. On 25 May 2021, the European Court of Human Rights ("ECtHR") Grand Chamber further developed those principles in *Big Brother Watch v United Kingdom* (2022) 74 EHRR 17 ("*BBW GC"*) [**AU/56/2204**]. Ds accept that in light of *BBW GC,* the legal framework created by and under the Act is currently incompatible with the ECHR in one particular way relating to bulk interception. The framework under Part 6 Chapter 1 of the Act does not currently provide for independent authorisation, where the SIAs either intend to select confidential journalistic material ("CJM") for examination from bulk intercept; or such selection is "highly probable"; or they intend to retain CJM which has inadvertently been selected for examination. As explained in a written Ministerial Statement to Parliament from the Home Secretary dated 31 March 2022 ("the 31 March 2022 WMS", **[SB/15]**)[2], the Government will be making necessary changes to the Act and Codes of Practice in due course.

5. The ECtHR's judgment in *BBW GC* also identified that there was a need for internal authorisation of "strong selectors" used to select material for examination from bulk intercept. At the time C lodged its appeal, the scheme under Part 6 Chapter 1 of the Act did not provide for this. However, the 31 March 2022 WMS makes clear that strong selectors are now applied. It states ([**SB/15/202**]):

   "*The Security and Intelligence Agencies use strong selectors to select data acquired under bulk interception warrants under Part 6 Chapter 1 of the IPA. Where those strong selectors are applied to identifiable individuals, prior internal authorisation will be required. Plans to implement this additional step already well-developed and are soon due to be incorporated into the systems used by the analysts within the Security and Intelligence Agencies. This will be accompanied by additional guidance and training."*

   For the avoidance of doubt, those changes have now been made, and the relevant SIAs' systems include these additional steps.

6. Therefore, save in relation to independent authorisation for CJM in the context of bulk interception, the legal framework under and in the Act is compatible with the ECHR and with retained EU law.

[2] https://questions-statements.parliament.uk/written-statements/detail/2022-03-31/hcws759

7. Ds set out below in turn: (i) their response to the ECHR appeal; and (ii) their response to the EU law appeal.

B. RESPONSE TO THE ECHR APPEAL

I Overview

8. The DC ([2020] 1 WLR 243, **"2019 J**") considered the ECHR compatibility of the Act over a five-day hearing with the benefit of extensive written evidence and submissions. C's appeal on ECHR grounds is in part simply a disagreement with the DC's conclusions, which rehashes the arguments that failed below; and in part a contention that the ECHR Judgment has been overtaken by the conclusions of the ECtHR Grand Chamber in *BBW GC*. Insofar as it is the former, the DC was manifestly right. Insofar as it is the latter, the implications of *BBW GC* for surveillance powers under the Act are much more limited than C suggests. Most importantly:

   (1) The ECtHR in *BBW GC* conducted a close analysis of the factual background to the operation of bulk interception, and repeatedly and explicitly confirmed that its detailed consideration of the safeguards necessary was made in the context of bulk interception. C's assumption that the reasoning of *BBW GC* on bulk interception applies to all forms of surveillance is unwarranted.

   (2) The ECtHR in *BBW GC* addressed the previous legal regimes for bulk interception and acquisition of communications data, contained respectively in s.8(4) and Part I Chapter II of the Regulation of Investigatory Powers Act 2000 ("**RIPA**") [**AU/68**]. The Act operates in a new way, with very substantially strengthened safeguards. Moreover, the ECtHR stated that the safeguards required should be considered in light of the content of the entire legal regime. That was also the way in which the DC approached the issues: see e.g. 2019 J at §193 (*"what has to be considered in the present context is the entire suite of interlocking safeguards…"*) [**CB/30/929**].

II Legal framework

9. It is common ground between the parties that the general legal test whether a secret surveillance regime is "in accordance with the law"/"prescribed by law" for the purposes of A8 and A10 ECHR requires that the domestic law is sufficiently clear to give citizens an adequate indication as to the circumstances in which and conditions on which public authorities are empowered to resort to such measures; and must indicate the scope of any discretion and the manner of its exercise

with sufficient clarity to give the individual adequate protection against arbitrary interference: see e.g. *Zakharov v Russia* (2016) 63 EHRR 17 at §§229-230 [**AU/49/1817**], *BBW GC* at §333 [**AU/56/2295**]. That general test is supplemented in *BBW GC* by particular requirements that apply to bulk interception. Cs elide that general test and the particular requirements of a bulk interception regime, when the judgment in *BBW GC* itself takes pains explicitly to separate them.

BBW GC

10. Unlike the bulk interception regime in Part 6 Chapter 1 of the Act, the regime under s.8(4) RIPA ("**the s.8(4) Regime**") considered by the ECtHR provided for no independent authorisation of warrants; did not include any requirement that selection for examination be for "operational purposes"; and had more limited protections *inter alia* for journalistic material.

11. The ECtHR carried out a detailed factual analysis of exactly how GCHQ used the s.8(4) power for foreign intelligence gathering and the identification of threats. It explained that intercepted material was either selected for examination using "*strong selectors*" linked to identifiable individuals, which were applied to all intercepted bearers; or was selected for examination using techniques applied to a subset of intercepted bearers. These latter techniques required the initial application of rules designed to discard material least likely to be of intelligence value, and then the application of "*complex queries*", designed to draw out material likely to be of the highest intelligence value: [17-18] [**AU/56/2210**]. The ECHR analysed the various stages of the power's use, commencing with the interception, filtration and initial retention of the post-filtration material ("Stage 1"); then the application of specific selectors to intercepted material to produce a list of items for potential examination, with the remainder being discarded ("Stage 2"); then the actual examination of items by analysts ("Stage 3"); and finally, the subsequent retention of data and use of the "final product", including data sharing. See §325 [**AU/56/2293**]. It observed that although A8 applied at each stage, the initial interception did not entail a "*particularly significant*" interference with individuals' rights, and the degree of interference increased as the bulk interception process progressed: §330 [**AU/56/2294**]. Its analysis was critically affected by that factual context.

12. Against that context, the ECtHR held as far as material as regards the s.8(4) Regime and compliance with A8:
    (1) In view of the proliferation of threats faced by States, and the existence of sophisticated technology enabling bad actors to avoid detection, the use of bulk interception to identify threats to national security was within States' margin of appreciation: §340 [**AU/56/2297**].

(2) In its case law concerning both targeted and bulk interception, in addition to the general test of foreseeability in *Zakharov,* the ECtHR had previously applied six "minimum requirements" that should be set out in law in order to avoid abuse of power: §§335, 341 (the "*Weber* criteria[3]") [**AU/56/2296- 2297]**. However, the nature and scale of bulk interception meant that the *Weber* criteria needed to be adapted to reflect "*the specific features of a bulk interception regime and, in particular, the increasing degrees of intrusion into the Article 8 rights of individuals as the operation moves through the stages identified in paragraph 325 above"*: §347 [**AU/56/2298**].

(3) In the context of bulk interception, the Court would therefore conduct a "*global assessment of the operation of the regime*", which focused principally on the existence of sufficient safeguards against abuse: §360 [**AU/56/2301**]. The assessment should apply 8 criteria: (i) the grounds on which bulk interception might be authorised; (ii) the circumstances in which an individual's communications might be intercepted; (iii) the procedure for granting authorisation; (iv) the procedures for selecting, examining and using intercept material; (v) the precautions to be taken when communicating the material; (vi) the limits on the duration of interception, the storage of intercept material and the circumstances of its erasure and destruction; (vii) the procedures for supervision by an independent authority; and (viii) the procedures for independent *ex post facto* review of compliance: §361 [**AU/56/2302**].

(4) Certain additional safeguards should apply to the transfer of material obtained by bulk interception to foreign states or international organisations (§362) [**AU/56/2302**]:

"First of all, the circumstances in which such a transfer may take place must be set out clearly in domestic law. Secondly, the transferring State must ensure that the receiving State, in handling the data, has in place safeguards capable of preventing abuse and disproportionate interference…"

(5) The ECtHR was "*not persuaded that the acquisition of related communications data ["RCD"] through bulk interception is necessarily less intrusive than the acquisition of content":* §363 [**AU/56/2302**]. On that basis, the interception, retention and handling of RCD should be analysed by reference to the same eight minimum safeguards applicable to content. However (§364) [**AU/56/2303**]:

"…as long as the aforementioned safeguards are in place, the Court is of the opinion that the legal provisions governing [the treatment of RCD] may not necessarily have to be identical in every respect to those governing the treatment of content".

[3] See *Weber and Saravia v Germany* (2005) 46 EHRR SE5 at §95 [**AU/31/1179]**.

(6) The s.8(4) Regime met the requirements of foreseeability under A8 as regards all of criteria (i), (ii), and (v)-(viii) of the eight criteria identified at §361 (as to which, see sub-paragraph (3) above), including the requirements for transferring material to foreign states. However, it had three defects as regards criteria (iii) and (iv):

i. The s.8(4) Regime lacked "*one of the fundamental safeguards…that bulk interception should be subject to independent authorisation at the outset*": §377 [**AU/56/2306]**;

ii. The application for a s.8(4) warrant did not have to include an indication of the categories of selectors to be employed, which meant that their necessity and proportionality could not be assessed at the authorisation stage: §381 [**AU/56/2307]**;

iii. It was of fundamental importance for *"strong selectors linked to identifiable individuals to be subject to prior internal authorisation"*. The s.8(4) Regime did not do this: §382 [**AU/56/2307**].

Although the Interception of Communications Commissioner provided "*independent and effective oversight*" of the Regime, and the Investigatory Powers Tribunal ("IPT") offered a "*robust judicial remedy*", those safeguards were insufficient to "*counterbalance the shortcomings highlighted at paragraphs 377-382*": §425 [**AU/56/2318**].

13. The ECtHR did not find that protections specifically for material covered by LPP were insufficient, notwithstanding that that had been an issue raised in submissions (see §321) [**AU/56/2292**].

14. As regards the s.8(4) Regime and A10, the ECtHR reasoned as follows at §§447-448 [**AU/56/2323**]:

"*447. Under the section 8(4) regime, confidential journalistic material could have been accessed by the intelligence services either intentionally, through the deliberate use of selectors or search terms connected to a journalist or news organisation, or unintentionally, as a "bycatch" of the bulk interception operation.*
448. Where the intention of the intelligence services is to access confidential journalistic material, for example, through the deliberate use of a strong selector connected to a journalist, or where, as a result of the choice of such strong selectors, there is a high probability that such material will be selected for examination, the Court considers that the interference will be commensurate with that occasioned by the search of a journalist's home or workplace; regardless of whether or not the intelligence services' intention is to identify a source, the use of selectors or search terms connected to a journalist would very likely result in the acquisition of significant amounts of confidential journalistic material which could undermine the protection of sources to an even greater extent than an order to disclose a source…Therefore, the Court considers that before the intelligence services use selectors or search terms known to be connected to a journalist, or which would make the selection of confidential journalistic material for examination highly probable, the selectors or search terms must have been authorised by a judge or other independent or impartial body invested with the power to determine whether they were "justified by an overriding requirement in the public interest"…"

15. On that basis, the ECtHR found that there had been a breach of A10, because the s.8(4) Regime did not provide for such independent authorisation: see §§456-457 [**AU/56/2326]**.

16. As concerns the regime under Part 1 Chapter II RIPA, the ECtHR simply adopted the reasoning of the First Section in its judgment of 13 September 2018: see §§521 and 527 [**AU/56/2339 – 2340**]. The First Section had concluded that Part 1 Chapter II RIPA was contrary to A8/A10, because it had the same defects which Ds had conceded meant that Part 4 of the Act was incompatible with EU law, and which were reflected in 2018 J: i.e., in the sphere of criminal justice, access to retained data was not limited to the purpose of combating "serious crime", and was not subject to prior review by a court or independent administrative body. Thus, Part 1 Chapter II RIPA was not "in accordance with the law" for the purposes of A8, or "prescribed by law" for the purposes of A10, because (and insofar as) it was contrary to domestic law, as interpreted in light of the CJEU's jurisprudence. See the First Section's Judgment at §467 (A8) [**AU/52/2088**] and §§497-499 (A10) [**AU/52/2096]**.

17. Importantly, therefore, the First Section's reasoning on Part 1 Chapter II RIPA (adopted by the Grand Chamber) was based not on the minimum safeguards required as a matter of Convention law under A8 or A10; but instead upon the failure of the regime to comply with domestic law.

III Ground 1 of the ECHR appeal: "Absence of Journalistic Protections"

18. The bulk interception regime under Part 6 Chapter 1 of the Act provides various specific protections for "confidential journalistic material" ("**CJM**") as defined in s.264 of the Act, and "sources of journalistic information" as defined in s.263, both in the Act and in the Interception of Communications Code of Practice ("**the Interception Code**"). Those are set out in the annex to 2019 J, §§52-56 [**CB/30/981**]. In brief:
    (1) Under the Act, where CJM is retained, the IPC must be informed (s.154) [**AU/67/2809]**; and where a targeted examination warrant is required to select for examination material either considered to be CJM, or for the purpose of identifying a journalistic source, the warrant application must so state (so that a Judicial Commissioner will consider the issue under the "double lock"): s.28(2) [**AU/67/2670]**. Also, the warrant can be issued only if appropriate and specific handling arrangements for the protection of such material exist: see ss.113 and 114 [**AU/67/2768]**.

    (2) Under the Code, when a person selects material for examination from bulk in order to identify a source or (in the case of the selection of content) to obtain CJM, they must receive the

approval of a senior official[4] from a different authority, who must be satisfied that appropriate handling arrangements are in place: see the Interception Code, §§9.85 – 9.87 [**AU/90/4464]**.[5] No selection for examination can take place prior to such approval. Also, reasonable steps must be taken to mark CJM or material identifying a source as confidential, where it is retained and disseminated to an outside body: §9.88 [**AU/90/4465]**.[6]

19. The DC in 2019 J held that those safeguards (together with the other general safeguards in the Act and Codes) were sufficient to comply with A10: §§293-352 [**CB/30/948 - 961]**.

20. Ds accept that the DC's conclusion has been overtaken by the reasoning in *BBW GC* at §§448-453 in one specific respect [**AU/56/2323]**. It is now clear that independent authorisation is required, whenever the SIAs either intend to select CJM for examination from bulk intercept; or such selection is "highly probable"; or they intend to retain CJM which has inadvertently been selected for examination from bulk intercept (and not only, for example, when a targeted examination warrant is needed for such examination/retention[7]). See *BBW GC* at §448 [**AU/56/2323**].

21. Ds do not accept that the DC's conclusion on A10 is otherwise vitiated by *BBW GC,* or indeed is wrong for any other reason, as asserted in CSkel§§20-24. Ds deal with Cs' assertions in turn below.

"The circumstances in which the protections apply": CSkel§20.

22. Each of the contentions in CSkel§20 is based on an over-wide reading of *BBW GC*. In this context, as in the appeal generally, C relies upon a decontextualised approach to the judgment, which ignores the central feature of the ECtHR's jurisprudence referred to by Laws LJ at §88 of *R(Miranda) v Home Secretary* [2014] 1 WLR 3140[8], that *"although the court's reasoning is*

[4] The term "senior official" is defined in s.145 of the Act.

[5] At the time of the initial drafting of this skeleton argument, the relevant guidance was contained in the 2018 Code, now superseded by the 2022 Code. The appropriate reference for the 2018 Code is §§9.84 – 9.86 [**AU/76/3523]**.

[6] 2018 Code, §9.87 [**AU/76/3523].**

[7] In broad terms, this applies where selection of material for examination uses criteria referable to an individual known to be in the British Islands, for the purpose of identifying the content of communications sent by or intended for that individual (known as "the British Islands safeguard"). See §44 of the annex to 2019 J, and s.152(3) of the Act [**AU/67/2806]**.

[8] The CoA allowed Mr Miranda's appeal against the Divisional Court's judgment, but nothing in the reasoning on appeal casts doubt on this principle.

sometimes expressed in very general terms…in this area as in others its method and its practice is to concentrate on the facts of a particular case" [**AU/3/119**].

23. *First*, as to CSkel§20.1, the context in which the ECtHR referred at §448 of *BBW GC* to search terms *"known to be connected to a journalist"* must be understood. The ECtHR's stated concern was to ensure independent authorisation for search terms which had the intention or highly probable result of selecting CJM for examination. In that context, the ECtHR referred in the first sentence of §448 to "*the deliberate use of a strong selector*[9] *connected to a journalist*" as an example of such a search term [**AU/56/2323**]. In other words, it assumed that where a "*strong selector connected to a journalist*" was applied, it would be used to obtain CJM, or would be highly likely to do so. The ECtHR did not consider, and was not asked to consider, what the position might be where a strong selector "*connected to a journalist*" was used in circumstances where there was no intention to select CJM, or where the use of the selector was not highly likely to have that effect. Yet such circumstances may undoubtedly occur. There is no reason of principle why such a search should require particular protection for the journalist under A10 ECHR. Nor is there anything in the Strasbourg case law to suggest that A10 safeguards should apply on a blanket basis to any communication of any journalist, irrespective of its nature. As the DC observed at §342, apropos of *Telegraaf Media v The Netherlands* (2012) 34 BHRC 193*, "it does not state that any documentation held by a journalist is protected, and indeed such a provision would be unworkable, applying to any interchange between a journalist and anyone else at all"* **[CB/30/959]**.

24. *Secondly*, as to CSkel§20.2, C's submission both (i) misunderstands the reasoning in *BBW GC* concerning the acquisition of CD under Part 1 Chapter II RIPA; and (ii) wrongly applies that reasoning to the bulk interception of communications.

25. C's assertion that independent authorisation should apply where it is "*likely*" that CJM will be selected for examination relies upon *BBW GC* at §525 [**AU/56/2340**]. There, the ECtHR recorded and applied the reasoning of the First Section that provisions for obtaining a court order under Part 1 Chapter II RIPA did not apply in *"every case where there was a request for the communications data of a journalist, or where such collateral intrusion was likely",* and the regime was therefore not "in accordance with the law" for the purposes of A10. However, as explained above, the First

[9] The Grand Chamber used the term "strong selector" as shorthand for specific identifiers linked to a particular target (such as an email address), as opposed to complex queries made up of a number of components. "Strong selectors", in the ECtHR's rubric, correspond to "simple selectors" as addressed at §17. See §§17, 327 [**AU/56/2185; 2294]**.

Section's reasoning was not concerned with the intrinsic requirements of A10. It was concerned with whether Part 1 Chapter II RIPA was consistent with domestic law. The First Section's reference to circumstances where collateral intrusion was "likely" denoted its assumption that A10 would be engaged in such circumstances, so that the regime under Part I Chapter II RIPA would need to meet the standards of domestic law as set out in 2018 J for the purposes of A10, as well as A8.

26. By contrast, the First Section did not say that independent authorisation was required as a matter of ECHR principle whenever collateral intrusion into a journalist's CD was *"likely*". Nor can it possibly have intended to do so. Unlike the Grand Chamber, the First Section's reasoning on the s.8(4) Regime did not state that independent authorisation was required at all before selecting CJM for examination from bulk intercept material. Rather, it held that the A10 complaint about the s.8(4) Regime gave rise to *"no separate argument over and above that arising out of Article 8",* so that it was unnecessary to consider it: §474 [**AU/52/2090**]. Yet the selection for examination of CJM from bulk intercept is undoubtedly likely to represent a greater interference with A10 rights, than the mere acquisition of CD. So it would make no sense if independent authorisation was required as a matter of ECHR principle for the latter, but not the former.

27. C's argument is also flawed, because it adopts a "pick and mix" approach to different parts of *BBW GC,* dealing with different subject matter. §§525-528 of *BBW GC* is concerned with the acquisition of CD under Part 1 Chapter II RIPA, not with bulk interception under the s.8(4) Regime [**AU/56/2340**]. The different requirements and different reasoning applying to one cannot be read across as if they applied to the other. In fact, it would be wholly illogical to do so. In the context of the s.8(4) Regime, the ECtHR explicitly stated at §448 of *BBW GC* that independent authorisation would be required if strong selectors were used, which made the selection for examination of CJM "*highly probable"* **[AU/56/2324**]. C's submission that the test is a lower one of mere "likelihood" assumes that the ECtHR did not mean what it said at §448, but that a different test applying to different subject matter should be applied instead.

28. *Thirdly,* as to CSkel§20.3, C both misrepresents Ds' position in their response to C's application for PTA[10], and misstates what the nature is of the requirement imposed by *BBW GC.*

29. At §448 of *BBW GC,* the ECtHR stated that relevant selectors or search terms must be authorised by an independent body "*invested with the power to determine whether they were "justified by an overriding requirement in the public interest"",* quoting from *Sanoma Uitgevers v The*

[10] See 4(b) of Ds' Submissions in Response to the Application for Permission to Appeal **[SB/10/185]**.

Netherlands [2011] EMLR 4 **[AU/56/2324]**. The need for an "*overriding requirement in the public interest*" to provide sufficient justification for an interference under A10(2) has been stated frequently in the ECtHR's case law, including in *Sanoma* and *BBW GC*. Its genesis is *Goodwin v UK* (1996) 22 EHRR 123, a case concerning whether a High Court order requiring a journalist to disclose a source constituted a violation of his A10 rights (see §39 of *Goodwin,* **[AU/27/1046**]). The condition of an "*overriding requirement"* reflects the importance attached by the ECtHR to the protection of journalistic sources for press freedom. It does not represent some separate, freestanding need for the language of "*overriding requirement"* 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. It would also be inconsistent with the reasoning in *Goodwin* (where the measure was "in accordance with the law" for the purposes of A10, although disproportionate, notwithstanding the fact that the language of "*overriding requirement*" was absent).

30. Ds of course accept that any independent body assessing whether to authorise the selection for examination or retention of CJM would need to assess whether the importance of the public interest at stake justified overriding the journalist's A10 rights. But that does not require the language of "*overriding requirement*" to be in the statutory scheme. And in any event, the Act already requires decision-makers determining whether CJM should be selected or retained to apply this test. It is a statutory requirement that selection for examination and retention of material intercepted under a bulk interception warrant be necessary and proportionate in all the circumstances: ss.150(6) and 152(1)(b) of the Act [**AU/67/2804]**. When those circumstances include the fact that the material selected for examination is CJM, the assessment of necessity and proportionality must properly entail consideration whether the interests pursued by the use of such search terms, or the use of such material, override the rights of individuals under A10. See also §§9.83, 9.85-9.89 of the Interception Code [**AU/90/4465]**.[11]

31. In short, the need for an "*overriding requirement in the public interest"* does not represent a reason for impugning the DC's judgment, separate from the requirement for independent authorisation itself. Any Judicial Commissioner (or other independent authority) determining whether to authorise the selection for examination or retention of CJM would be bound to apply the test of an "*overriding requirement in the public interest*", whether or not the statutory scheme so stated explicitly; and nothing in the DC's judgment suggests otherwise.

[11] 2018 Code, §9.82; §§9.84 – 88 [**AU/76/3524]**

"Various definitions in relation to CJM cut back the protections afforded, incompatibly with A10 (and A8)": CSkel§21

32. CSkel§21 does not relate to the reasoning in *BBW GC.* Rather, it repeats arguments made below, which were rejected by the DC for reasons which are plainly right.

33. As to CSkel§21.1 (the definitions of "journalistic material" and CJM in the Act), the DC clearly set out at §§340-347 of 2019 J the reasons why those definitions are consistent with Strasbourg case law on journalistic protections [**CB/30/959 – 960]**. Nothing in CSkel§21.1 suggests that those conclusions are wrong, and *BBW GC* does not touch on the point. C gives two instances of circumstances where it says the Act's protections are insufficient. As to those:

    (1) C argues in reliance on Cobain 1 (p.**) that information acquired by a journalist should be treated as "journalistic material", even if not acquired for journalistic purposes, because it might be used for journalism in the future. But this argument goes far too wide. In effect, it means any information ever provided to a journalist would need to be treated as "journalistic material". So the protections for CJM would need to apply to every interchange between a journalist and anyone else at all. That is an unrealistic position, unsupported by ECtHR jurisprudence, and the DC rightly rejected it at §342 [**CB/30/959]**.

    (2) C also asserts that public information a journalist gathers for their investigations would not be CJM, and would thus not be protected under the Act. But a communication containing such information would be CJM, if it were sent to another person in confidence. See the definitions at s.264(2) and s.264(6)(a) of the Act [**AU/67/2925]**. Moreover, the journalist's own work based on that information, while still in preparation, would in any other person's hands also be the subject of an implied obligation of confidence owed to him. The "draft news piece" at CSkel fn12 plainly would be protected on that basis.

34. As to CSkel§21.2, this argument again is untouched by any of the reasoning in *BBW GC* or any other Strasbourg case, and the DC was clearly right to reject it at §352 [**CB/30/961]**. The effect of s.264(5) of the Act is to exclude from the definition of "journalistic material" material that is "*created or acquired with the intention of furthering a criminal purpose*". So (to use C's example) a document in which a senior government official sought to further a criminal purpose would not itself be protected. However, a person who provided the document 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, just because the material in question is not "*journalistic material*" for the purposes of s.264 of the Act. Nor would the

definition in s.263 be disapplied, simply because the source had (again, to use C's example) acted unlawfully in disclosing the material. So the source (and journalist themselves) would benefit from the relevant protections for journalistic sources in the Codes and Act, as appropriate. The protections within and under the Act for "*confidential journalistic material*" and for "*sources of journalistic information*" overlap, but they do not depend on each other.

"Coextensive defects apply to other surveillance powers": CSkel§23

35. C's final complaint under this head at CSkel§23 is that equivalent requirements for CJM to those set out in *BBW GC* should be read across to other surveillance powers. But that complaint ignores the intensely context-specific nature of the reasoning in *BBW GC.* The core reasoning at §§447-448 of *BBW GC* is explicitly based on the nature of the interference with A10 rights effected by the operation of the s.8(4) Regime **[AU/56/2324**]. It is founded on the ECtHR's view that selection for examination using strong selectors against a "feed" of material from intercepted bearers is commensurate in intrusiveness to a search of a journalist's home or workplace: see §448 **[AU/56/2324**]. That same reasoning cannot be read across without more to the treatment of CJM within other surveillance powers, which operate in a different way and with a different level of intrusiveness. In such circumstances, applying *BBW GC* to other surveillance powers on a blanket basis would be contrary to the mirror principle, as explained in *R(AB) v Secretary of State for Justice* [2022] AC 487 at §§56-57 per Lord Reed **[AU/10/386**]. It would give rise to a particular risk of undermining the aim of the HRA to enable Strasbourg rights to be enforced domestically, by taking the protection of Convention rights further than the Court could be confident Strasbourg would go, in circumstances where Ds would have no right to apply to Strasbourg to correct any error.

36. C's purported reliance on *Ekimdzhiev v Bulgaria* (2022) 75 EHRR 8 (***"Ekimdzhiev 2"***) in this context at CSkel§23.3 is misplaced. The passage quoted by C (§395 of the judgment, [**AU/59/2520**]) does no more than refer to, and rely upon, the principles established in *BBW GC* itself as regards RCD obtained via bulk interception: see *BBW GC* at §§363-364 **[AU/56/2302**]. Those principles establish that where both content and RCD are obtained by bulk interception, as under the s.8(4) Regime, RCD should be subject to the same eight categories of safeguard; but per §364, the applicable legal provisions do not have to be the same in every respect.

37. Ds do not accordingly accept that the requirements for CJM in *BBW GC* as regards the s.8(4) Regime can be applied without more outside the bulk interception context. Specifically:

(1) The requirements plainly cannot be read across to Parts 3 and 4 of the Act and the acquisition of CD. In that context, *BBW GC* adopted the reasoning of the First Section, which said nothing about independent authorisation as a freestanding requirement of A10, when obtaining CD. If the ECtHR had intended that the same requirements applying to bulk interception should also apply to acquisition of CD, it could very easily have said so. But it did not. That is unsurprising. The acquisition of CD is intrinsically less sensitive in this context than the interception of content. CD might in combination with other information reveal a journalistic source, but it could not be "*journalistic material*", and would by definition not be CJM.

(2) The same points apply *mutatis mutandis* to the bulk acquisition of CD under Part 6 Chapter 2 of the Act.

(3) The requirements cannot be read across to EI under Part 5 or Part 6 Chapter 3 of the Act either[12]. Although only a very limited amount can be said publicly, the techniques for obtaining information via EI differ from the techniques for obtaining information via bulk interception. That in part reflects the fact that bulk interception requires tasking of particular means of communication in order to obtain information on an ongoing basis, which the ECtHR in *BBW GC* has assessed to involve a particularly high degree of potential intrusion when strong selectors are used; whereas EI is essentially "backward looking", insofar as it collects information held on equipment at a particular moment in time. See Montgomery-Pott w/s, §52, [**SB/17/232-233**]. That being so, and given the sensitivity of the ECtHR to factual context, this Court should not simply "read across" requirements for bulk intercept, as if they applied to EI. It would be important in this context to examine how EI actually operated (including, as necessary, with the use of CLOSED material) in order to be able properly to compare the two types of power.

(4) Finally, coextensive requirements can plainly not be read across to Part 7 of the Act. Part 7 of the Act is concerned with BPDs, that is, sets of information including personal data relating to a number of individuals, the nature of which is such that the majority of individuals are not, and are unlikely to become, of intelligence interest. Typical examples might be a spreadsheet of travel data from a port, or a list of visa applicants. Those are datasets which will

[12] *Contra* CSkel§23.5, Ds have not "conceded" that similar requirements should apply in all contexts to equipment interference, as to bulk interception. Rather, they accepted below that the A8 compatibility of equipment interference should like bulk interception (at that time) be assessed by reference to the *Weber* criteria.

intrinsically not be apt to contain CJM at all, though (as the BPD Code notes at §7.12, [**AU/79/3889**]) searches for journalistic sources could *"in rare cases be facilitated by the examination of data within BPDs"* [**AU/79/3889]**. So this is an entirely different factual context, much more closely analogous to the acquisition of CD than to bulk interception.

IV Ground 2 of the ECHR Appeal: "Absence of Safeguards in the Bulk Regimes and Part 5"

(a) CSkel§§26-29: "No independent authorisation of categories of search terms or warrant issue"

38. There are two insuperable problems with C's complaint that Parts 5, 6 and 7 of the Act do not comply with the requirement at *BBW GC* §354 that "*the types or categories of selectors to be used*" should be identified in any warrant for bulk interception [**AU/56/2300**].

39. *First*, the ECtHR was specifically and solely concerned with bulk interception, and the purposes for which and way in which it was conducted. It was not dealing with other surveillance powers. The very passage upon which C relies at §354 commences by stating that it sets out conditions "*taking into account the characteristics of bulk interception"* **[AU/56/2300**]. There is no basis for reading across its conclusions on bulk interception into other surveillance powers generally.

40. *Secondly*, Part 6 Chapter 1 of the Act clearly does require "*the types or categories of selectors to be used*" to be identified in the warrant. And for good measure, the same is also true of all the other impugned powers in Part 5, Part 6 Chapters 2 and 3, and Part 7 of the Act.

41. By contrast to the s.8(4) Regime, Part 6 Chapter 1 of the Act contains a new statutory requirement that the 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) [**AU/67/2796]**. Those "operational purposes" must be set out in a list maintained by the heads of the SIAs (s.142(4)) [**AU/67/2796]**; they may be specified only with the approval of the Secretary of State (s.142(6)) [**AU/67/2796]**; the Secretary of State may only give approval if satisfied that they are "*specified in a greater level of detail"* than the statutory purposes for which interception may be authorised (s.142(7)) [**AU/67/2797]**; a copy of the list of statutory purposes must be given to the ISC every three months (s.142(8)) [**AU/67/2797]**; and the Prime Minister must review the list at least once a year (s.142(10)) [**AU/67/2797]**. The Interception Code explains at §6.62[13] that: "*Operational purposes must describe a clear requirement and contain sufficient details to satisfy the Secretary of State that intercepted content or secondary data may only be selected for examination for specific reasons"*. When data is

[13] 2018 Code, §6.63 [**AU/76/3479]**.

selected for examination, the analyst must record why such selection is necessary and proportionate for one or more of the operational purposes set out in the warrant, and such explanation is subject to internal audit and external audit by the IPC: see §6.15 of the Interception Code[14] [**AU/90/4408]**.

42. Parallel requirements apply to all the other bulk powers in the Act. See s.161 (Part 6 Chapter 2) [**AU/67/2815]**; s.181 (Part 6 Chapter 3) [**AU/67/2832]**; ss.212 and 221 (Part 7) [**AU/67/2861 ; 2870]**.

43. There is no magic in the language "*types or categories of selector"* used by the ECtHR at §354 of *BBW GC* **[AU/56/2300**]. "Types" and "categories" are wide words. Their obvious purpose is to ensure that selection for examination is not at large, and subject to the wide discretion of the analyst; but is constrained by some limitation on what selectors may be used, which is written into the warrant. But as to what sort of limitation that must be, they are silent.

44. The statutory requirement for the warrant to set out the "operational purposes" for which material may be selected is precisely such a limitation. Its effect is to ensure that any selector used must seek information on defined subject-matter, set out in the warrant (say, hypothetically, "Child Sexual Exploitation".) A selector which only seeks such information is clearly a "type" or "category" of selector. C complains at CSkel§28.2 that it does not involve "*identifying individual selectors (such as a name or phone number*" or "*categories of them (such as people who use a particular discussion forum)".* But that approach seeks impermissibly to limit the meaning of "types or categories" in a way which suits C's argument. The ECtHR did not do so. That is unsurprising. It was intensely focused on the practicability of safeguards it set out, and it had been told (and recorded) that (i) many thousands of selectors might be used, which would sometimes need to *"change rapidly in order to keep pace with fast moving investigations and threat discoveries"* (§292) **[AU/56/2286**]; and (ii) bulk interception was used for the early detection and investigation of threats, not necessarily to target particular individuals (§345) **[AU/56/2298**]. So it would have been inconsistent with the characteristics of the bulk interception regime the ECtHR was dealing with for it to suggest that "types or categories" should be limited to a particular category of individual, rather than (say) a particular category of threat.

45. That is the answer to C's case on bulk powers. The answer to C's case on targeted examination warrants under Part 2 of the Act (see CSkel§27) and targeted EI warrants under Part 5 of the Act (see CSkel§28.1) is *a fortiori*:

[14] 2018 Code, §6.15 [**AU/76/3469].**

(1) A targeted examination warrant will authorise a person to select content for examination from bulk intercept material using criteria referable to an individual known to be in the British Islands at that time, for the purpose of identifying the content of communications sent by, or intended for, that individual (such examination being otherwise forbidden under the Act). For example, it will authorise a person to select content for examination using a telephone number of a person known to be in the British Islands, which will be stated in the warrant. See ss.15(3) [**AU/67/2656]** and 152(4) of the Act [**AU/67/2806]**. Such a criterion is the very paradigm of a "category" or "type" of selector.

(2) A targeted EI warrant under Part 5 of the Act will authorise a person to obtain communications, equipment data or other information falling within s.101 of the Act [**AU/67/2753]**. S.101 requires that the warrant relates to one or more specified matters in s.101(1)(a)-(h) (and the same applies *mutatis mutandis* to a targeted examination warrant under s.101(2)(a)-(e)). Subsections 101(1)(a)-(h) require the subject-matter of the warrant to be limited by reference to matters such as (i) equipment belonging to a particular person or organisation; (ii) equipment in a particular location; or (iii) equipment used for the purposes of a particular activity. It is difficult to know what could more obviously be a "category" or "type" of information[15].

CSkel§§30-33: "no requirement for internal authorisation of strong selectors"

46. In light of *BBW GC*, Ds have accepted that prior internal authorisation is required for the use of "*strong selectors linked to identifiable individuals*" to select data acquired under bulk interception warrants pursuant to Part 6 Chapter 1 of the Act. To that extent, Ds accept that the regime considered by the Divisional Court was not in accordance with A8. As explained at paragraph 5 above, the SIAs that use the bulk interception power have now amended their internal operational procedures to ensure prior internal authorisation when bulk interception systems are tasked with strong selectors to seek data referable to an identifiable individual.

47. However, for the reasons already set out, the "*strong selectors*" requirement that the Grand Chamber identified in relation to bulk interception cannot simply be transposed onto parts of the

[15] The use of the terminology "selector" is inapposite in the case of a targeted EI warrant under s.101(1) of the Act, because such a warrant does not authorise the collection of bulk material in the first place. S.101(2) of the Act is the equivalent for bulk EI of a targeted examination warrant under Part 2 of the Act i.e. it authorises the selection from bulk EI collected under Part 6 Chapter 3 of material which would otherwise contravene the "British Islands safeguard".

Act that deal with other investigatory powers. The ECtHR's findings in relation to internal authorisation at §§353-355 **[AU/56/2300**] and §382-383 **[AU/56/2307**] are, as explained, critically dependent upon the nature of bulk interception carried out under the UK regime. The ECtHR's conclusions were tied to the fact that "strong selectors" could be used to target particular individuals on an ongoing basis by selecting their communications from bulk intercept, although a targeted warrant would be needed to obtain equivalent information under s.8(1) RIPA. See e.g. §353: "*The use of selectors – and strong selectors in particular – is one of the most important steps in the bulk interception process, as this is the point at which the communications of a particular individual may be targeted by the intelligence services"* **[AU/56/2300**]. As to the suggestion that this requirement should be transposed into other powers:

(1) Part 5 is itself a targeted power. It authorises or requires the person to whom it is addressed to secure interference with equipment for the purpose of obtaining material falling within the specific categories at s.101(1)(a)-(h). That is a wholly different context. Material within the categories at s.101(1)(a)-(h) is intrinsically of intelligence interest, even if its collection involves significant amounts of data. There is no basis for reading across the "*strong selectors"* requirement in such circumstances, because the warrant itself already provides the type of safeguard to which the "*strong selectors"* requirement is directed.

(2) Part 6 Ch 2 concerns both a different type of data (i.e. BCD), and a very different factual context. The use of search terms against a "pool" of CD acquired from telecommunications operators ("TOs") is not the equivalent of the use of "strong selectors" to target individuals' communications on an ongoing basis. There is no equivalent within Part 6 Ch 2 of "stage 2" of the bulk interception process, as explained at §325(b) of *BBW GC*, where selectors are applied to material in order to determine what may be retained for potential examination by an analyst; and it is <u>that stage</u> to which the ECtHR applied the "strong selectors" requirement **[AU/56/2293**]. The ECtHR has never suggested that the search of a database for information about a particular individual intrinsically requires internal authorisation, as a precondition of compliance with A8. That reflects the fact that searching a pool of data provided by TOs for CD in relation to an individual is, in general terms, very much less intrusive than targeting them on an ongoing basis through the application of a "strong selector". Again, therefore, there is no proper basis to assume that the "strong selectors*"* requirement should (or realistically could) be read across to Part 6 Ch 2.

(3) Part 6 Ch 3 concerns bulk EI. As explained above, that is an intrinsically "backwards looking" power, insofar as it concerns access to stored data. Moreover, the techniques for obtaining

information by the use of EI vary, and are different from those used in bulk interception. As a result, EI may be used to obtain data by the use of evolving search terms which may relate to particular devices or individuals, but in circumstances where (i) the intrusiveness of doing so is not comparable to the intrusiveness of applying "strong selectors" to communications bearers; and (ii) the practicability of applying a requirement for internal authorisation of each search term may be considerably less. The EI Code of Practice provides a pertinent example at §6.5, relating to the use of bulk EI to obtain equipment data from a large number of devices in a specified location [**AU/78/3762**]. Further, and as explained at Montgomery-Pott w/s §52 ([**SB/17/232-233**]), those agencies that use bulk EI apply end-to-end safeguards that are consistent with the level of intrusion at each stage of the process. Given the differences between bulk interception and bulk EI, the appropriate safeguards for each power will not necessarily be the same; and Ds consider that safeguards proper to the nature of bulk EI are already applied by the SIAs. At the very least, therefore, it would be important carefully to examine the factual circumstances of the use of bulk EI – as might occur for example in CLOSED in proceedings in the IPT - before any assumption could be made that the "*strong selectors*" requirement should be read across.

(4) As to Part 7, the power to retain and examine BPDs is fundamentally different from the other bulk powers under the Act, in that it does not concern the exercise of any power to <u>obtain</u> information at all, but simply regulates the way in which the SIAs treat information obtained from a variety of sources in accordance with their statutory functions (including their general functions under s.2(2)(a) Security Service Act 1989[16] ("**SSA**") and ss.2(2)(a)[17] and 4(2)(a)[18] Intelligence Services Act 1994 ("**ISA**")). There is no basis for saying that the ECtHR would consider the same safeguards should apply to datasets obtained without use of intrusive surveillance powers, as to bulk intercept material: the reasoning of *BBW GC* is to the contrary[19].

[16] As regards the Security Service.

[17] As regards the Secret Intelligence Service.

[18] As regards GCHQ.

[19] Part 7 provides for the possibility of the Secretary of State making a direction, authorising a dataset obtained using other surveillance powers in the Act to be treated as a BPD: see s.225. However, any such direction would need to be approved by a Judicial Commissioner under the "double lock", and would require consideration to be given to whether regulatory provisions applicable to the original power under which the dataset was obtained should continue to apply: see e.g. BPD Code §3.7 [**AU/79/3849]**. If a direction were made authorising a dataset obtained under Part 6 Chapter 1 to be

CSkel§§34-38: "No objective and reasonable basis for any differential treatment of content and secondary data / communications data / non-protected material".

48. *BBW GC* states in terms that, in "*the context of bulk interception*", "*the legal provisions governing the treatment of related communications data do not necessarily have to be identical in every respect to those governing the treatment of content*": §416 **[AU/56/2315**]. What matters is that the legal provisions for the treatment of each category of material are sufficient in themselves to comply with Convention rights.

49. *BBW GC* also held in terms that under RIPA, it was justifiable for the "British Islands safeguard" not to apply to communications data: §421 **[AU/56/2317**]. *A fortiori,* that same conclusion applies equally to the Act: not least, because the safeguards for both content and communications data under Part 6 Chapter 1 of the Act are stronger and more extensive than was the case under RIPA.

50. Nothing in this sub-ground casts any doubt on the reasoning at §§171-178 of the 2019 ECHR Judgment [**CB/30/925 – 926]**. C derives no support from *BBW GC* on this point, which is a simple disagreement with the DC's conclusions. The DC properly and appropriately recognised that the acquisition of secondary data was not necessarily less intrusive than the acquisition of content; but rightly upheld Ds' argument that "*as a general rule*" the examination of the most sensitive content will raise greater concerns than the examination of secondary data. That conclusion not only reflects the ECtHR's own jurisprudence, but is common sense. In the context of terrorism or other serious crimes, for instance, the content of communications might reveal matters such as the intention, mindset and motivations of a subject of interest; their plans; and operational details of their activities: none of which would be apparent from metadata. On that basis, there is a proper objective basis for treating them differently. *Ekimdzhiev 2* does not suggest otherwise: see above.

51. As to C's contention that when BPDs are searched for content, no "British Islands" safeguard applies, that is wrong: (i) where BPDs contain content, such content is "protected data" for the purposes of Part 7 under s.203 of the Act [**AU/67/2853]**; (ii) s.202 provides that an intelligence service may not retain, or retain and examine a BPD in reliance on a class BPD warrant if the BPD

---

treated as a BPD under Part 7, the Secretary of State in making it, and a Judicial Commissioner in approving it, would need to consider what regulatory provisions were required by A8, including (where appropriate in light of the nature of the dataset) the "*strong selectors"* requirement. In practice, s.225 is most important as a means of ensuring that appropriate examination safeguards apply to "BPD-like" information obtained under targeted powers – e.g., a customer list attached to a target's email.

includes protected data [**AU/67/2852]**; (iii) if protected data is retained under a specific BPD warrant, and it is proposed to select it for examination on the basis of criteria referable to an individual known to be in the British Islands, then the Secretary of State may impose conditions in the warrant which must be satisfied before that can be done (s.207) [**AU/67/2857]**. So the Secretary of State must consider whether some form of British Islands safeguard should appropriately apply, in light of the nature of the material; and (iv) the Secretary of State must ensure that those conditions are met when selection for examination is effected (s.221) [**AU/67/2870]**.

52. Moreover, three further points should be noted. First, *BBW GC* did not suggest that the British Islands safeguard was required for compliance with A8 in any case, placing much more weight on the requirement for internal authorisation of "strong selectors" – see §421 [**AU/56/2317**][20]. Secondly, the nature of BPDs is not generally analogous to the nature of bulk intercept under Part 6 Chapter 1. Part 6 Chapter 1 is a foreign intelligence-focused power. The main purpose of a warrant under Part 6 Chapter 1 must be the interception of "*overseas-related"* communications and RCD: see s.136. The fact that Part 6 Chapter 1 concerns foreign intelligence is an important part of the context for the British Islands safeguard. That focus explains why it may be practicable and workable to apply the safeguard, when information collected under Part 6 Chapter 1 is searched for information about persons in the UK, because the use of the power for that purpose will be (comparatively) rare. It also explains why the safeguard may be appropriate to ensure that a foreign-focused bulk power is not used in circumstances where it would be appropriate and practicable to conduct targeted interception of a SOI in the British Islands. By contrast, Part 7 entails dealing with data of different types that may be acquired from a variety of different sources, and by different methods: see e.g. §4.31 of the BPD Code [**AU/79/3859**].

V Ground 3 of the ECHR Appeal: "Absence of safeguards when sharing material with overseas authorities"

53. In principle "sharing" of material with overseas authorities may take place in two ways, either by (i) allowing third party access to the material on the SIAs' systems; or (ii) providing copies of material to a third party. It is the latter about which C complains, and which is addressed below.

54. This Ground has two basic defects.

[20] The reasoning of *BBW GC* departs in this respect from the reasoning of the First Section: see §343 and §357 of the First Section's judgment [**AU/52/2056; 2060]**.

55. *First*, the relevant legal principles in *BBW GC* were specifically and explicitly concerned with the transmission of bulk intercept material to overseas states, not the transmission of intelligence material generally: see §362 of *BBW GC* **[AU/56/2302]** and the points already made above about the fact-sensitive nature of the judgment.

56. *Secondly*, and in any event, the ECtHR held that the provisions of the s.8(4) Regime for sharing intercept material with other States were compatible with Convention rights (see §§395-399, [**AU/56/2310**]); and the relevant provisions of the Act and Codes in relation to all the impugned powers contain either strengthened or at least materially equivalent protections by comparison to those applicable within the regimes replaced by the Act.

57. Dealing first with bulk intercept, by reference to CSkel§§41.2 and 43(b):

    (1) Under the s.8(4) Regime, disclosure overseas is addressed in ss.15(2)-(3) and (7) RIPA and §§7.3-7.5 of the RIPA Interception Code (in its last edition from 2016) ("**the RIPA Code"**) [**AU/81/4015**]. S.15(2) and (3) RIPA requires that intercepted material is copied and disclosed to the minimum extent necessary for the authorised purposes, and destroyed when no longer necessary. S.15(7) provides that requirements corresponding to those in s.15(2) should apply "*to such extent (if any) as the Secretary of State thinks fit*" when material is disclosed to overseas authorities. By §7.5 of the RIPA Code, where intercepted material is disclosed to a foreign state, the SIA must take "*reasonable steps"* to ensure that the authorities have procedures necessary to safeguard the intercepted material, and to ensure that it is disclosed, copied, distributed and retained to the minimum extent necessary. That includes that material must not be disclosed to a third country *"unless explicitly agreed"* and must be returned or destroyed when no longer necessary [**AU/81/4015**].

    (2) Under the Act, s.151 and s.150(2) and (5) [**AU/67/2803 - 2805]** are of equivalent effect to ss.15(2)-(3) and (7) RIPA. S.150(2) and (5) of the Act mirror s.15(2) and (3) RIPA. S.150(2) and (5) are disapplied in the case of disclosures to foreign states by s.150(7)-(8), but s.151 provides that requirements corresponding to those in s.150(2) and (5) should apply to overseas disclosures "*such extent (if any) as the Secretary of State thinks appropriate".* That is materially indistinguishable from the statutory test under s.15(7) RIPA.

(3) The Interception Code explains at §§9.28-9.29[21] [**AU/90/4451]** how the Secretary of State should approach the task of determining what safeguards it will be "appropriate" for a foreign state to apply:

"9.28…In most circumstances, intelligence sharing will take place with countries with which the United Kingdom has long and well established intelligence sharing relationships and which apply corresponding safeguards to material obtained under a warrant as those provided in the Act.
9.29 But there will also be occasions where material derived from interception warrants may need to be shared with a country overseas with whom we do not have an existing intelligence relationship and whose authorities do not apply safeguards to intercepted material corresponding to those in the Act. Issuing authorities will need to consider the arrangements that should be in place to regulate such disclosure. These should require the person considering authorising such a disclosure to balance the risk that the material will not be subject to the same level of safeguards that it would be in this country, against the risks to national security if material is not shared."

(4) §§9.28-9.29 of the Interception Code accordingly regulate the exercise of the SoS's discretion as to the overseas safeguards which should apply more tightly in some respects than the RIPA Code. They explain that countries with whom the SIAs customarily share intelligence apply equivalent safeguards; but that where intelligence must be shared with a country with whom the SIAs do not have an existing intelligence relationship, the SoS must apply a test which balances the risk of less stringent safeguards against the risks to national security of not sharing information. The Interception Code is less prescriptive than the RIPA Code only insofar as it does not provide for agreement as regards onwards disclosure to third states and destruction of material that is no longer needed; but safeguards relating to onwards disclosure and destruction must of course be applied to the extent the SoS considers appropriate under the scheme of the Act anyway. It is fanciful to suggest that *BBW GC* would have reached a different conclusion as to the adequacy of safeguards for overseas sharing, simply on the basis of that distinction. Nothing in *BBW GC* suggests otherwise.

58. The position as regards sharing with overseas authorities of material obtained under Part 5, Part 6 Chapter 2 and Part 6 Chapter 3 of the Act is materially identical to that regarding bulk interception under Part 6 Chapter 1.

59. As to BPDs under Part 7 of the Act:

(1) The SIAs (it being neither confirmed nor denied whether any of them transmit BPD to foreign partners) have explained and publicly disclosed that if they were to transmit BPD to foreign partners, they would (i) follow the principles and approach in their respective handling

[21] 2018 Code, §§9.28 – 9.29 [**AU/76/3510].**

arrangements and policy guidance; (ii) take into account the nature of the BPD to be disclosed; (iii) take into account the nature/remit of the body to which disclosure would be made; (iv) take into account the approach taken by any other SIAs who may have shared BPD, and have regard to protocols/understandings that may have been used or followed in such circumstances; (v) depending on the circumstances, seek assurances that the BPD in question would be handled in accordance with statutory safeguards i.e. disclosed, copied, distributed and retained only to the minimum extent necessary for authorised purposes; (vi) if relevant, seek assurances that its use was in accordance with the UK's statutory obligations; and (vii) share data on the basis that it must not be shared beyond the recipient organisation unless explicitly agreed in advance or approved through the Action-on process. See *Privacy International v (1) SSFCO (2) SSHD* [2018] UKIPTrib IPT_15_110_CH (23 July 2018) at §62 [**AU/89/4279]**.[22] The IPT held that in light of this statement, the arrangements for sharing of BPD under the previous regime were in accordance with the law under A8: see §71 [**AU/89/4285**]. That statement continues to apply. Nothing in *BBW GC* suggests that those publicly avowed principles in relation to overseas sharing of BPD would not satisfy A8.

(2) Further, the applicable regime for sharing of BPDs under Part 7 of the Act (and indeed in relation to sharing of information under other parts of the Act) now includes specific statutory provision as to transfers of personal data outside the UK by s.109 Data Protection Act 2018, which states [**AU/69/3267]**:

"(1) A controller must not transfer personal data to –
(a) a country or territory outside the United Kingdom, or
(b) an international organisation,
unless the transfer falls within subsection (2).
(2) A transfer of personal data falls within this subsection if the transfer is a necessary and proportionate measure carried out-
(a) for the purposes of the controller's statutory functions, or
(b) for other purposes provided for, in relation to the controller, in section 2(2)(a) of the Security Service Act 1989 or section 2(2)(a) or 4(2)(a) of the Intelligence Services Act 1994."

[22] The IPT's judgment, and the 2018 statement, addressed "sharing" both as it related to disclosing BPDs to foreign partners on the SIAs' own systems, and transmitting BPDs overseas. However, the former is now regulated by all the safeguards for examination in Part 7 IPA. The 2018 statement continues to apply to the transmission of BPDs overseas (which is not subject to the regime under Part 7 IPA: see §7.51 of the BPD Code, [**AU/79/3898**]). The IPT's judgment was upheld by the Divisional Court (Sharp P, Johnson J) on judicial review: see *R(Privacy International) v Investigatory Powers Tribunal* [2022] 4 WLR 75.

60. In light of the above, there is no reasonable argument that the regime for sharing BPDs is not in accordance with law in this regard.

VI Ground 4 of the ECHR Appeal: "Impermissibly Broad Bulk Personal Datasets Regime"

61. This Ground is unrelated to the conclusions of *BBW GC*. It is a simple disagreement with the DC's conclusions, in circumstances where the DC did not arguably err. There is no basis for impugning the DC's reasoning at §§210-240 of 2019 J [**CB/30/933 – 938]**.

62. The essential answer to the Ground is that it misunderstands what Part 7 of the Act does. Contrary to CSkel§47, Part 7 does not "*capture*" any information at all. Rather, it provides for a new and comprehensive system of safeguards within the Act and the BPD Code for the retention and handling of BPDs acquired under other powers (most materially, using the SIAs' general powers to obtain information in s.2(2)(a) SSA and ss.2(2)(a) and 4(2)(a) ISA). So *contra* CSkel§47, it is not a weakness but an obvious strength of Part 7 that it applies to BPDs of all types, including BPDs which contain content, health records, or other types of sensitive information. It means that all kinds of information within BPDs benefit from the protection of warrants requiring Judicial Commissioner approval, and from other safeguards within the Part 7 regime, including tailored safeguards for sensitive categories of information. In respect of BPDs, Part 7 provides exactly what *S and Marper v UK* (2009) 48 EHRR 50 requires: that is, clear, detailed rules and minimum safeguards governing the retention, use and destruction of information [**AU/37/1305**].

63. C's complaint about the "lack of safeguards" in Part 7 is at CSkel§48. There is nothing in any of the points made in that paragraph. As to the supposed defects to which CSkel§48 refers:
    (1) CSkel§48(i) is wrong. The Part 7 regime obviously does contain mandatory requirements for deletion of BPDs. BPDs can only be retained at all pursuant to a warrant.[23] If a warrant ceases to have effect, then BPDs must be deleted. That position is inherent in the entire scheme of Part 7. See s.200(1): "*An intelligence service may not exercise a power to retain a bulk personal dataset unless the retention of the dataset is authorised by a warrant under this Part"* [**AU/67/2851]**. Further, the BPD Code provides (see §§7.53-7.56, [**AU/79/3898]**) that:

[23] Subject to the limited "bridging" power under s.219 addressed by the DC at §§236-238 of 2019 J **[CB/30/938]**.

a. Each SIA must regularly review the operational and legal justification for its continued retention of each BPD retained under a class warrant, at intervals agreed with the Secretary of State and using a process set out in detail at §§7.53-7.54 [**AU/79/3898]**;
b. Where the continued retention of any data within a BPD no longer meets the tests of necessity and proportionality, all copies, extracts and summaries of it held within the SIA must be scheduled for destruction as soon as it is no longer needed for any authorised purpose: §7.55 [**AU/79/3899]**;
c. The retention of any BPD should be subject to scrutiny under an effective system to ensure (inter alia) that its retention remains necessary for the specified operational purposes (§7.56) [**AU/79/3899]**.

(2) CSkel§48(ii) is wrong. The BPD Code contains mandatory requirements to minimise the disclosure and copying of information in BPDs, which are supplemented by the general provisions regulating disclosure of information in s.2(2)(a) SSA and ss.2(2)(a) and 4(2)(a) ISA. For instance, by §§7.5, 7.9 and 7.50-7.52 of the Code [**AU/79/3886; 3898]**:
a. If individuals access information within a BPD with a view to its subsequent disclosure they may only do so if such disclosure is necessary for the performance of the statutory functions of the relevant SIA or for the additional limited purposes contained in the information gateway provisions in ss.2(2)(a) SSA, and 2(2)(a) and 4(2)(a) ISA.
b. Before disclosing information from a BPD, individuals must consider whether to do so would be proportionate, applying the detailed approach described at §§5.21-5.24 of the Code [**AU/79/3872]**;
c. The number of results presented for analysis from a BPD must be minimised by requiring queries to be framed in a proportionate way, and if necessary confining access to specific datasets (or subsets of them) to a limited number of analysts;
d. Disclosure of BPDs continues to be regulated by s.2(2)(a) SSA and ss.2(2)(a) and 4(2)(a) ISA. Those subsections impose a duty on the SIAs to ensure that there are arrangements in place to ensure inter alia that no information is disclosed by them, except so far as necessary for their functions or for the additional limited purposes in those subsections.

(3) CSkel§48(iii) is wrong. It is inaccurate to say that no "British Islands safeguard" applies to BPDs. Appropriately tailored safeguards for protecting the information of persons believed to be in the British Islands apply, albeit for good reasons they may not be identical to those in Part 6 Chapters 1 and 3 of the Act. See paragraphs 51 and 52 above.

(4) Finally, CSkel§48(iv) is wrong too. The safeguards regarding the sharing of BPDs with foreign partners have been addressed at paragraphs 59-60 above.

VII Ground 5 of the ECHR Appeal: "Absence of Adequate Safeguards for Lawyer-Client Communications"

64. The DC addressed the protections for lawyer-client communications in the Act at 2019 J §§271-292, and concluded that the rules regarding legally privileged items were set out in the Act and Codes with sufficient clarity and safeguards so as to avoid arbitrary interference, and render the statutory scheme compatible with A8: §292 [**CB/30/948]**. It addressed all C's complaints about the Act's provisions concerning LPP in detail, and held in the round that the Act contained a variety of special safeguards for different kinds of legally privileged material, which provided appropriate protection in the particular context. That conclusion is unaffected by *BBW GC*, and is plainly right.

65. Under Ground 5, C's primary argument is that the DC was mistaken, on the basis that requirements *"equivalent to those identified in BBW GC for journalistic material apply also to lawyer-client communications"*: CSkel§54. However, that contention is not supported by any of the case law that C cites, including *BBW GC* itself. To the contrary: in *BBW GC*, the argument was made that special protections were required for lawyer/client communications by the Law Society and International Council for Jurists (among others): see §§321-322 [**AU/56/2292**]. So the issue was squarely before the ECtHR. If the ECtHR had thought that equivalent safeguards should be applied to journalistic material and to lawyer/client communications, it would no doubt have said so. It did not.

66. Rather, the Strasbourg authorities on communications between lawyers and their clients, including all those relied upon by C, are authority for a general principle applying to all the ECtHR's case law in this area, which is that the extent of safeguards required will depend upon the level of interference with an individual's right to respect for private life. 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 the cases 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.

67. The basic Strasbourg principles concerning surveillance of lawyer/client communications are set out in *RE v United Kingdom* (2016) 63 EHRR 2 [**AU/47**]. *RE* concerned targeted surveillance of the content of lawyer/client communications in a police station, pursuant to an authorisation for intrusive surveillance under Part II RIPA. 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"* **[AU/47/1691**]. It stated for obvious reasons that the surveillance in question entailed a very high degree of intrusion into A8 rights, and held that in the circumstances the relevant provisions of Part II RIPA and the relevant code did not comply with A8. That was because they did not contain safeguards concerning the examination, use, handling and destruction of material obtained, equivalent to the more detailed safeguards applying in the context of the targeted interception of communications under Part I RIPA: §§131-141 [**AU/47/1694**]. The ECtHR had found the safeguards for targeted interception under Part 1 RIPA compatible with A8 in *Kennedy v UK* (2011) 52 EHRR 4 [**AU/39/1369**]. Notably, however, those safeguards did not include any requirement for independent authorisation (or an "*overriding public interest*"), before communications were intercepted, or viewed, or retained. So the reasoning in *RE* clearly does not support (indeed, is directly contrary to) any proposition that independent authorisation must be obtained as a precondition for lawfulness, before a lawyer/client communication is acquired, selected for examination, or retained.

68. As to the case law relied upon by C at CSkel§53, none of the cases implies, still less states, that judicial authorisation is a precondition for seizure or retention of lawyer/client communications, or that some formal test for an "overriding public interest" must be present before material is accessed (indeed, none of the cases use the rubric of "overriding public interest" at all):

    (1) *Michaud v France* (2014) 59 EHRR 9 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 A8 conferred "*strengthened protection"* for the confidentiality of lawyer/client exchanges (as per *RE v UK*), in view of the importance of the repercussions for the proper administration of justice (§§117-120 [**AU/44/1605**]): but held that the obligation on lawyers to report suspicions did not constitute a disproportionate interference with professional privilege: §131 [**AU/44/1608**]. Independent authorisation was not addressed.

    (2) *Wolland v Norway* (app. 39731/12, 17 May 2018) was a case concerning a search of the applicant lawyer's premises in the course of a fraud investigation. Privileged material was

seized. He complained that the seizure was unlawful, because even though the search had been authorised, domestic law did not permit him to review the seizure decision. The ECtHR rejected his complaint, holding that the relevant domestic law contained sufficient legal safeguards as respected the search, collection and seizure of material: §§71-73 [**AU/53/2143**]. The ECtHR did not consider whether prior judicial authorisation was a precondition for seizure of legally privileged material, so the fact that such authorisation happened to exist in the (lawful) circumstances addressed in *Wolland* cannot assist C's argument, *pace* CSkel§53.5(c).

(3) *Kopp v Switzerland* (1998) 27 EHRR 91 was a case where the Federal public prosecutor ordered monitoring of the lawyer applicant's professional and private telephone lines over a 3-week period, in order to identify a civil servant who might have disclosed official secrets. The monitoring required officials of the Swiss Postal Services to listen to conversations of the applicant and other lawyers in his office over all 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 required to listen to a multitude of privileged conversations, although the prosecutor's order stated that *"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, *"with no supervision by an independent judge*": §74 [**AU/28/1072**]. *Kopp* did not purport to lay down any general principle that any decision about whether to examine material subject to LPP should be supervised (let alone authorised *ex ante*) by an independent judge, as the DC rightly found at 2019 J, §288 [**CB/30/947]**.

(4) *Szabo and Vissy v Hungary* (2016) 63 EHRR 3 was not a case about lawyer-client communications, and §77 of *Szabo* does no more than purport to summarise principles from cases including *Kopp* **[AU/48/1706**].

(5) *Sallinen v Finland* (app. 50882/99, 27 September 2005) was a case about a search and seizure at a law office, in the course of which the police copied a hard disk containing information passing between the applicant lawyer and his clients. The Court noted that the search and seizure were "*rather extensive*" and was *"struck by the fact that there was no independent or judicial authorisation*": §89 [**AU/32/1206**]. However, this was not the reason given for the Court's finding of breach of A8; nor did the Court state that such authorisation was a precondition for compliance of A8. Rather, the Court found that the law governing the search

was insufficiently precise, because the relationship between the various relevant legal provisions was unclear, and gave rise to diverging views as to the extent of the protection for privileged material: §91 [**AU/32/1206**].

(6) *Heino v Finland* (app. 56720/09, 15 February 2011) is directly against C's argument. That was a case concerning the same Finnish law at issue in *Sallinen,* where the applicant lawyer's office was searched and documents were seized. Unsurprisingly, the ECtHR found that the law contained insufficient safeguards against abuse. It observed that (as in *Sallinen*) there was no independent or judicial supervision when granting the search warrant (§44) [**AU/41/1472**]. It then continued:

"*The Court notes that the absence of a prior judicial warrant may be counterbalanced by the availability of an ex post factum judicial review…However, in the present case the applicant did not have any effective access, a posteriori, to a court to have both the lawfulness of, and justification for, the search warrant reviewed*". The stated problem, therefore, was the lack of one or other of prior judicial authorisation or effective *ex post factum* review. The ECtHR has found both in *Kennedy* and *BBW GC* that the IPT provides such effective review.

(7) *Lindstram Partners v Sweden* (app. 18700/09, 20 December 2016) provides no support for C either. That was a case concerning a search warrant in criminal proceedings. The ECtHR stated that in such cases generally, "*elements taken into consideration*" in assessing the presence of effective safeguards against abuse include whether the warrant has been authorised by a judge: §95 [**AU/50/1870**]. The Court did not state that *ex ante* authorisation is required as a precondition of lawfulness in the case of a search involving material subject to LPP. *Wieser* is to the same effect.

69. In sum, C cites a large number of ECtHR authorities, on the apparent basis that weight of numbers can compensate for the fact that none of the cases supports the proposition for which it is cited.

70. That is a sufficient answer to C's arguments at CSkel§54, 55.1 and 55.2, which rely upon the absence of safeguards equivalent to those said to be required for CJM.

71. CSkel§55.3 makes the further argument that the BCD regime in Part 6 Chapter 2 of the Act "*contains no provision at all for lawyer-client communications",* which C says is incompatible with A8. But that argument was fully addressed in 2019 J at §§282 and 290-291 [**CB/30/946; 948]**. As the DC pointed out: (i) the general privacy duty in s.2 of the Act, to which the BCD Code makes specific reference in this context, includes a requirement for relevant authorities to take into

account the sensitivity of material subject to LPP; (ii) §§6.19-6.23 of the BCD Code explicitly direct officers to take particular care when selecting for examination the CD of persons known to be in sensitive professions (including lawyers); (iii) although CD may reveal when a communication occurred, it cannot reveal what was discussed or the subject matter (unlike, for example, the content of intercepted communications under Part 6 Chapter 1). It will not therefore touch upon the central purpose of legal privilege, to enable a client to disclose whatever he wishes to in order to obtain legal advice, without the fear of that material being disclosed to others without his consent. The DC found that in that context, the safeguards for lawyers' CD within the BCD regime were sufficient. It was entitled to reach that conclusion, and nothing in CSkel§55.3 suggests otherwise.

C. RESPONSE TO THE EU LAW APPEAL

VIII Overview

72. The background to the EU law aspects of the claim is set out in 2018 J, §§11-19 [**CB/29/852]**, and the more recent EU case law is summarised in 2022 J, §§41-51 [**CB/31/1008**].

73. As set out in paragraph 3 above, the DC considered the compatibility of Part 4 of the Act with EU law over a two-day hearing in February 2018, and held in 2018 J that Part 4 of the Act was incompatible with EU law in two specific respects conceded by Ds following the judgment in *Watson CJEU*, namely that, in relation to criminal justice: (i) access to and use of retained data was not limited to the purpose of preventing and detecting serious crime; and (ii) access to retained data was not subject to prior independent review. Three EU law issues were stayed to await the judgment of the CJEU in the reference made by the IPT in the *Privacy International* case. The EU challenge was otherwise dismissed.

74. Judgment in *Privacy International CJEU* was given by the Grand Chamber of the CJEU on 6 October 2020 alongside judgment in *La Quadrature CJEU*. The stayed aspects of the EU challenge were then considered by the DC, alongside C's EU law challenge to other "bulk" data provisions in the Act, at a two-day hearing on 17-18 May 2022. In 2022 J, the DC rejected all of the remaining EU arguments except to find that, when the SIAs acquired CD retained by TOs under Part 4 of the Act not for national security purposes but for preventing or detecting crime, they were required to obtain prior independent authorisation in the same way as (for example) the police: §130 [**CB/31/1026]**.

75. C's appeal on EU law concerns three aspects of 2018 J and 2022 J. C argues that:

(1) Contrary to the findings in 2018 J and 2022 J, Parts 3, 4, 5, Part 6 Chapters 1 to 3 and Part 7 of the Act are provisions for "general and indiscriminate" retention of, and access to, data within the meaning of retained EU law, and yet lack the safeguards that retained EU law requires in respect of such regimes (CSkel§§57.1, 75-90);

(2) the DC erred by holding that there is prior independent authorisation of access to data retained under the bulk powers because a bulk (or Part 5 thematic) warrant is initially authorised by a Judicial Commissioner ("JC"), whereas retained EU law requires authorisation of each particular access request (CSkel§§57.2, 91-97);

(3) The DC erred in not holding that the IPA breaches the requirements of Arts 7 and 11 of the EU Charter and/or equivalent general principles of retained EU law, for the same reason as it breaches Articles 8 and 10 ECHR. (CSkel§§57.3, 98-106).

IX Ground 1 of the EU Law Appeal: "The Act provides for general and indiscriminate retention and access"

76. Unbowed by the DC's rejection of equivalent arguments in both 2018 J and 2022 J, C renews before this Court its contention that the impugned provisions in the Act are unlawful because they fail to meet the requirements that (retained) EU law imposes in respect of "*general and indiscriminate*" regimes for the retention of, and access to, data.

77. It is a necessary (and express) premise of C's argument under Ground 1 of the EU law appeal that the relevant powers are "*general and indiscriminate*" in the sense in which that phrase has been used by the CJEU. C's skeleton argument on this ground of appeal is largely devoted to arguing that the DC's two carefully reasoned judgments on this very point are wrong. There is also a discrete issue as to whether Part 7 falls within the scope of EU law at all.

78. C is incorrect on both issues. The DC was correct to decide both that (i) none of the relevant powers in the Act is general and indiscriminate in nature, and that (ii) Part 7 (which merely concerns the way in which the SIAs handle data that they have already obtained under *other* powers) is outside the scope of EU law altogether. The "general and indiscriminate" and "Part 7" issues are considered in turn below.

(a) The "general and indiscriminate" issue (CSkel§§75-84 and §§87-90)

The notion of a "general and indiscriminate" regime in the CJEU jurisprudence

79. It is important, before considering C's specific arguments, to understand the way in which the notion of a "*general and indiscriminate*" regime has arisen in the CJEU's jurisprudence. Whereas C treats "*general and indiscriminate*" as if it were synonymous with "*bulk powers*", the reality is that the CJEU has used the phrase "*general and indiscriminate*" as a descriptor for various legal regimes which share key features with each another but which differ – radically – from the scheme set out in the Act. Thus:

(1) In *Watson CJEU*, the CJEU considered Swedish legislation that imposed an obligation on CSPs to retain "*all traffic and location data of all subscribers and registered users with respect to all means of electronic communications*" and to do so "*systematically and continuously, with no exceptions*": §97 [**AU/15/551**]. It was in light of those features that the CJEU (perhaps unsurprisingly) characterised the Swedish legislation as requiring the "*general and indiscriminate*" retention of data, and as a regime under which retention is "*the rule*" and not "*the exception*": §104 [**AU/15/552]**. Notably the CJEU did not describe DRIPA (the predecessor to the Act) as providing for "*general and indiscriminate*" retention, despite DRIPA being considered (alongside the relevant Swedish legislation) in the same judgment.

(2) In *Privacy International CJEU*, the CJEU considered section 94 of the Telecommunications Act 1984 ("**TA 1984**"), which allowed the Secretary of State to give such general or specific directions to CSPs as appeared to the Secretary of State to be necessary in the interests of national security or foreign relations. The CJEU emphasised that this direction-giving power enabled the Secretary of State to "*require [CSPs] to carry out the general and indiscriminate transmission of traffic data and security data to the security and intelligence agencies for the purpose of safeguarding national security*": §82 (emphasis added) [**AU/17/647]**.

(3) In *Le Quadrature CJEU*, the CJEU took as its starting point that the French and Belgian legislation considered in that judgment shared the feature that they imposed on CSPs "*an obligation requiring the general and indiscriminate retention of traffic and location data*": §81 (emphasis added) [**AU/18/745]**. That starting point reflected the fact that the three referring courts in that case had already concluded that the regimes in issue were general and indiscriminate, as is apparent from the terms of the three references set out at §68(1), §73(1), §79(1)-(2) of the CJEU's judgment [**AU/18/741 – 742]**. The CJEU's analysis in that case was therefore concerned with the extent to which general and indiscriminate regimes are permissible under EU law, and not with the logically prior question of what constitutes a general and indiscriminate regime (cf. §1 of the *dispositif*).

80. It is clear, therefore, that a critical feature shared by the legal regimes that the CJEU has characterised as "*general and indiscriminate*" is that those regimes required CSPs to retain all users' data of a prescribed type (or, in the case of the statutory provision considered in *Privacy International CJEU*, permitted the Secretary of State to achieve the same result by requiring CSPs to transmit all data of a prescribed type to the SIAs).[24] Thus, in its 2018 judgment in the *Watson* litigation, the Court of Appeal described the Swedish legislation considered in *Watson CJEU* as imposing a "*requirement of blanket retention of all communications data by all communications services providers*", and specifically rejected a submission that the CJEU's conclusions in relation to the Swedish legislation could be 'read across' to DRIPA (the Act's predecessor): [2018] EWCA Civ 70 at §26(2) (emphasis added) [**AU/9/360]**; see also 2018 J at §126, observing that the blanket nature of the requirement in the Swedish legislation "*precluded any possibility of any consideration being given to the nature of any connection between the data to be retained and the pursuit of the objective of fighting serious crime*" [**CB/29/877]**.

81. As the DC observed at 2018 J §127, the Act contrastingly does not require the "*blanket*" retention of communications data; indeed it does not impose "*any*" requirement on CSPs to retain data [**CB/29/877]**. Nor does the Act preclude the possibility of any consideration being given to the connection between the data to be retained and the objectives pursued by retention. In short, there is no question of any data ever being retained – let alone transmitted to the state authorities – by CSPs unless and until a "retention notice" has been given by the Secretary of State, with all the attendant safeguards (including judicial approval) surrounding such notices. That is why, in 2018 J, the DC observed at §137 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. The rigorous approach required by the 2016 Act will be reinforced when the provisions for judicial scrutiny are brought into force*" (as they now have been) [**CB/29/879]**.

82. Similarly, none of the bulk powers in the Act imposes a blanket requirement of retention / transmission to the State authorities. Rather:

[24] Similar features were exhibited by the German legislation described as "general and indiscriminate" by the CJEU in Joined Cases C-793/19 and C-794/14 *SpaceNet AG* (EU:C:2022:702). In his Opinion preceding that judgment (EU:C:2021:939), Advocate General Campos Sánchez-Bordona specifically emphasised that the German legislation in issue "*directly imposes a requirement to retain the data indefinitely*": §54 (emphasis added) [**AU/21/920**].

(1) In each case, there must first be a positive application by the "head of an intelligence service, or a person acting on his or her behalf" to the Secretary of State for a warrant issued in accordance with the relevant part of the Act: see respectively ss. 138(1), 158(1), 178(1), 102(1), 204(1) and 205(1) of the Act [**AU/67/2793 - 2855]**.

(2) Each of the bulk powers requires the Secretary of State to be satisfied as to the necessity and proportionality of the warrant for one or more of the specified statutory purposes:[25] see respectively ss. 138(1)(b)-(d); 158(1)(a)-(c); 178(1)(b)-(d); 102(1)(a)-(b); 204(3)(a) and b); and 205(6)(a) and (b) [**AU/67/2793 - 2855]**.

(3) The requirements of necessity and proportionality provide essential context to, and underpin the arrangements for, each of these bulk powers, both at the point of issuing a warrant (which must be of fixed duration) and at the point of any renewal. Thus, the contention at CSkel§78 that "*as long as the purpose of a "bulk" warrant is to safeguard national security…then any data can be retained*" is not correct.

(4) Each of the bulk powers is subject to approval by a Judicial Commissioner: see ss. 138(1)(g), 158(1)(e), 178(1)(f), 102(1)(d), 204(3)(e) and 205(6)(e) [**AU/67/2793 - 2855]**.

83. In short, there is no sense in which the Act itself requires the retention of any data. *A fortiori*, it does not require (or even permit) general and indiscriminate retention to occur.

84. No doubt in recognition of the clear differences between the Act and the regimes considered in the CJEU case law, C seeks to contend at CSkel§§77-80 that the relevant powers in the Act can be meaningfully compared with the provision that was described as "*general and indiscriminate*" in *Privacy International CJEU*, namely s. 94 TA 1984. It is ironic that C should draw such a comparison in circumstances where it argued before the DC in 2018 that a preliminary reference to the CJEU was required precisely because of the differences between the Act and the s. 94 TA 1984 power, the latter of which was at the time the subject of a pending reference in *Privacy International CJEU*.

85. In any event, the comparison C now seeks to draw is inapt:

[25] And, in relation to the powers in Part 6, Chapters 1 to 3 and Part 7 and that each of the "specified operational purposes" in the warrant is or may be necessary, and that the examination of the data for each such purpose is necessary on any of the grounds on which the warrant is itself considered to be necessary.

(1) As recognised at CSkel§76, the critical feature of s. 94 TA 1984 for the purposes of the CJEU's analysis in *Privacy International CJEU* was that "*All communications data could be required to be transmitted and, once transmitted, accessed*" (emphasis added). A direction to this effect would result in transmission to the State authorities of data that is "*comprehensive in that it affects all persons using electronic communications services*": *Privacy International CJEU* at §80, emphasis added [**AU/17/647**]. In other words, a s. 94 TA 1984 direction could result in the same situation as obtained under the Swedish legislation considered in *Watson CJEU*. Such a situation would entail "*general access to all retained data, regardless of whether there is any link, at least indirect, with the aim pursued*": ibid, §78 [**AU/17/647**].

(2) The suggestion by C that the Act exhibits similar features is hopeless. It is based essentially on the proposition that the bulk powers "*permit the retention and access of vast amounts of data about persons who are not likely to be of any legitimate interest to the authorities*": CSkel§77 (emphasis added). But this ignores the fact that, as set out above, the bulk powers may only be exercised in the first place pursuant to a judicially-approved warrant and subject to the range of other interlocking safeguards under the Act. The same is true of retention notices under Part 4 of the Act. The fact that the operation of that system may, depending on the outcome of the operation of the warrantry regime under the Act, result in a large amount of data being retained does not mean that such retention is "*general and indiscriminate*" in the sense in which that phrase has been used by the CJEU. Otherwise, all bulk powers would – by definition – be "*general and indiscriminate*".

(3) The fact that the bulk provisions do not contain any provision requiring warrants to be narrower than directions under s. 94 TA 1984 (cf. CSkel§78) is also nothing to the point. The breadth of a warrant under the Act will be determined by operation of the restrictions and safeguards in the Act, including judicial approval: this is the opposite of an indiscriminate power, and insofar as it is results in the generalised collection of data, this could only occur where generalised retention is itself necessary and proportionate to the objectives pursued (and judicially approved on that basis).

(4) Accordingly, in circumstances where the Act "*imposes a set of detailed interlocking safeguards...which did not previously apply...under the 1984 Act*" (2019 J §260 [**CB/30/942]**), C's comparison between the Act and s. 94 TA 84 is unilluminating.

86. Thus, even before considering the specific errors that C purports to identify in the DC's judgments on this issue, it is plain that C's attempt to characterise the Act as providing for "*general and*

indiscriminate" retention involves a category error. It rests on the premise that the bulk powers (and the access/retention powers in Parts 3 - 4 of the Act) are *ipso facto* general and indiscriminate because of the quantity of data that may in principle be encompassed by such powers. But the CJEU has never conflated bulk powers with "*general and indiscriminate*" powers in this manner.

Alleged errors in the DCs' judgments on the "general and indiscriminate" issue

87. Having adopted the mistaken approach to the issue described above, C contends that the DC's conclusion that the relevant powers in the Act are not general and indiscriminate is incorrect in two respects.

88. The **first** error C purports to identify (Cskel§82) is that the DC in 2022 J applied the same reasoning to the bulk powers as it did when concluding in 2018 J that the Part 3 – 4 powers were not general and indiscriminate in nature. C argues that this approach was wrong because the bulk powers are "*broader*" than those in Parts 3 – 4 of the Act: CSkel§82. However, the fact that C is able to identify differences between the bulk powers and the powers in Part 3 – 4 (e.g. that the former provide for the possibility of obtaining the content of communications) is neither here nor there. The key point is that, just like Parts 3 – 4 of the Act but unlike the regimes considered by the CJEU in the cases referred to above, the bulk powers do not require (or permit the Secretary of State to require) the blanket retention or transmission of data, precisely because of the interlocking safeguards that apply to all relevant powers in the Act. As above, the fact that the bulk powers may be used to obtain large quantities of data, much of which will be of "*no interest*" to the SIAs, does not make those powers general and indiscriminate.

89. The **second** set of alleged errors concerns the reasoning in 2018 J at §§118-138, which led the DC to conclude that the Part 3 – 4 powers were not general and indiscriminate [**CB/29/875 – 879]**. C contends that the DC's reasoning here was incorrect in three respects:
    (1) First, C argues that the DC in 2018 erroneously "*elide[d] the nature of the regime for collection with the safeguards for access*"; that a general and indiscriminate regime is "*characterised by the absence of a link between any criminal suspicion (or other ham to the interest protected) and the data collected*"; and that *Privacy International CJEU* and *La Quadrature CJEU* have since made clear that "*the critical question is the scope of obtaining and retention, and not (for example) safeguards on access or ability to seek review of a retention notice*": CSkel§83.1 (emphasis in original). However:
        a. It is true that the CJEU's case law has emphasised the need for "*clear and precise rules"* concerning both "*the scope and application*" of the measures in question and the imposition of "*minimum safeguards*". C wrongly suggests that this is a development

arising from *Privacy International CJEU* and *Le Quadrature*, when in fact this was a central feature of the CJEU's judgment in *Watson CJEU*: see §109 of the latter judgment [**AU/15/553]**.

b. In any event, C's argument fails to recognise that the "*scope*" of the data that will be retained or accessed under the Act is itself a result of the safeguards that the Act puts in place. Contrary to the impression given by C, those safeguards do not just concern "*access*", but also bear on the nature and extent of the data that can be retained / transmitted to the State in the first place. Thus, taking retention notices as an example, the power to issue such a notice cannot be exercised unless the Secretary of State considers it both necessary and proportionate for one or more of the purposes listed in s. 61(7) of the Act **[AU/67/2707]**; the Secretary of State must also have regard to the range of matters specified in s. 88(1) of the Act and consult with the relevant operator under s. 88(2) of the Act before issuing a notice**[AU/67/2742]**; and the notice must be approved by a Judicial Commissioner under s. 89 of the Act **[AU/67/2743]**. Equivalent restrictions apply to all of the bulk powers. *Pace* CSkel §83.1, these are not "*safeguards on access*" but constitute clear and precise rules concerning the "*scope of obtaining and retention*". These rules were central to the DC's reasoning at §§118-138 of 2018 J [**CB/29/875 – 879]** (and, by incorporation, its reasoning at §140 of 2022 J [**CB/31/1028]**).

(2) Secondly, C contends (CSkel§83.2) that the DC in 2018 took the "*flawed*" approach of eliding the Swedish regime considered in *Watson CJEU* with "*general and indiscriminate*" retention under EU law, and wrongly assumed that "*[a]nything less*" than a blanket retention requirement on CSPs was not general and indiscriminate. But the DC did no such thing. It is true that the DC referred to the Swedish legislation at 2018 J §127 **[CB/29/877]** (and emphasised how different it was from the Act), but this was entirely appropriate given that it was the Swedish legislation that was characterised as "*general and indiscriminate*" in *Watson CJEU*. The DC did not commit the error of "*treating the example as the test*": it did not simply proceed from the premise that the Act differed from the Swedish legislation to the conclusion that the Act was not general and indiscriminate in nature. Rather, its conclusion was based on a detailed consideration of the specific features of the Act and their effect on the nature and scope of the data that could be retained thereunder. As set out above, those features distinguish the Act not only from the Swedish legislation but also from other regimes which the CJEU has described as general and indiscriminate.[26]

[26] Ds do not necessarily accept the contention at CSkel§83.2 that the regimes at issue in *Privacy International CJEU* and *Le Quadrature CJEU* were "*far more limited*" than the Swedish legislation

(3) Thirdly, and finally, C argues that the DC erred in concluding at 2018 J §136 that even if the retention notices issued under Part 4 were "*as broad in scope as the statute permits*", they would nevertheless not be general and indiscriminate because of the seven restrictions and safeguards to which the DC had referred [**CB/29/879]**. C asserts that the DC here failed to recognise that "*if such wide retention may be required, then the features relied on by the DC do not limit the discretion to require retention*", and that the Act "*thus permits general and indiscriminate retention*": Cskel§83.3, emphasis in original. But that argument involves a clear logical error. The fact that the operation of the restrictions and safeguards in the Act may in practice result in "*wide*" retention of data does not mean that the restrictions and safeguards have not had any effect on the discretion to require retention. Rather, *ex hypothesi*, those restrictions / safeguards will have required the Secretary of State to justify (and secure judicial approval) of "*wide*" retention. As above, that is the antithesis of a regime that requires wide retention as the rule rather than the exception.

Permissible purposes for general and indiscriminate retention

90. For the reasons given above, the DC was correct in both 2018 and 2022 to conclude that the impugned provisions of the Act are not general and indiscriminate. In the circumstances, the submissions at Cskel§§87-90 concerning the purposes for which general and indiscriminate retention is permissible in (retained) EU law do not arise. In any event, those submissions are misconceived:

(1) The contention at Cskel§88 that general and indiscriminate retention and access is only permissible for the purpose of "*preventing the most serious threats to national security*" (emphasis added) is simply wrong. C purports to derive this principle from *Le Quadrature CJEU*. But that judgment contains no such limitation on the use of general / indiscriminate powers. Rather, at §135, the CJEU described a notion of national security that [**AU/18/756**]:

"…encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in

---

considered in *Watson CJEU*. But in any case, as explained above, the key feature shared by all of these regimes is that they required (or, in the case of s. 94 TA 84, permitted the Secretary of State to require) the blanket retention / transmission of data. As set out above, it is also to be noted that the three referring courts in *Le Quadrature CJEU* had themselves already concluded that the regimes in issue were general / indiscriminate, and this was therefore the starting point (not the conclusion) of the CJEU's analysis at §§81ff.

particular, of directly threatening society, the population or the State itself, such as terrorist activities".

(2) It is therefore clear that "*safeguarding national security*" in this context includes addressing both economic and (at least insofar as terrorism is concerned) criminal threats to national security.[27] Nor did the CJEU purport to give an exhaustive account of matters falling within the scope of national security: a matter which the CJEU would no doubt regard as primarily for the EU Member States to determine.[28] Accordingly, and contrary to Cskel§89, the fact that (e.g.) thematic equipment interference warrants under Part 5 may be issued for purposes concerning serious crime, economic well-being and the prevention of death/injury does not render those purposes unlawful, even if (which is denied) the power in question is properly characterised as general and indiscriminate.

(3) C also identifies no authority for the proposition at Cskel§90 that the powers in Part 6 permit the retention and accessing of data for a collateral purpose. To the contrary, it follows from §135 of *Le Quadrature CJEU* (quoted above) that retention and/or access in the interests of economic well-being or serious crime may itself fall within the scope of national security (which is not a concept that is the subject of any autonomous definition in retained EU law).

(b) The "Part 7" issue (Cskel§§85-86)

91. The DC was also correct to hold at 2022 J §139 that Part 7 of the Act does not fall within the scope of retained EU law at all [**CB/31/1028]**. Part 7 does not contain any power to acquire information at all, still less impose any duty upon CSPs to provide information to the SIAs. Rather, it concerns how the SIAs should handle BPDs that they have already obtained under other powers. But processing by the SIAs themselves is outside the scope of retained EU law: see/compare *Privacy International CJEU* at §§45-46 **[AU/17/640**].

[27] The reference at *Quadrature* §135 to threats capable of "*seriously*" destabilising constitutional, economic (etc.) structures does not in Ds' submission add anything of substance. It is very difficult to conceive of such matters being "*destabilised*" in a way that would not be "*serious*".

[28] That is consistent with the domestic approach. Successive UK governments have avoided defining in statute "national security" so as to preserve the flexibility to apply the term to new threats that may emerge. In *Secretary of State for the Home Department v Rehman* [2001] UKHL 47 at §50 Lord Hoffman held that *"…there is no difficulty about what 'national security' means. It is the security of the United Kingdom and its people*" [**AU/1/45**]

92. C's attempt to identify an error in the DC's analysis on this issue gives the game away. C concedes that the DC was correct to observe that "*Part 7 does not contain any power to acquire information, still less impose a duty upon CSPs to provide information to the state*": CSkel§86.1. But that is precisely why Part 7 falls outside the scope of retained EU law, which for present purposes only 'bites' on "*operations processing personal data carried out by [CSPs]... including processing operations resulting from obligations imposed on those providers by public authorities*": *Privacy International CJEU* at §46 (emphasis added) [**AU/17/640**]. Where data that has already been obtained by an intelligence service from a CSP under another part of the Act is retained/examined pursuant to a direction under Part 7 (s. 225) of the Act, there is no relevant "*processing operation*" by a CSP.

93. None of this means that the State can "*avoid the requirements of retained EU law by placing the retention provisions in another section of legislation and making them more generally applicable (as Part 7 does)*" (cf. CSkel§86.1, emphasis added). The requirements of retained EU law are fully in play – and are not avoided - at the point at which the relevant data are obtained by the intelligence service from the CSP concerned. For that reason, and *pace* CSkel§86.2, the claimant in *Privacy International CJEU* was correct to concede that a regime that does not require controllers to provide BPDs to an agency is "*outside the scope of EU law*" (cf. 2022 J §139 [**CB/31/1028]**).

X Ground 2 of the EU Law Appeal: "Absence of Prior Independent Authorisation outside National Security in the Bulk Provisions"

94. By Ground 2 of the EU Law Appeal, C takes issue with the DC's conclusion at 2022 J, §145, that *Watson CJEU* does not require the Act to make provision for separate independent authorisation each time that retained data is selected for examination or accessed for a purpose outside national security. The DC found that *Watson CJEU* did not identify any such requirement and that the requirement under the Act for Judicial Commissioner approval of a bulk warrant to obtain retained data, reinforced by the statutory safeguards summarised in the Annex to 2019 J, §§42-65, is sufficient to meet the EU law requirement for prior independent authorisation [**CB/30/978 – 983]**.

95. CSkel§95 argues that *Watson CJEU* distinguishes between prior authorisation of retention and prior authorisation of access and that §120 of *Watson CJEU* "*envisages separate authorisation for access on a case-specific basis*" beyond any authorisation for retention.

96. It is correct that *Watson CJEU* deals separately with *retention* and *access*. §§62-112 *Watson CJEU* addresses "*The first question in Case C-203/15*" (i.e. *Tele2,* the Swedish reference), namely whether EU law permits national legislation such as the Swedish legislation, providing for general and indiscriminate retention by communication service providers. §§113-125 *Watson* CJEU then address "*The second question in Case C-203/15* [*Tele2*] *and the first question in Case C-698/15* [*Watson*]", namely whether EU law "*precludes national legislation governing the protection and security of traffic and location data, and more particularly, the access of the competent national authorities to retained data…where that access is not subject to prior review by a court or an independent administrative authority*" (*Watson CJEU*, §114, emphasis added, [**AU/15/554**]).

97. The reference to "access" in *Watson CJEU* is to the ability of national authorities to *obtain* retained data from communications service providers. That is clear from the relevant reasoning in *Watson CJEU*, which refers to:

(1) "*national legislation governing the conditions under which the providers of electronic communications services must grant the competent national authorities access to the retained data*" (§116) [**AU/15/554**];

(2) "*clear and precise rules indicating in what circumstances and under which conditions the providers of electronic communications services must grant the competent national authorities access to the data*" (§117) [**AU/15/554**]; and

(3) "*access of the competent national authorities to retained data …* [and] *the conditions under which the providers of electronic communications services must grant such access*" (§118) [**AU/15/555**].

98. The reference to "access" in *Watson*, §120 is therefore to national authorities obtaining retained data held by communication service providers [**AU/15/555**]. It does not relate to decisions by national authorities to select or examine items of data that they already hold, e.g. the SIAs' selection for examination of material collected pursuant to bulk interception under Part 6 Chapter 1 of the Act. That was not in issue in *Watson CJEU*.

99. The DC was accordingly correct to find that there is no requirement for "*separate authorisation for access on a case-specific basis*", and that the *Watson CJEU* requirement for prior authorisation for "access" to retained data is met by the existing safeguards and arrangements, notably the requirement for approval by a Judicial Commissioner of a bulk warrant authorising the obtaining of retained data from communication service providers.

100. The Act requires a reasoned application to be made when any bulk power is sought to be used, and the initial issuing of a warrant is subject to approval by the Judicial Commissioners (which will be *prior* approval, except in an urgent case). That is one of the numerous interlocking safeguards that apply to obtaining (i.e. accessing) data, and further interlocking safeguards apply to the subsequent use of such data. A warrant under Part 6 will authorise both the obtaining and examination of data for specified operational purposes, and examination can only be carried out for the purposes set out in the warrant, which will have been considered by a Judicial Commissioner.

101. C's approach assumes that that the requirements of *Watson CJEU*, which concern 'access' by state authorities to the retained data held by CSPs, can be "read across" to apply to internal activities such as the selection by the SIAs of material from data they already hold, imposing a requirement on them to obtain prior independent authorisation each time such data is accessed. There is no such requirement in EU case law. Moreover, given the way in which bulk data is used, e.g. for target discovery, such a requirement for independent authorisation every time a new piece of information is uncovered and accessed, relating to a new individual, would be wholly impracticable and unrealistic.

102. There is no inconsistency between the DC's obviously correct finding on this point and the finding at 2022 J, §§121-132 that, when the SIAs obtain CD under Part 3 of the Act for the purposes of preventing or detecting crime, they should be required to obtain prior independent authorisation, like the police **[CB/31/1025 – 1026]**. That finding properly applies *Watson CJEU*, §120 to the act of *obtaining* communications data from communications service providers and not, as C would have it, to the act of examining and accessing data that a competent authority already holds.

XI Ground 3 of the EU Appeal: "At Least Equivalent Protection under the Charter to the ECHR"

103. By Ground 3 of the EU Law Appeal, C argues that the DC erred in not holding that the Act automatically breaches the requirements of Articles 7 and 11 of the EU Charter and/or equivalent general principles of retained EU law, for the same reason as it has been conceded to be incompatible with Articles 8 and 10 ECHR following *BBW GC*. (CSkel, §§57.3, 98-106). Essentially, C maintains that relevant rights under EU law are at least as extensive as the rights under the ECHR, and the DC was obliged to find that any breach of the ECHR was also a breach of EU law.

104. Ds submit that the reasoning of the DC at 2022 J, §§151-158 discloses no error of law [**CB/31/1030]**.

105. First, it is clearly correct that *BBW GC* was not binding on the DC, although the DC had a duty to take it into account where relevant under section 2 of the Human Rights Act 1998. The fact of the May 2021 judgment in *BBW GC*, and Ds' concessions which followed it, did not impose any duty or obligation on the DC to grant C a remedy (whether under the Human Rights Act, EU law or otherwise) at the time of the second EU law hearing in May 2022, when the DC had already decided the arguments under the ECtHR in 2019 J.

106. Second, the DC was also correct to proceed on the basis that the CJEU would not regard itself as being bound by the reasoning of the Strasbourg Court in *BBW GC* in relation to the application of Directive 2002/58/EC (the "e-Privacy Directive") or Articles 7 and 8 of the EU Charter (the latter of which has no equivalent in the ECHR). As the CJEU made clear in *Watson CJEU*, §§127-129 [**AU/15/557]**[29]:

"*the ECHR does not constitute, as long as the European Union has not acceded to it, a legal instrument which has been formally incorporated into EU law*"; "*the interpretation of Directive 2002/58…must be undertaken solely in the light of the fundamental rights guaranteed by the Charter*"; "*the explanation on Article 52 of the Charter indicates that paragraph 3 of that article is intended to ensure the necessary consistency between the Charter and the ECHR, 'without thereby adversely affecting the autonomy of Union law and … that of the Court of Justice of the European Union'*"; and "*Article 8 of the Charter concerns a fundamental right which is distinct from that enshrined in Article 7 of the Charter and which has no equivalent in the ECHR*".

107. Third, since the UK is no longer a member of the EU and *BBW GC* would therefore not be binding on the Court as retained EU law even if it had been delivered by the CJEU itself, the DC was entitled to take the view that C should not be able to achieve relief under retained EU law indirectly, by relying on a judgment of the ECtHR, when such relief would not be available under the scheme of the European Union (Withdrawal) Act 2018. The effect of C's argument is that an ECtHR judgment can in effect become binding, and be the subject of the direct remedies under EU law that go beyond those available under the Human Rights Act 1998, because such a judgment can be read across and applied in any claim relying on equivalent rights in the EU Charter. That is inconsistent with Parliament's intention, reflected in the Human Rights Act 1998 and the EU (Withdrawal) Act 2018, that neither ECtHR judgments, nor CJEU judgments delivered after 31 December 2020, should be automatically binding on our courts.

[29] Referring to C-601/15 PPU, *JN* [2016] 1 WLR 3027; see also *Opinion 2/13* [2015] 2 CMLR 21 at §§164 – 177 [**AU/88/4233]**.

108. Moreover, s.6(3) of the EU (Withdrawal) Act 2018 specifically provides that "[a]ny question" as to the validity/meaning/effect of any retained EU law is to be decided in accordance with (*inter alia*) "retained case law", defined in s.6(7) as including "retained EU case law", itself defined as any principles laid down by, and any decisions of, the European Court, *as they have effect in EU law immediately before IP completion day* [**AU/71/3301**]. That cannot include the reasoning in *BBW GC* (and would not do so even if that judgment had been delivered or followed by the CJEU after 31 December 2020).

109. Fourth, the DC was entitled to have regard to the fact that the Government had already undertaken to amend the Act to address the defects identified in *BBW GC*, and to wish to avoid granting relief that would pre-empt the steps the Government intended to take. That alone was sufficient reason for the DC to decline to grant the relief C was seeking under retained EU law.

D CONCLUSION

110. For the reasons set out above, the Divisional Court's judgments in 2019 J and 2022 J were correct in law, save in respect of the single issue concerning CJM addressed in 2019 J and set out at paragraph 4 above, where the Government has made it clear it will be legislating to remove any incompatibility with the ECHR.

SIR JAMES EADIE KC
GERRY FACENNA KC
JULIAN MILFORD KC
MICHAEL ARMITAGE
JOHN BETHELL

11 November 2022
Amended 29 March 2023