IN THE COURT OF APPEAL (CIVIL DIVISION) **Appeal Nos: CA-2022-001019**

ON APPEAL FROM THE HIGH COURT OF JUSTICE **CA-2022-001594**

KING'S BENCH DIVISION **CA-2022-001635**

ADMINISTRATIVE COURT

[2018] EWHC 975 (Admin) and [2022] EWHC 1630 (Admin)

B E T W E E N:

THE KING

on the application of

LIBERTY

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

APPELLANT'S COMBINED ECHR AND EU LAW APPEAL SKELETON ARGUMENT

References are as follows:

- The Divisional Court's judgment on the ECHR claim: *R (Liberty) v Secretary of State for the Home Department* [2019] EWHC 2057 (Admin), [2020] 1 WLR 243 (DC): **2019 J §*para***
- The two EU law judgments below: (i) *R (Liberty) v Secretary of State for the Home Department* [2018] EWHC 975 (Admin), [2019] QB 481 (DC): **2018 J §*para*** — judgment of 27 April 2018 on Liberty's challenge to Parts 3–4 of the IPA on EU law grounds; and (ii) *R (Liberty) v Secretary of State for the Home Department* [2022] EWHC 1630 (Admin) (DC): **2022 J §*para*** — judgment of 24 June 2022 on Liberty's challenge to the other impugned IPA provisions on EU law grounds
- Grand Chamber judgment in *Big Brother Watch v United Kingdom* (Application Nos 58170/13, 62322/14, 24960/15, 25 May 2021) (2022) 74 EHRR 17: ***BBW GC* §*para***
- Core, Supplementary and Authorities Bundles: **C/*tab*/*page***, **S/*tab*/*page*** and **Auth/*tab*/*page*** respectively (to be inserted when bundles are agreed)
- ECHR Grounds of Appeal dated 20 May 2022: **ECHR Grounds §*para***
- EU law Grounds of Appeal dated 12 August 2022: **EU Grounds §*para***

A INTRODUCTION AND OVERVIEW

1 Are the safeguards in the Investigatory Powers Act 2016 sufficient to meet Convention rights and retained EU law? The questions are important because the necessary safeguards in issue are those that protect individuals from the abuse of intrusive powers and ensure such powers are used properly. The Respondents have already conceded that the Act is in part incompatible with both the ECHR and retained EU law. Some amendments have already been made to the legislation. Others are said to be in progress. These appeals deal with a limited number of further areas where the Divisional Court ("**DC**") rejected Liberty's submissions.

2 There are two appeals: first, Liberty's appeal against the DC's orders on Liberty's challenge to the Investigatory Powers Act 2016 (the "**Act**" or "**IPA**") under the ECHR (the "**ECHR Appeal**"); secondly, its appeal against the decisions of the DC in 2018 and 2022 as to whether certain provisions of the IPA are compatible with (what is now) retained EU law (the "**EU Law Appeal**"). The appeals have been combined and Liberty directed to file this combined Skeleton Argument (with a 45-page limit).

3 The ECHR Appeal is brought with the permission of the DC on ECHR Grounds 1–5,[1] and is addressed in **Part B**. The EU Law Appeal is brought with the permission of the DC on Grounds 1–3, and is addressed in **Part C**. Liberty invites the Court to make a declaration of incompatibility under s 4 of the Human Rights Act 1998 ("**HRA**") and to declare that the IPA is incompatible with retained EU Law, as identified below. Relief is addressed in **Part D**.

4 Before reading this skeleton, the Court may find it useful to read the judgments below, in particular the 2019 J Annex summarising the statutory scheme,[2] *BBW GC* §§332–364, which is now the authoritative statement of the relevant ECHR principles, and *BBW GC* §§324–331, which contains a helpful explanation of bulk interception.

---

1 Permission on Ground 6 was refused.

2 The Annex appears at [2020] 1 WLR 243, 325–351.

B ECHR APPEAL

(1) Summary

5 Liberty submits that the DC was wrong to hold that certain provisions in the IPA are compatible with Arts 8 and 10 of the ECHR and thus to refuse Liberty's claim for a declaration of incompatibility under s 4 HRA.

6 It is now common ground that the DC's decision was wrong. *BBW GC*, which was handed down after the judgment below, establishes that the IPA is incompatible with Arts 8 and 10 in important respects. The IPA lacks safeguards the ECHR requires. Rs properly concede that the IPA is incompatible with Arts 8 and 10 in some respects. But the concessions are too narrow. Further, the DC erred in rejecting Liberty's other arguments.

7 The surveillance that the IPA enables to be authorised by warrant or other instrument takes various forms. Broadly speaking, the IPA provides for:

7.1 retention by communications service providers (e.g. mobile and fixed line telephone network operators and internet service providers) of "communications data" (broadly speaking, metadata, i.e., the who, what, where, when of communications) and access requests by public bodies (**Parts 3–4**);

7.2 the interception by the state in bulk (i.e. on a massive scale) of both "content" (i.e. the meaning / substance of a communication, eg an email, WhatsApp message or SMS) and the "secondary data" (broadly metadata, but including the wider concept of "systems data") of communications in transmission (**Part 6 Chapter 1**);

7.3 bulk and "thematic" equipment interference (**Part 6 Chapter 3** and **Part 5**), that is, obtaining electronic information from devices and systems by hacking and any other means apart from interception;

7.4 the obtaining of communications data in bulk (**Part 6 Chapter 2**); and

7.5 the storage of "bulk personal datasets" ("**BPDs**"), namely, electronic databases that may include personal data, most of which is not and is unlikely to become of any interest to the intelligence services (**Part 7**).[3]

8 As surveillance regimes necessarily operate in secret, the ECtHR jurisprudence permits an *in abstracto* challenge to legislation: *Zakharov v Russia* (2016) 63 EHRR 17 (GC) §178. The law requires that a surveillance regime provides a minimum of safeguards, which themselves ensure that secret surveillance occurs only where its interference with privacy and freedom of expression is necessary and proportionate. Such safeguards now include prior independent authorisation for many intrusive activities.

(2) Legal Framework

9 It is well established (*BBW GC* §360) that, in order to satisfy the requirement under Arts 8 and 10 that an inference is "in accordance with the law" or "prescribed by law", it is required that "*the domestic legal framework contains sufficient guarantees against abuse*" and that "*the process is subject to 'end-to-end safeguards'*". As *BBW GC* §333 explained:

> "… where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on secret surveillance measures, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (see *Roman Zakharov* … §229; …). Moreover, the law must indicate the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see *Roman Zakharov* … §230; …)." [emphasis added]

10 *BBW GC* §361 identifies (and expands) the minimum safeguards Arts 8 and 10 require:

> "in addressing jointly 'in accordance with the law' and 'necessity' as is the established approach in this area the Court will examine whether the domestic legal framework clearly defined:
> 1. the grounds on which bulk interception may be authorised;
> 2. the circumstances in which an individual's communications may be intercepted;
> 3. the procedure to be followed for granting authorisation;
> 4. the procedures to be followed for selecting, examining and using intercept material;

---

[3] Part 7 regulates the use by MI6, GCHQ and MI5 of their underlying powers to obtain and hold evidence in Intelligence Services Act 1994 ss 1–2 (MI6), 3–4 (GCHQ); Security Service Act 1989 ss 1–2 (MI5). References to Part 7 include these underlying powers.

5. the precautions to be taken when communicating the material to other parties;
6. the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;
7. the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;
8. the procedures for independent ex post facto review of such compliance and the powers vested in the competent body in addressing instances of non-compliance."

11 In addition, in situations where there is a heightened expectation of confidentiality — for journalists or watchdog organisations and their sources, and for lawyers and clients — additional safeguards are required: see ECHR Grounds 1 and 5 below.

12 Due to the similarity between the IPA and the legislation considered in *BBW GC*, namely, the UK's previous bulk interception regime in s 8 of the Regulation of Investigatory Powers Act 2000 ("**RIPA**"), the defects in the RIPA regime that *BBW GC* identified are also defects in the IPA, as Rs concede in certain instances.

13 As explained on ECHR Ground 4, substantially similar requirements for detailed and rigorous safeguards apply to state databases of personal information, such as BPDs.

(3) ECHR Ground 1: Absence of Journalistic Protections

14 2019 J §§293–352 held that, contrary to Liberty's and the National Union of Journalists' ("**NUJ**") submissions below, the IPA provides sufficient protections for journalistic and watchdog[4] materials. This finding is incorrect in light of *BBW GC*. The DC accepted that the direction of travel of the ECtHR authorities might support Liberty and the NUJ. So it has proven. Rs now concede that Part 6 Chapter 1 (the bulk interception power) is incompatible with Art 10, but the concession is too limited: the same incompatibility applies in respect of the other IPA powers, and Rs do not accept that the protections are required in all the circumstances that *BBW GC* identifies.

(a) The importance of a free press in a democratic society and the law and the principles

15 A free press is essential to a functioning democracy. Art 10 (and Art 8) require states to have rigorous safeguards constraining powers that affect journalism. Thus in *R (Miranda) v SSHD* [2016] EWCA Civ 6, [2016] 1 WLR 1505 at [100]–[115] and [119],

[4] 2019 J §351 rightly held that campaigning / watchdog organisations such as Liberty must be accorded the same protections as journalists and media organisations. References herein to "journalists" and "journalistic" accordingly encompass also such organisations.

Lord Dyson MR held that the stop-and-search power under Schedule 7 of the Terrorism Act 2000 was not "prescribed by law" under Art 10 (and thus incompatible with the ECHR) because it did not provide for independent authorisation of searches of journalistic material, whether or not the material revealed a source (at [107]).[5] He held at [113]–[114]:

> "…The central concern is that disclosure of journalistic material (whether or not it involves the identification of a journalist's source) undermines the confidentiality that is inherent in such material and which is necessary to avoid the chilling effect of disclosure and to protect article 10 rights. If journalists and their sources can have no expectation of confidentiality, they may decide against providing information on sensitive matters of public interest. That is why the confidentiality of such information is so important. …
>
> Laws LJ [in the DC below] may be right in saying that the European Court of Human Rights has not developed an 'absolute' rule of judicial scrutiny for cases involving state interference with journalistic freedom. But prior judicial or other independent and impartial oversight (or immediate post factum oversight in urgent cases) is the natural and obvious adequate safeguard against the unlawful exercise of the Schedule 7 powers in cases involving journalistic freedom. For the reasons that I have given, the other safeguards relied on by Laws LJ provide inadequate protection." [emphasis added]

16 *BBW GC* puts beyond doubt that, to be "prescribed by law" under Art 10 (and under Art 8), a secret surveillance regime must contain requirements that:

16.1 There is prior independent authorisation of a search directed to journalistic materials where search terms ("selectors") are (i) known to be connected to a journalist or news organisation or (ii) which would make the selection of confidential journalistic material ("**CJM**") likely, whether or not the intention is to identify a journalistic source;

16.2 Such a search is justified by an overriding requirement in the public interest (and no less intrusive measures would suffice to serve that interest), which the independent judge or body must itself assess and consider to be the case; and

16.3 Even if search terms were not intended or thought likely to yield CJM, where it becomes apparent that CJM has been, or likely has been, selected for examination,

---

5 "*I can see no reason in principle for drawing a distinction between disclosure of journalistic material simpliciter and disclosure of journalistic material which may identify a confidential source.*"

continued use and retention of the material must at that stage be made subject to substantively the same safeguards.

17 These requirements are at *BBW GC* §§447–450, 456–457 and 525–528, especially:

> "448. … 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 and impartial decision-making body invested with the power to determine whether they were 'justified by an overriding requirement in the public interest' and, in particular, whether a less intrusive measure might have sufficed to serve the overriding public interest (see *Sanoma Uitgevers BV* [[2011] EMLR 4]] §§90–92). …"

18 The law as stated in *BBW GC* was, in substance, Liberty and the NUJ's position below: see the arguments at 2019 J §302. The DC accepted there was force in those submissions, but concluded that "*it would not be appropriate to anticipate what the Grand Chamber may say about this in Big Brother Watch*" and thus did not accept them as representing the law: 2019 J §337. As is apparent from Rs' concessions, *BBW GC* establishes that the DC erred.

(b) Application of the legal requirements to the IPA

19 Rs concede that Part 6 Chapter 1 (bulk interception) is not compatible with Art 10 "*insofar as it does not require authorisation by a judge or other independent body, where (i) the intention of the search is to select … CJM … for examination, or the selectors/search terms used are such as to make the selection of such material highly probable; or (ii) a decision is made to retain CJM which has been inadvertently selected for examination*".[6] That is correct, but does not go far enough.

20 First, as to Part 6 Chapter 1, Rs take several bad points about the circumstances in which the protections apply:

20.1 Rs wrongly do not accept that the safeguards must apply where search terms are used that are "*known to be connected to a journalist*" (*BBW GC* §448).[7]

---

6 Defendants' Submissions Resisting PTA filed 1 December 2021 ("**D PTA Subs**") §6(a) (emphasis added) [***]; see generally §§4–6(a).

7 D PTA Subs §4(a) [***].

20.2 Rs assert that the safeguards do not apply where it is likely (rather than "*highly probable*") that CJM will be selected for examination.[8] This cannot be reconciled with *BBW GC* §§525–528; indeed the UK did not even contest the Chamber's findings before the Grand Chamber (*BBW GC* §527).

20.3 Rs suggest that there is no requirement for an overriding requirement in the public interest (assessed by the independent authoriser), on the basis that "*[t]he ECHR Judgment did not separately consider*" this.[9] That is untenable on the passages from *BBW GC* set out above.[10] It is also illogical where (i) Rs accept that there must be independent authorisation and (ii) the Grand Chamber expressly requires that the independent authoriser verifies whether the search/retention is justified by an overriding requirement in the public interest. The requirements are inextricably linked.

21 Secondly, various definitions in relation to CJM cut back the protections afforded, incompatibly with Art 10 (and Art 8):

21.1 The DC wrongly held (2019 J §§340–347) that the IPA definitions of "*journalistic material*", which is limited to material created or acquired for the purposes of journalism (s 264(2)), and "*confidential journalistic material*", which requires an express or implied undertaking to hold material in confidence (s 264(6)–(7)), both of which form part of the triggers for certain journalistic safeguards in the IPA, are wide enough to provide the protection required. For example, material not acquired initially for journalism but which becomes relevant to a journalist's work would not be "*journalistic material*" and is not protected.[11] Information not held pursuant to an undertaking of confidence, such as public information a journalist gathers (which might tend to reveal their investigations and intended reporting) or, arguably, information a source intends to be disclosed is not "*confidential*

---

8 D PTA Subs §4(a) [***].

9 D PTA Subs §4(b) [***].

10 And also *BBW GC* §449.

11 Cobain 1 §§39, 47(1) [***], which explains that this is commonplace in investigative journalism. Mr Cobain is a well-known investigative journalist. His evidence was referred to at 2019 J §295.

journalistic material".[12] But this material is protected under *BBW GC* as set out above. And a journalist's willingness to investigate and publish will be chilled by secret surveillance of such material, just as it will be chilled by surveillance directed to material from sources.[13]

21.2 The DC further erred in holding (2019 J §352) that the exclusion of material that was "*created … with the intention of furthering a criminal purpose*" from journalistic protections in the IPA is compatible with Art 10 (and Art 8). This exception would apply, for example, to a document disclosing misconduct by a senior government official that was copied and provided to a journalist, assuming the copying and disclosure to be unlawful.[14] But this would be protected by the principles explained in *BBW GC*.

22 Thirdly, Rs contest the application of these protections to powers other than the bulk interception power, but this is unreasoned and unprincipled.

23 Rs assert that it does not follow from *BBW GC*, which considered bulk interception under RIPA, that equivalent requirements or coextensive defects apply to other IPA secret surveillance powers.[15] They suggest that it is "*plainly inappropriate*" to apply the findings in *BBW GC* to other powers, including bulk acquisition of communications data and bulk equipment interference.[16] This is wrong:

23.1 The requirements in *BBW GC* apply "*in the context of secret surveillance*" and "*secret measures of surveillance, <u>such as</u> the interception of communications*": *BBW GC* §333 (emphasis added). The impugned IPA regimes other than bulk interception are just as much secret surveillance regimes.

---

12 See, in this regard, Cobain 1 §§47(3) [***]. An example would be a draft news piece based on work combining various different sources of publicly available information with freedom of information responses and/or official refusals to comment (or other official responses), which enable an inference of government malpractice or wrongdoing.

13 See Cobain 1 §§32, 39 [***].

14 Mr Cobain gives the example of a disclosure that would be prohibited under s 1 of the Official Secrets Act 1989: see Cobain 1 §§48–54 [***].

15 D PTA Subs §6(b) [***].

16 D PTA Subs §3 [***].

23.2 *BBW GC* §363 held that acquisition of communications data is not necessarily less intrusive than acquisition of content and that "*the interception, retention and searching of related communications data should be analysed by reference to the same safeguards as those applicable to content*" in the context of the RIPA regime (which permitted acquisition of communications data as well as bulk interception, like the IPA). Moreover, the Court applied identical requirements under Art 10 to the RIPA communications data acquisition regime at *BBW GC* §§525–528. Accordingly, it is apparent from *BBW GC* that the same safeguards apply in relation to communications data regimes (Parts 3–4 and Part 6 Chapter 2) as to bulk interception.

23.3 This point has been decided against Rs in *Ekimdzhiev v Bulgaria* (App No 70078/12, 11 January 2022, Fourth Section) §395 ("***Ekimdzhiev 2***"), which applied *BBW GC* to hold that "*the general retention of communications data by communications service providers and its access by the authorities in individual cases must be accompanied, mutatis mutandis, by the same safeguards as secret surveillance*" (emphasis added).

23.4 Further, Rs identify no principled or logical reason why the safeguards for different kinds of secret surveillance should be different. It does not matter from the point of view of the rights to freedom of expression, private life and correspondence protected by Arts 10 and 8 whether the interference with privacy occurs by (for example) retaining and searching all email communications (by bulk surveillance) or by hacking or creating a back door (by bulk or thematic equipment interference). The different technical means do not reduce the degree of interference with privacy, nor the need for rigorous safeguards that ensure that interferences are necessary and proportionate.

23.5 Indeed, it was expressly conceded below that, for regimes that enable content to be obtained (Part 6 Chapter 3 and Part 5), the same foreseeability requirements apply as for bulk interception.[17] That concession was and is right (albeit too limited).

---

[17] See D Trial Skel §32(1) [***] (emphasis added): "*It is common ground that, when considering whether domestic law providing for the interception of communications is sufficiently foreseeable, compliance with the six minimum safeguards known as the*

24 Accordingly, the provisions of the IPA are incompatible with Arts 8 and 10 ECHR. The specific defects in each power are summarised in the **Annex**.

(4) ECHR Ground 2: Absence of Safeguards in the Bulk Regimes and Part 5

25 *BBW GC* strengthened the safeguards that any system of secret surveillance or data retention must contain: see generally *BBW GC* §§347–362. Part 5, Part 6 Chapters 1–3 and Part 7 do not satisfy several of these requirements, as is now partly conceded. The three defects are identified below.

(a) No independent authorisation of categories of search terms at warrant issue

26 It is now established that there must be independent authorisation of the categories of "selectors" (search terms) at the point of initial authorisation of secret surveillance: *BBW GC* §§353–355, 381–383, 416, 425. At §354, the Court said:

> "Taking into account the characteristics of bulk interception (see paragraphs 344-345 above), the large number of selectors employed and the inherent need for flexibility in the choice of selectors, which in practice may be expressed as technical combinations of numbers or letters, the Court would accept that the inclusion of all selectors in the authorisation may not be feasible in practice. Nevertheless, given that the choice of selectors and query terms determines which communications will be eligible for examination by an analyst, the authorisation should at the very least identify the types or categories of selectors to be used." [emphasis added]

27 At §425, the Court concluded that a "*fundamental deficiency*" in the RIPA regime was "*the failure to include the categories of selectors in the application for a warrant*". There is, however, no requirement for independent authorisation of categories of selectors in any of the provisions mentioned above (including the provisions for targeted examination warrants) or the accompanying Codes,[18] which are accordingly incompatible with Art 8.

'Weber' criteria … must be considered. Ds accept that the same minimum safeguards apply mutatis mutandis to the obtaining of the content of communications via surveillance methods analogous to interception (e.g. via equipment interference): see DGR, §§30–31". No application for permission to withdraw this has been made.

[18] Compare ss 102 and 115 (Part 5), 142 (Part 6 Chapter 1), 161 (Part 6 Chapter 2), 183 (Part 6 Chapter 3), 212 (Part 7), as well as Equipment Interference Code of Practice §§5.34–5.35 (thematic / targeted examination) and 6.10–6.13 (bulk), Interception Code of Practice §§5.29–5.30 (targeted examination) and 6.17–6.20 (bulk), Bulk Acquisition

28 Rs do not appear to contest that *BBW GC* establishes such a requirement. They instead suggest that the statutory provision that selection for examination occurs for "operational purposes" is sufficient.[19] That is wrong:

28.1 Under Part 5, there is no requirement for operational purposes. Thematic equipment interference warrants permit the obtaining of vast amounts of information, given their scope, yet there is no statutory mechanism to ensure that searches of this material are constrained (even by operational purposes).

28.2 As to Part 6 Chapters 1–3 and Part 7, an "*operational purpose*" is not a category of selectors, as contemplated by *BBW GC* §§353–355, 381–383, 416, 425. They are purposes for which selection for examination is thought potentially necessary when the warrant is issued and for which it must occur (see, eg, in Part 6 Chapter 1 ss 138(1)(d), 142(3)–(11), 144(2)I(1), 150(1)(b), 152(1)–(2)).[20] The only statutory requirement is that they are more specific than "*national security*", "*preventing and detecting serious crime*" or "*the economic well-being of the United Kingdom so far as … relevant to … national security*" (see, eg, in Part 6 Chapter 1 s 142(7)).[21] For example, a lawful operational purpose might be "international counter-terrorism". However, that would not be a category of selectors or search terms as explained in *BBW GC*. It does not involve identifying individual selectors (such as a name or telephone number) or categories of them (such as people who use a particular discussion forum).

29 Rs contend again that this requirement does not apply other than in relation to bulk interception, but this is wrong for the reasons in paragraph 23 above.

Code of Practice §§4.1–4.5, Bulk Personal Datasets Code of Practice §§4.10, 4.19–4.10 (and generally section 4).

19 D PTA Subs §13(b) [***].

20 Corresponding provisions are ss 158(1)(c), 159(1)(c), 161(3)–(11) (Part 6 Chapter 2), 178(1)(d), 179(1)(c), 183(4)–(12) (Part 6 Chapter 3), 204(3)(c), 205(6)(c), 212(3)–(12) (Part 7).

21 Corresponding provisions are ss 161(7) (Part 6 Chapter 2), 183(8) (Part 6 Chapter 3) and 212(8) (Part 7).

(b) No requirement for separate and objective internal authorisation of strong selectors

30 There must be a requirement for separate and objective internal authorisation and verification of the proportionality of the use of "strong selectors" (e.g. a specific email address, telephone number) linked to identifiable individuals before they are applied, and a record of the justification for their use: *BBW GC* §§353–355, 382–383, 416, 425. At §355 the Grand Chamber said:

> "Moreover, enhanced safeguards should be in place when strong selectors linked to identifiable individuals are employed by the intelligence services. The use of every such selector must be justified — with regard to the principles of necessity and proportionality — by the intelligence services and that justification should be scrupulously recorded and be subject to a process of prior internal authorisation providing for separate and objective verification of whether the justification conforms to the aforementioned principles." [emphasis added]

31 At §§381–383, the Grand Chamber referred to this requirement as of "*fundamental importance*", and held that RIPA did not satisfy it, notwithstanding the existence of after-the-fact supervision of selectors by the (then) Interception of Communications Commissioner. At §425 it identified as a defect "*the failure to subject selectors linked to an individual to prior internal authorisation*".

32 There is no such requirement in any of the provisions mentioned or accompanying Codes,[22] which are accordingly incompatible with Art 8.

33 Rs rightly concede that Part 6 Chapter 1 is incompatible with Art 8 on this basis.[23] But

---

[22] Compare, for example, Interception Code of Practice §§6.72–6.76, BCD Code of Practice §§6.12–6.17; Equipment Interference Code of Practice §§6.6–6.9, BPD Code of Practice §§7.6–7.9, which refer to the procedure by which selectors are applied and a record of the justification is kept. No specific provision is made for the application of strong selectors linked to identifiable individuals.

[23] D PTA Subs §§12, 14(a) [***].

Rs incorrectly contend that it is sufficient to remedy this with an internal policy. In order to give the arrangement sufficient character of effectiveness, permanence and indeed law, the IPA and/or the relevant Codes of Practice must be amended. A non-public internal policy that can be amended without publication or formality does not have the quality of law under Art 8 and is thus insufficient: *Zakharov v Russia* (App No 47143/06, 4

they do not accept this for Part 5, Part 6 Chapter 2, Part 6 Chapter 3 or Part 7, repeating that there is "*no principled basis for transposing this requirement that the Grand Chamber identified in relation to bulk interception onto parts of the IPA that deal with other investigatory powers*".[24] That is wrong: see paragraph 23 above.

(c) No objective and reasonable basis for differential treatment of content and secondary data / communications data / non-protected material

34 *BBW GC* §§416–423 establishes that, insofar as lesser safeguards apply to metadata than those that apply to content, because metadata is no less intrusive than content (§363), there must be an objective and reasonable justification for the different treatment.

35 The IPA has made substantial changes to the treatment of metadata compared to RIPA. More may be collected and what is collected is far more intrusive. Treating a wider set of metadata as not subject to the safeguards that apply to content cannot be justified.

36 As set out in ECHR Grounds §7:

36.1 "Content" and "secondary data" in Part 6 Chapter 1, and "protected information" and non-"protected information" in Part 6 Chapter 3, are treated differently in that that the British Islands safeguard does not apply to the latter in both cases. The British Islands safeguard is a requirement for separate independent authorisation prior to examining the content of a communication of a person in the British Islands, obtained under bulk powers. This safeguard gives effect to the principle that there is no practical difference between a targeted warrant against an individual here and extracting the same content from bulk data already collected.

36.2 The new definition of "secondary data" and non-"protected material" include anything that is "systems data" or "equipment data" (ss 137(3)) and 193(9)), even if it discloses meaning. For example, Rs accepted below that inter alia: (i) a Google search;[25] (ii) a full web address (which will usually reveal all of the content being viewed); and (iii) the time, date and location of a photograph would each be

---

December 2015, Grand Chamber) §240, §242; *Leander v Sweden* (App No 9248/81, 26 March 1987, Chamber) §54.d

24 D PTA Subs §14(b) [***].

25 Note from the Secretaries of State on "Systems Data" and "Identifying Data" (handed up) §5 [***].

"secondary data"/non-"protected material",[26] so not subject to the British Islands safeguard. But an email containing that same information would be "content".

36.3 There is no objective and reasonable justification for the absence of any requirement for the British Islands safeguard to apply when a BPD is examined in Part 7, in circumstances where BPDs may (and indeed do in fact: 2019 J §230)[27] contain "content". The British Islands safeguard does apply where exactly the same data is held and searched under Part 6 Chapter 1 or Part 6 Chapter 3.

37 The Court (2019 J §§171–178) erred in failing to address the gravamen of Liberty's complaint about the expansion of "secondary data" and non-"protected material". The Court (2019 J §§228–234) also erred in failing to address the substance of Liberty's complaint in relation to Part 7, namely, that there was arbitrary uneven protection of the same information under Part 7, as compared with Part 6 Chapter 1 and Chapter 3 (where the very same information — not just type of information — obtained under Part 6 Chapters 1 or Chapter 3 may subsequently retained under Part 7 under s 225).

38 Rs' responses to this argument[28] are incorrect or absent:

38.1 Insofar as Rs contend that the requirement for objective justification of differential treatment does not apply other than for bulk interception regimes, this is untenable: see paragraph 23 above.

38.2 Rs' suggestion that examining "secondary data" or non-"protected material" under Part 6 Chapter 1 and Part 6 Chapter 3 is less intrusive than examining "content" is incorrect: as recognised in *BBW GC* at §363, communications data can be just as intrusive as content data. Further, Part 6 Chapter 1 has replaced the concept of "*related communications data*" ("**RCD**") that existed under RIPA with a much wider concept of "*secondary data*", such that much "secondary data" discloses even more meaning: see the examples in paragraph 36.2 above. The same is true

---

26 Defendants' Response to Claimants' Examples of "Content" under RIPA Now Treated as "Secondary Data" or Non-"Protected Material" (filed following hearing) §§ 4–5 [***].

27 2019 J §230 correctly accepts that a BPD retained under Part 7 may include content and that, as at the date of Lord Anderson QC's *A Question of Trust* (2015), some in fact did so. Rs have at no point suggested that the position has changed.

28 D PTA Subs §15 [***].

of non-"protected data" under Part 6 Chapter 3. Rs rightly accepted below that "*secondary data is designedly broader than RCD, and includes material that can (in particular cases) be relatively sensitive*".[29]

38.3 There has been no defence of the absence of safeguards for "content" in Part 7.

(5) ECHR Ground 3: Absence of Safeguards when Sharing Material with Overseas Authorities

39 *BBW GC* §362 extends the mandatory requirements under Art 8 as to "*the precautions to be taken when communicating the material to other parties*" (§361(5)), holding:

> "… the transmission by a Contracting State to foreign States or international organisations of material obtained by bulk interception should be limited to such material as has been collected and stored in a Convention compliant manner and should be subject to certain additional specific safeguards pertaining to the transfer itself. 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. In particular, the receiving State must guarantee the secure storage of the material and restrict its onward disclosure. This does not necessarily mean that the receiving State must have comparable protection to that of the transferring State; nor does it necessarily require that an assurance is given prior to every transfer. Thirdly, heightened safeguards will be necessary when it is clear that material requiring special confidentiality — such as confidential journalistic material — is being transferred. Finally, the Court considers that the transfer of material to foreign intelligence partners should also be subject to independent control." [emphasis added]

40 Thus, as set out in ECHR Grounds §8, Art 8 requires that a secret surveillance regime under which data may be transferred to a third state in turn:

40.1 requires that the material shared is collected and stored in a Convention-compliant manner;

40.2 sets out clearly the circumstances in which a transfer may occur;

40.3 requires the transferring state to ensure that the receiving state has safeguards preventing abuse and disproportionate interference, in particular to guarantee secure storage and restrict onward disclosure;

---

[29] Note from the Secretaries of State on "Systems Data" and "Identifying Data" (handed up) §12 [***].

40.4 requires heightened safeguards where "*material requiring special confidentiality*", such as CJM (and, Liberty submits, privileged material), is transferred; and

40.5 makes transfer to foreign intelligence partners subject to independent control.

41 Part 5, Part 6 Chapters 1–3 and Part 7 do not contain any of these mandatory requirements:

41.1 Part 7, even when read with the underlying powers of MI5, MI6 and GCHQ, makes no provision at all in relation to supplying BPDs to overseas authorities.

41.2 Each of Part 5, Part 6 Chapter 1, Part 6 Chapter 2 and Part 6 Chapter 3[30] requires there to be arrangements where material is given to "*overseas authorities*". But all permit the Secretary of State, as a matter of discretion, to reduce to nil the protections that must be accorded to such material:

(a) The provisions in Part 6 Chapter 1 and Part 6 Chapter 3 permit the Secretary of State to provide such material to an overseas authority where "*it appears to the Secretary of State — (a) that requirements corresponding to the requirements of section 150(2) and (5) [to minimise disclosure of material obtained and destroy copies when they are no longer necessary] and section 152 [the examination safeguards] will apply, to such extent (if any) as the Secretary of State considers appropriate, in relation to any of the material which is handed over, or any copy of which is given, to the authorities in question*": ss 151(2)(a) (emphasis added) and 192(2)(a).

(b) The provisions in Part 5 (s 130) and Part 6 Chapter 2 (s 171(8)–(9)) are to similar effect, but do not mention examination safeguards.[31]

42 Each of those provisions is accordingly incompatible with Art 8.

---

30 Respectively in ss 129(2), (5), (9)–(10), 130 (Part 5), ss 150(2), (5), (7)–(8), 151–152 (Part 6 Chapter 1), ss 171(2), (5), (7)–(10) and 172 (Part 6 Chapter 2), and ss 191(2), (5), (7)–(8), 192–193 (Part 6 Chapter 3).

31 That is explicable in relation to Part 5 because examination is authorised when a Part 5 warrant is issued. It appears to be arbitrary, however, that s 171(8)–(9) in Part 6 Chapter 2 does not even refer to the s 172 examination safeguards.

43 Rs' arguments to the contrary are incorrect:

43.1 Rs argue that, because *BBW GC* §§395–398 accepted that the RIPA code provisions were adequate in relation to sharing, the same result must follow under the IPA.[32] That is wrong:

(a) As mentioned, Part 7 makes no provision at all for overseas sharing, and so is plainly incompatible with Art 8 in this respect.

(b) Otherwise, most of the code of practice provisions on which the Grand Chamber relied in upholding the RIPA intelligence sharing regime (in *BBW GC* §§396–398), which are set out in §96,[33] have now been removed from the Codes of Practice under the IPA. In particular, none of the IPA Codes of Practice currently includes requirements equivalent to those that previously existed to: (i) take reasonable steps to ensure that a third country or territory has and will maintain the necessary procedures to safeguard intercept material and to ensure it is disclosed, copied, distributed and retained only to the minimum extent necessary; (ii) explicitly agree with the issuing agency that intercept material will be further disclosed to a third country or territory;[34] or (iii) require return of the material to the issuing agency or secure destruction when it is no longer needed. The new Codes for Part 5 and

---

32 D PTA Subs §§16(b), 16(c)(ii) [***].

33 In particular, those that existed under RIPA Interception of Communications Code of Conduct §7.5, set out on p 33 of *BBW GC*.

34 Rs have asserted (D PTA Subs §16(d) [***]) that a requirement for a third state explicitly to agree with the issuing agency before intercept material is further disclosed to a third country or territory exists in Interception Code of Practice §§9.15, 9.19 and 9.26, contending in particular that §9.26 "*states in terms that §§9.15–9.19 of the Code apply to disclosure of material overseas*". This is incorrect. §9.26 requires only that consideration be given to the requirements in §§9.15–9.19 and, in any event, §§9.27–9.29 make clear that there is no requirement that there must be explicit agreement as Rs contend and as previously existed in the RIPA code. In particular, §9.29 states that disclosure may be permitted to "*a country overseas with whom we do not have an existing intelligence sharing relationship and whose authorities do not apply safeguards to intercepted material corresponding to those in the Act*".

Part 6 Chapters 1–3 by contrast emphasise that whether a third country/territory must apply safeguards is wholly discretionary.[35]

(6) ECHR Ground 4: Impermissibly Broad Bulk Personal Datasets Regime (Part 7)

44 Ground 4 is that the scope of application of Part 7 (read with the underlying powers of MI5, MI6 and GCHQ to obtain information)[36] is so wide, and its provisions as to retention, use and destruction so discretionary, that it fails to provide the citizen with any indication of what data the state may retain and how it might be used, and therefore does not satisfy the requirement for foreseeability for state databases.

45 As to the law, that requirement is essentially the same heightened foreseeability requirement as for secret surveillance regimes. The Grand Chamber explained it in *S and Marper v United Kingdom* (2009) 48 EHRR 50 §99 as follows:[37]

> "… it is as essential, in this context, as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness." [emphasis added]

46 The same requirements for state databases are well established and set out, for example, in: *MM v United Kingdom* (App No 24029/07, 13 November 2012) §§193–195, where the Court concluded at §§196–207 that the criminal records regime was not "*in accordance with the law*"; *Catt v United Kingdom* (App No 43514/15, 24 January 2019)

---

35 Compare the current Interception Code of Practice §§9.26–9.29; Bulk Acquisition Code of Practice §§9.10–9.12; Equipment Interference Code of Practice §§9.33–9.35 (relating to both Part 5 and Part 6 Chapter 3).

36 See footnote 3 for the relevant provisions, which were held in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* [2016] UKIPTrib_15_110-CH [84] (October 2016) not (without more) to meet the foreseeability requirements in relation to BPDs.

37 The Court there cited a number of secret surveillance cases, namely: *Kruslin v France* (1990) 12 EHRR 547 §§33, 35; *Rotaru v Romania* (App No 28341/95, 4 May 2000) §§57–59; *Weber v Germany* (2008) 46 EHRR SE5; *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* (App No 62540/00, 28 June 2007) §§75–77; *Liberty v United Kingdom* (2009) 48 EHRR 1 §§62–63.

§§94–95, where the analysis at §§96–105 is instructive (and the Chamber doubted but did not finally decide whether the quality of law requirements were satisfied); and *PN v Germany* (App No 74440/17, 11 June 2020) §§62–64, where the requirements were met.

47 The scope of application of Part 7 is too wide to satisfy these Convention requirements. The data that may be captured and held in a Part 7 database is essentially unlimited:

47.1 The only statutory requirements as to what a BPD is are that the data includes "personal data", relates to a number of individuals, the majority of those individuals are not (and are unlikely to become) of interest to the intelligence service, and the set is retained and held electronically (s 199(1)). This could cover any and all large-scale databases of personal information on the general public.

47.2 A Part 7 BPD may include content (and BPDs in fact do so).[38]

47.3 Section 206 makes explicit that a BPD may include health records. Sections 222–223 make clear that a BPD may include items subject to legal privilege.

47.4 Section 225, which permits information obtained under the other powers in the IPA (other than Part 6 Chapter 2) to be made into a BPD (and the existing safeguards modified or disapplied), indicates that any such information (and indeed highly intrusive information obtained, for example, via hacking) may form a BPD.

48 At the same time, Part 7 lacks many of the safeguards of the Part 6 powers, in particular (i) mandatory requirements for deletion of BPDs and information extracted from them,[39] (ii) mandatory requirements to minimise the disclosure and copying of information, (iii) certain safeguards in relation to examination, such as the British Islands safeguard (compare s 207), and (iv) safeguards as to sharing of BPDs with third countries, as noted at paragraph 41.1 above. Given its broad scope and lack of safeguards, Part 7 can fairly be said to be analogous to the interception regime held to be impermissibly wide in scope and ill-defined in *Liberty v United Kingdom* (2009) 48 EHRR 1 (compare especially at §§16–27 and 64–69). Liberty is not aware of any Strasbourg case that has upheld such a broad state database regime, whereas the cases set out in paragraphs 45-46 show that

---

38 See footnote 27 above.

39 Part 7 contains no requirement equivalent to s 150 in Pt 6 Ch 1. Compare ss 204(3)(d), 205(6)(d) and 221.

narrower regimes have been held to be too broad.

49 2019 J §§223–224 err in that they do not address this fundamental point. The DC failed to make any finding as to whether and, if so, why the scope of the provisions is sufficiently defined and the safeguards adequate.

50 Instead, 2019 J §§223–224 focus on an example Liberty gave[40] to illustrate the breadth of the provisions, namely, that the provisions could be used to authorise the retention of fingerprint and DNA databases held to be unlawful in *S and Marper* and *MK v France* (App No 19522/09, 18 April 2013). The DC said that, because a Judicial Commissioner (and the Secretary of State) must consider necessity and proportionality, the system "*is designed to ensure that retention of the kind which was found to be in breach of the ECHR in S and Marper or in MK would not be authorised and would therefore be prohibited by section 200*" and that it was "*wrong as a matter of principle to argue that Part 7 is incompatible with articles 8 and 10 by advancing factual scenarios which would be incompatible with legal principles (and independent mechanisms to give effect to those principles) enshrined in the Act itself*": 2019 J §224.

51 This does not answer Liberty's complaint. *S and Marper* and the other database cases require that powers to authorise retention of databases of private information be sufficiently well defined in law to (*inter alia*) enable citizens to foresee in what circumstances their personal data will be retained. If it were otherwise, simply inserting a requirement for necessity and proportionality of decision making would be sufficient to render any regime in accordance with the law.

52 Rs suggest that it is somehow an answer that BPDs are defined in Part 7.[41] This is wrong. Part 7 of course defines BPDs. The complaint is that, in doing so, it permits too broad a range of information to be held with inadequate safeguards.

(7) ECHR Ground 5: Absence of Adequate Safeguards for Lawyer–Client Communications

53 *BBW GC* did not directly address lawyer–client communications. Read with other Strasbourg authority, however, the protection required for lawyer–client communications

---

40 Claimant's ECHR Skeleton §108 [***].

41 D PTA Subs §19 [***].

is at least equivalent to that which applies to journalistic materials:

53.1 The rationale for protecting the confidentiality of lawyer–client communications is very similar to that for protecting journalistic materials. As *Michaud v France* (App No 12323/11, 6 December 2012) §118 ("***Michaud***") explains:

> "… Article 8… affords strengthened protection to exchanges between lawyers and their clients. This is justified by the fact that lawyers are assigned a fundamental role in a democratic society, that of defending litigants. Yet lawyers cannot carry out this essential task if they are unable to guarantee to those they are defending that their exchanges will remain confidential. It is the relationship of trust between them, essential to the accomplishment of that mission, that is at stake." [emphasis added]

That corresponds with the rationale for the protection of journalistic materials, namely, the important role journalists play in publishing information that is of benefit to society generally and the necessity for journalists and sources to have confidence that communications/materials obtained remain secret: see paragraphs 15 and 21 above.

53.2 The requirement in *Michaud* §118, accepted in 2019 J §290, that lawyer–client communications must be accorded "*strengthened protection*" is in practice meaningless unless domestic law requires that there be (at least) an overriding requirement in the public interest that justifies the targeting/risk of capture, and examination, of lawyer–client communications, assessed independently. That is supported by, for example, *Wolland v Norway* (App No 39731/12, 17 May 2018) §66 (emphasis added) which held that "*lawyer-client confidentiality may only be derogated from in exceptional cases and on condition that adequate and sufficient safeguards against abuse are in place*".

53.3 In *Kopp v Switzerland* (App No 13/1997/797/1000, 25 March 1998) §74, where the Court considered the lawfulness of telephone tapping of a lawyer's offices, it held that: "*Above all, in practice, it is, to say the least, astonishing that this task [determining which communications were privileged] should be assigned to an official of the Post Office's legal department, who is a member of the executive, without supervision by an independent judge, especially in this sensitive area of the confidential relations between a lawyer and his clients…*"

53.4 In the context of secret surveillance regimes, *Szabó and Vissy v Hungary* (2016) 63 EHRR 3 §77 held that *ex ante* authorisation was required in circumstances such as *Kopp v Switzerland* (telephone tapping of a lawyer's offices) and suggested that the principles are the same as those protecting journalists:

> "… Indeed, in certain respects and for certain circumstances, the Court has found already that ex ante (quasi-)judicial authorisation is necessary, for example in regard to secret surveillance measures targeting the media. In that connection the Court held that a post factum review cannot restore the confidentiality of journalistic sources once it is destroyed (see *Telegraaf Media Nederland Landelijke Media BV and Others v the Netherlands*, no. 39315/06, § 101, 22 November 2012; for other circumstances necessitating ex ante authorisation see *Kopp v Switzerland*, 25 March 1998, Reports 1998 II). …" [emphasis added]

2019 J §287 refers to *Szabó*, but asserts, without explanation or specific reference to §77 (on which Liberty relied below), that it supports the view that Strasbourg jurisprudence does not lay down a requirement for prior authorisation in relation to lawyer–client communications. That is incorrect.

53.5 ECtHR decisions in the context of searches of lawyers' offices suggest that the safeguards in practice required to ensure that any interference is necessary and proportionate include independent authorisation and independent supervision of the search (in particular, to protect professional secrecy), which are analogous to the safeguard of independent authorisation now (clearly) established for journalistic materials in a bulk surveillance regime (*BBW GC* §444). For example:

(a) In *Sallinen v Finland* (App No 50882/99, 27 September 2005), where a number of deficiencies meant the law authorising searches of lawyers' offices was not "in accordance with the law", the Court was "*struck by the fact that there was no independent or judicial supervision*": §89. Similarly, in *Heino v Finland* (App No 56720/09, 15 February 2011), the Court held that the law authorising the search of a lawyer's offices was not "in accordance with the law" (§47) because it did not provide either for "*independent or judicial supervision when granting the search warrant*" or for the lawyer to be able to require "*an ex post factum judicial review … to have both the lawfulness of, and justification for, the search warrant reviewed*" (§§44–45).

(b) In *Lindstrand Partners Advokatbyrå AB v Sweden* (App No 18700/09, 20 December 2016) §95, and in *Wieser and Bicos Beteiligungen GmbH* (App No 74336/01, 16 October 2007) §57, the Court noted (in the context of examining the necessity of searches) that it examines "*whether domestic law and practice afforded adequate and effective safeguards against any abuse and arbitrariness*" and that:

> "Elements taken into consideration are, in particular, whether the search was based on a warrant issued by a judge and based on reasonable suspicion, whether the scope of the warrant was reasonably limited and — where the search of a lawyer's office was concerned — whether the search was carried out in the presence of an independent observer in order to ensure that materials subject to professional secrecy were not removed …"

(c) In *Wolland v Norway* (App No 39731/12, 17 May 2018) the Court relied on domestic requirements for "*prior judicial authorisation [of the search], which included an examination of whether reasonable suspicion existed*" (§67), a requirement to place materials obtained under seal if their seizure was contested (§68), and rights to challenge search and seizures (§§68–70).

54 Accordingly, Liberty submits that requirements equivalent to those identified in *BBW GC* for journalistic material (set out in paragraph 16 above) apply also to lawyer–client communications.

55 Parts 3–4, Part 5, Part 6 Chapters 1–3 and Part 7 do not have these safeguards (or do not require them in all circumstances where the protection is required) and each is to that extent incompatible with Art 8:

55.1 None of the IPA privilege provisions provides for prior, independent authorisation for the selection for examination/retention of legally privileged material (save, by default, where a targeted examination warrant is required) — in particular, there is no such requirement where (a) the communications of someone known to be a lawyer are accessed, (b) it is likely that that lawyer–client communications will be accessed or (c) it becomes apparent that such material is being, or is likely to be, retained.

55.2 While some IPA provisions do require an overriding requirement in the public interest (or even a more onerous requirement) before such material is accessed,[42] they do not require this in all the circumstances identified in paragraph 55.1 above. Nor do they require that the assessment of whether there is such an overriding requirement is carried out by an independent body.

55.3 Moreover, Part 6 Chapter 2 contains no provision at all for lawyer–client communications. It is notable that material obtained under Part 6 Chapter 1 receives better protection than privileged bulk communications data (Part 6 Chapter 2), even though the latter data may be equally intrusive and equally privileged. There is no objective and reasonable justification for this difference.

C EU LAW APPEAL

(1) Summary

56 In 2018, the DC held that Parts 3–4 of the IPA were incompatible with EU law in two respects: in the area of criminal justice, the IPA did not require prior independent authorisation by a court or administrative body of access to retained data (see 2018 J §186 and 2022 J §62) and access to retained data was not limited to the purpose of combatting serious crime (2018 J §186). In 2022, the DC held that amendments to the IPA had not cured these incompatibilities, because MI5, MI6 and GCHQ had been exempted from the requirement for prior independent authorisation: 2022 J §§56–72 and 121–132. The DC rejected various other arguments advanced by Liberty in 2018 and 2022.

57 On the appeal on retained EU law grounds, Liberty has three short points:

57.1 **EU Ground 1:** The provisions of the IPA that Liberty challenges, namely, Part 5, Part 6 Chapters 1 to 3 and Part 7 (the "**bulk powers**"), and in addition Parts 3 and 4, are provisions for "*general and indiscriminate*" retention of and access to data within the meaning of retained EU law. This is because they permit very wide retention of and access to data. (Part 7 is within the scope of EU law insofar as it is

[42] Sections 27(1)(b)(ii) (targeted examination for bulk interception), 112(1)(a), (b)(ii) (Part 5 and targeted examination for bulk equipment interference), 153(1) (Part 6 Chapter 1), 194(1) (Part 6 Chapter 3), 222(1)(a), (2) (Part 7).

used to retain information obtained under other provisions of the IPA.) Being "*general and indiscriminate"* is not a pejorative term. It simply means that, applying retained EU law, those provisions must have certain safeguards, which they currently lack. The DC's essential error was to misinterpret this principle of retained EU law and treat provisions requiring matters to be considered as actually constraining the scope of the powers to retain and access.

57.2 **EU Ground 2:** Irrespective of whether the provisions are general and indiscriminate, it is now well established by domestic and (pre-IP completion day)[43] EU decisions that, where retained data is accessed for a purpose other than national security, there must be prior independent authorisation of that access (except in cases of urgency). The DC accepted this in 2018, and declared that Part 4 was incompatible with EU law because it did not so provide. It further rightly held in 2022 that amendments to remedy this were inadequate, because MI5, MI6 and GCHQ could still self-authorise access for combatting serious crime. But in 2022 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**"). Retained EU law distinguishes between the requirements for authorisation of retention and authorisation of access (i.e. accessing that which has been retained in a generalised manner), and requires authorisation of the particular access request. On the DC's approach, this requirement is meaningless as a safeguard.

57.3 **EU Ground 3:** It was, prior to the DC's 2022 decision, well established that rights under the EU Charter of Fundamental Rights ("**Charter**") and the general principles of EU law provide at least the same level of protection as the ECHR. ECtHR decisions before and after IP completion day establish that Arts 8 and 10 ECHR require bulk secret surveillance regimes, such as the bulk powers, to have certain safeguards, which the bulk powers lack (and, in light of *BBW GC*, are to some extent conceded to lack). The DC erred in 2022 in not holding that the IPA breaches the requirements of Arts 7 and 11 of the Charter and/or equivalent general principles of retained EU law for the same reason. Indeed, the DC failed to consider

---

[43] Under the European Union (Withdrawal) Act 2018 ("**EUWA**") as amended, the implementation period ("**IP**") completion day was 31 December 2020.

at all whether retained EU law provides at least equivalent protection to the ECHR. It does, and the Court should so have held. Instead, the DC considered the question of whether the Court of Justice of the European Union ("**CJEU**") is formally bound by a decision of the Strasbourg Court, a question that is not dispositive. Even if the CJEU is not bound by a decision of the ECtHR, it would at least apply the principles in *BBW GC*. Indeed, in its own jurisprudence it has gone significantly further.

58 Liberty outlines the relevant principles, then addresses each EU Ground below.

(2) Relevant principles of retained EU law

59 As the DC recorded (2022 J §§2, 36), it is common ground that the principles summarised below remain part of the law of England and Wales as "retained EU law" under the European Union (Withdrawal) Act 2018 ("**EUWA**"). It is also common ground that the DC was bound by pre-IP completion day EU case law, under EUWA s 6(3): 2022 J §37.

60 In addition, it is also common ground (recorded in 2022 J §33) that, because the present claim was commenced in February 2017, well before IP completion day (31 December 2020), the effect of EUWA Schedule 8 para 39(3) is that s 5(4) and Schedule 1 paragraphs 3–4 do not apply. Accordingly, general principles of EU law and the Charter itself remain applicable (as retained EU law), and the Court may disapply a rule of law or determine it is unlawful on that basis of those principles. That outcome reflects Parliament's express post-Brexit choice to retain EU law.

(a) Framework

61 The relevant provisions of the **Charter** are set out at 2022 J §§8–12. They provide for:

61.1 the right to respect for private and family life, home and communications (Art 7);

61.2 the right to the protection of personal data, including control by an independent authority (Art 8);

61.3 the right to freedom of expression, including the right to receive and impart information and ideas and the freedom and pluralism of the media (Art 11);

61.4 the field of application of the Charter (Art 51); and

61.5 controls on derogations from rights to ensure they are provided by law, respect the essence of the right, necessary and proportionate (Art 52).

62 **Directive 2002/58/EC** (the "**e-Privacy Directive**") is the retained EU law *lex specialis* dealing with privacy and electronic communications over public networks (Art 3). Article 1 provides that it is a harmonising measure to ensure protection of fundamental rights within the scope of EU law. Article 15 provides for strict controls on derogations, reflecting Art 52 of the Charter. Further specific requirements are identified below. The relevant provisions are set out in 2022 J §§14–17. Pre-IP completion day EU case law establishes that the substantive requirements these provisions establish give effect to the rights under Charter Arts 7, 8 and 11 and corresponding general principles of EU law.[44]

(b) Relevant constraints imposed by retained EU law

63 Measures that interfere with rights recognised in the Charter/e-Privacy Directive must:

63.1 Have the quality of law. This means that the measures must be "*provided for by law*" (Art 52(1) Charter) and be "*legislative measures*" (Art 15(1) e-Privacy Directive).

63.2 Pursue an objective in the general interest (Art 52(1) Charter), from within those listed in Art 15(1) of the e-Privacy Directive.[45]

63.3 Respect the "essence" of the rights they interfere with (Art 52(1) Charter); and

63.4 Be strictly necessary and proportionate.

64 The CJEU has elaborated on these requirements in: (i) Joined Cases C-203/15 and C-698/15 *Watson v SSHD* and *Tele2 Sverige AB v Post-och telestyrelsen* [2017] QB 771 ("***Watson CJEU***"), which was in turn considered by the Court of Appeal in *SSHD v Watson* [2018] EWCA Civ 70, [2018] QB 912 ("***Watson CA 2018***"); (ii) Case C-623/17 *Privacy International v SSFCO* [2021] 1 WLR 4421 ("***PI***"); and (iii) a further decision of the CJEU heard with and handed down on the same day as *PI*, namely, Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net v Premier Ministre* [2021] 1 WLR 4457 ("***La Quadrature***").

(c) Scope of the e-Privacy Directive

65 The scope of the e-Privacy Directive (and retained EU law) extends to legislative

---

44 Case C-623/17 *Privacy International v SSFCO* [2021] 1 WLR 4421 [57].

45 Case C-623/17 *Privacy International v SSFCO* [2021] 1 WLR 4421 at [66].

measures requiring communications service providers ("**CSPs**") to retain traffic and location data, as well as to measures requiring them to grant public authorities — including security and intelligence agencies — access to that data and subsequent use of the data, including for national security purposes: *PI* at [41], [56] and *dispositif* point 1.

(d) General and indiscriminate regimes impermissible save for national security

66 General and indiscriminate retention (i.e. obtaining and keeping) of data is impermissible under EU law, except where its purpose is the protection of "national security" — there, states may impose measures requiring general and indiscriminate retention of traffic and location data for a limited period of time and subject to particular safeguards: *PI* at [74]–[75]; *La Quadrature* at [134]–[139], [141] and *dispositif* para 1. By contrast, the objectives of preventing and detecting serious crime or preventing serious threats to public security are not capable of justifying general and indiscriminate retention of traffic and location data: *La Quadrature* at [141]–[142].

(e) Legislation providing for retention/obtaining of and access to data must contain certain substantive and procedural requirements (safeguards)

67 *Watson* at [109], *PI* at [68] and *La Quadrature* at [132] establish that, to satisfy the requirement of proportionality, legislation which interferes with rights under Charter Arts 7 and 8 and the e-Privacy Directive must itself lay down clear rules about retention and access. As the CJEU stated in *La Quadrature* [132]:

> "In order to satisfy the requirement of proportionality, the legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse. That legislation must be legally binding under domestic law and, in particular, must indicate in what circumstances and under what conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary." [emphasis added]

68 However, there are different "safeguards" depending on whether the purpose of retention and access to data is protecting national security or any other purpose. One set of safeguards applies to retention and access for the purpose of protecting national security (the "**NS requirements**"). The other set of safeguards (the "***Watson* requirements**") applies to retention and access for the purpose of preventing serious crime and protecting public security, or any other non-national security purpose.

(f) EU law requirements within the context of national security: the NS requirements

69 Retention and access for national security purposes requires various safeguards. They are set out in *La Quadrature* at [176]–[182] and require requests to be specific and reliable, and non-discriminatory, and that there must be human review before automated results lead to a measure adversely affecting an individual. These requirements are not in issue.

(g) EU law requirements outside the context of national security: the Watson requirement for prior independent approval of access

70 The *Watson* requirements continue to apply outside the context of national security: *La Quadrature* at [140]–[151].

71 Only one is in issue: prior independent review for obtaining access. National authorities' access to data "*should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body*": *Watson CJEU* [120]; 2018 J §§18, 38.

72 As the DC said at 2022 J §131, "*the law as stated by the CJEU, and by the Court of Appeal and the Divisional Court in this country, is clear*" and includes such a requirement (described at 2022 J §§121–124). Moreover, Rs rightly conceded before the DC in 2018 that Part 4 was incompatible with the "*requirements*" of EU law because, in criminal investigations, access to retained data was not subject to the purpose of combating "*serious crime*" nor prior independent review by a court or independent administrative body: 2018 J at §§18, 186.

(h) Equivalent protection to the ECHR

73 Article 52(3) of the Charter states:

> "In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection." [emphasis added]

74 Thus, insofar as any IPA provisions are incompatible with ECHR Arts 8 and 10, they are also incompatible with EU law, specifically Charter Arts 7 and 11 (and corresponding general principles). Liberty addresses this point below under EU Ground 3.

(3) EU Ground 1: The Impugned Provisions Provide for General and Indiscriminate Retention and Access and Thus Require Certain Additional Safeguards

(a) The bulk provisions and Parts 3–4 are general and indiscriminate

75 Under the EU case law above, a regime permits (or requires) the "*general and indiscriminate*" retention of and access to data where it provides for the retention or access to data belonging to persons "*for whom there is no evidence to suggest that their conduct might have a link, even an indirect or remote one, with the objective*" pursued, such as preventing serious crime, and, "*in particular, without any relationship being established between the data which is to be transmitted*" (i.e. transferred to the state)[46] and the threat to be prevented: *PI* [80]; *Digital Rights Ireland* [58]–[59]. The CJEU similarly observed that a general and indiscriminate retention and access regime would have "*the effect of making the exception to the obligation of principle to ensure the confidentiality of data the rule, whereas the system established by Directive 2002/58 requires that that exception remain an exception*": *PI* [69].

76 The CJEU found in *PI* at [79]–[82] that Telecommunications Act 1984 ("**TA**") s 94 purported to allow "*general and indiscriminate*" retention of data because the regime did not rely on a link between the objective pursued and the data transmitted to the state. All communications data could be required to be transmitted and, once transmitted, accessed. At *PI* [52], the CJEU noted that these provisions enabled transmission of data that "*concerns all users of means of electronic communication*", and at [59] held that the transmission in that case was carried out "*in a general and indiscriminate way*".

77 The powers under Part 6 Chapter 1, Part 6 Chapter 2, Part 6 Chapter 3, Part 5 (in relation to warrants issued under s 101(1)(b), (c), (e) and (f)) and Part 7, that is, the bulk powers, as well as Parts 3–4, meet this description. By their very nature, bulk (and wide thematic) warrants 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. Rs acknowledged in their evidence below that "*the vast majority of information gathered under the bulk powers in*

---

46 "Transmission" here refers to that under s 94 of the Telecommunications Act 1984, by which CSPs could be compelled to provide communications data to the Secretary of State.

the Act will be of no intelligence interest": Dix 1 §50.[47] This is no accident. Their purpose is to collect data about most people to sift for patterns and people of interest.

78 The bulk provisions do not contain provisions requiring a warrant to be meaningfully narrower than a direction under TA s 94. Indeed, for a BPD, by definition, most of the data is and will be of no interest to the intelligence services (see s 199(1)) and, by s 225, data captured under any other warrant save for a bulk acquisition warrant may be turned into a BPD: see paragraph 47 above. Rather, as long as the purpose of a "bulk" warrant is to safeguard national security and its "main purpose" is to intercept foreign communications, then any data can be retained.

79 In relation to access (which is of limited relevance: see paragraph 83.1 below), for warrants under Parts 6 and 7, selection for examination must be for an operational purpose (see eg ss 138(1)(d), 152(1)) and necessary and proportionate in all the circumstances. However, the operational purposes are not public and their permissible scope is so wide that they do not limit the scope of a bulk warrant in any meaningful way. A warrant may contain all operational purposes (see eg s 142(5)), being all generic purposes for which the state might conceivably wish to select for examination: see paragraph 28.2 above. Further, Part 5 has no corresponding constraint in any event: see paragraph 28.1 above. And in any case, *PI* [80] establishes that, once the state obtains data in a general and indiscriminate manner, it is taken to permit access in a general and indiscriminate manner also.

80 Similarly, Part 4 permits wide retention of data via a retention notice directed to CSPs: 2018 J §136 correctly recognised that the statute permits a retention notice directed to each service provider to retain all communications data for 12 months. Part 3 then permits access to that data.

81 The DC's conclusion that bulk powers and Parts 3-4 are not general and indiscriminate retention and access regimes is, with respect, incorrect.

82 First, 2022 J §140 holds that the bulk powers should be analysed in the same manner as Parts 3–4, and repeats its analysis at 2018 J §§118–138. But even assuming that the

---

47 The Claimant's evidence (which was not contested) explained that this was a necessary effect of a bulk secret surveillance regime: Danezis 1 at §§47–50, 78–80 [***]; see further §§23, 26, 37, 69 [***].

earlier analysis from 2018 J is correct (it is not — see below), the bulk provisions are broader than Parts 3–4. Under Part 4, the Secretary of State is permitted to issue a retention notice to CSPs, who then retain data; the regime is limited to "communications data" (not "content"); at most one year's data can be retained; and Part 3 contains a limited access regime, by which the state may make specific requests linked to an "operation" for access. The suggestion that the bulk provisions can be equated with Parts 3–4 is wrong (and, in any case, as explained below Parts 3–4 are general and indiscriminate). The bulk provisions permit the state directly to access and retain vast amounts of data (including the "content" of communications), the vast majority of which will be of no interest or relevance to national security or the other purposes.

83 Secondly, the earlier analysis in 2018 J §§118–138 is also incorrect. The substance of the reasoning in 2018 J is to: (i) identify what the DC considered to constitute an instance of general and indiscriminate retention on the basis of *Watson CJEU* and *Watson CA*, focussing on the Swedish legislation that was the subject of the reference joined to *Watson* (*Tele2 Sverige*) (2018 J §§121–126); (ii) summarise various matters that must, under Part 4, be considered before a retention notice is given to a CSP, seeking to distinguish Part 4 from the Swedish legislation (2018 J §§127–134); and (iii) conclude that these matters mean the regime is not general and indiscriminate (2018 J §§135–138). Each of these steps is incorrect or flawed:

83.1 The basic error made by the DC is to elide the nature of the regime for collection with the safeguards for access. A general and indiscriminate regime is characterised by the absence of a link between any criminal suspicion (or other harm to the interest protected) and the data collected.[48] The DC's 2018 analysis (which it adopted in 2022 J §140) obviously did not take account of *PI* and *La Quadrature*, which post-date it. Those decisions make 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.

83.2 The Court's approach in 2018 was in any event flawed: instead of seeking to identify what "general and indiscriminate" meant in principle, in substance it elided

48 As Liberty submitted below: Claimant's Skeleton Argument for Substantive Hearing on the Stayed EU Law Challenge dated 26 April 2022 §37 [***].

the Swedish regime (which required the retention of all communications data by all CSPs)[49] with "general and indiscriminate" retention under EU law. Anything less, on the DC's analysis, was not general and indiscriminate, thus the Court's focus on distinguishing IPA Parts 3–4 from the Swedish regime: see 2018 J §127, where the Court begins to identify the provisions it relies upon.[50] Apart from the logical error this entails (treating an example as the test), that approach is unsustainable where the CJEU has since treated far more limited regimes containing safeguards and controls as general and indiscriminate in *La Quadrature* and *PI*.

83.3 Ultimately, the DC in 2018 erred in failing to recognise the key feature of Part 4 that makes it general and indiscriminate: the scope of retention. At 2018 J §135, having identified seven features of the legislation (2018 J §§127–134), it held that the regime was not general and indiscriminate because: "*The legislation requires a range of factors to be taken into account and imposes controls to ensure that a decision to serve a retention notice satisfies (inter alia) the tests of necessity in relation to one of the statutory purposes, proportionality and public law principles.*" But 2018 J §136 held that, even assuming that under Part 4 "*the retention notices that could be issued might be as broad in scope as the statute permits, namely a direction to each service provider to retain all communications data for 12 months*", Part 4 would not be general and indiscriminate, due to its seven features. This is the error in the DC's reasoning: if such wide retention may be required, then the features relied on by the DC do not limit the discretion to require retention. The IPA thus permits general and indiscriminate retention. It does not matter (as it did not matter in *PI* in relation to TA s 94) that the power might (secretly) be exercised in individual cases in a narrower manner.

84 Importantly, a finding that the regime is general and indiscriminate does not without more mean the regime is impermissible. It just means that certain safeguards are required, including limits to the purposes for which the regime may permit retention and access.

---

49 2018 J §121 [***].

50 "*The scheme laid down in Part 4 of the 2016 Act is very different from the Swedish legislation. …*"

(b) Part 7 is within the scope of EU insofar as challenged

85 Liberty's argument below[51] was that, where a BPD contains data that was obtained in the exercise of the other powers under the IPA (as s 225 permits), it is within the scope of EU law and the NS requirements or *Watson* requirements apply to retention and access under Part 7 (see, eg, *PI* [56]).

86 2022 J §139 rejects this submission, for two reasons, each of which is incorrect:

86.1 First, the DC observed that: "*Part 7 does not contain any power to acquire information, still less impose a duty upon CSPs to provide information to the state. Rather it concerns how state authorities should handle bulk personal datasets which they have already obtained under other powers.*" That is right as far as it goes, but fails to meet Liberty's point on Part 7: when Part 7 is applied to retain data obtained under other powers of the IPA, as s 225 expressly permits, Part 7 in substance forms the relevant retention and access regime under Parts 3–4, Part 5 and Part 6 Chapters 1 and 3, all of which were conceded to be within the scope of EU law. On the DC's reasoning, the state could 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). In short, this wrongly elevates form over substance.

86.2 The DC further noted that the Claimant in *PI* had "*conceded that, in the absence of a regime requiring controllers to provide bulk personal datasets to an agency, the regime was outside the scope of EU law*", as recorded at *PI* [45]–[46]. That is correct. But Liberty's challenge was and is to Part 7 where it is used as the regime to store communications that are compelled to be provided to the state under Parts 3–4, Part 5 and Part 6 Chapters 1 and 3.

(c) Incompatibility with EU law

87 Having incorrectly concluded that the bulk provisions and Parts 3–4 were not general and indiscriminate, the DC did not address the limited purposes for which general and indiscriminate retention and access is permitted (see paragraph 66 above).

---

51 Claimant's Skeleton Argument for Substantive Hearing on the Stayed EU Law Challenge dated 26 April 2022 §32.2 [***].

88 Liberty submits that the bulk provisions and Parts 3–4 permit general and indiscriminate retention and access other than for the purpose of "*preventing the most serious threats to national security*". This is unlawful applying *La Quadrature*: see paragraph 66 above.

89 **First,** the Act permits thematic equipment interference warrants under Part 5, BPD warrants under Part 7 and retention notices under Part 4 to be issued to permit the state to obtain, retain and access information for purposes other than national security:

89.1 Thematic equipment interference warrants (Part 5) and BPD warrants (Part 7) may be issued "*for the purpose of preventing or detecting serious crime*" (the "**serious crime purpose**") or "*in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security*" (the "**economic purpose**"): ss 102(1)(a), (5), 103(1)(b), (2)(b), 106(1)(a) in Part 5 and 204(3), 205(6)(a) in Part 7. Thematic equipment interference warrants may additionally be issued for the "*purpose of preventing death or any injury or damage to a person's physical or mental health or of mitigating any injury or damage to a person's physical or mental health*" (the "**death/injury purpose**") when the application is made by a law enforcement chief: ss 106(3).

89.2 Retention notices under Part 4 may by s 87(1) be issued for "*the applicable crime purpose*" (a mixture of serious and non-serious crime depending on the type of data retained), the economic purpose, "*in the interests of public safety*", the death/injury purpose, and "*to assist investigations into alleged miscarriages of justice*".

90 **Secondly**, the Part 6 provisions (bulk interception, acquisition warrants and equipment interference warrants) permit the government to obtain data for the national security purpose as well as the serious crime purpose or the economic purpose, but then (unlawfully) to access data only for the economic purpose or the serious crime purpose. This is because, while the warrant itself and thus the initial retention of data under a bulk warrant must be necessary for purposes including the national security purpose (see, eg, s 138(1)(b)(ii)),[52] selection for examination of content and secondary data may occur for any operational purpose, and an operational purpose may be referable only to the crime

[52] Warrants themselves may be issued for the national security purpose or for the national security purpose and one or both of the economic purpose and the serious crime purpose.

purpose or the economic purpose (see, eg, s 138(1)(d)(ii)).[53]

(4) EU Ground 2: Failure to Provide for Prior Independent Authorisation outside National Security in the Bulk Provisions

91 Even if the regimes are not general and indiscriminate, the *Watson* requirements apply to the bulk powers where data is obtained and retained or accessed for the crime purpose or economic purpose and also (in the case of Part 5) for the death/injury purpose.

92 The *Watson* requirement in issue is prior independent authorisation of access to retained data under the bulk powers, where a targeted examination warrant is not required.

93 As explained in paragraph 71 above, the DC correctly accepted that a requirement for prior authorisation by a court or other independent body exists. Further, it rightly proceeded on the basis that it applied to the bulk powers (save for Part 7)[54] where data was accessed for a purpose other than national security: 2022 J §§144–145.

94 However, the DC incorrectly concluded (2022 J §145) (emphasis added): "*The requirement for independent authorisation is satisfied by the need for approval to be obtained from a Judicial Commissioner for a bulk warrant which addresses not only the obtaining of data but also access thereto.*" This is, with respect, incorrect.

95 The DC held that "*Watson CJEU did not go so far as to require separate independent authorisation each time retained data is selected for examination or accessed*": 2022 J §145. That does not answer Liberty's point, which is that *Watson CJEU* distinguishes between the retention and access, and envisages separate authorisation for access on a case-specific basis (not just initial authorisation for retention, as the DC in effect held):[55]

---

53 This is because an operational purpose may be included in the warrant where examination for that operational purpose is necessary on any of the grounds on which the warrant is considered necessary, which includes, if they are included as purposes of the warrant, (just) the economic purpose and/or the serious crime purpose.

54 The DC wrongly held that Part 7 falls outside the scope of EU law: paragraphs 85–86 above.

55 For example, an authorisation may permit multiple searches (i.e. selections for examination or access requests) and, perhaps, further searches based on their results, for a given case. But it is impermissible to have no independent access authorisation at all.

95.1 *Watson CJEU* addresses authorisation of retention at [62]–[112] in answer to the first question, and at [109] states that a *Watson* requirement is that "*legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary*" (emphasis added).

95.2 The CJEU then addresses authorisation of access to retained data at [113]–[125] in answer to the second question, and at [120] says:

> "In order to ensure, in practice, that those conditions are fully respected, it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime …" [emphasis added]

The DC's suggestion that (outside situations where a targeted examination warrant is required) the initial authorisation of retention under the bulk powers, which makes no provision for access authorisation (beyond, in the case of Part 6 Chapters 1 and 3 and Part 7,[56] but not Part 5, specifying the generic operational purposes for which material may be searched), is sufficient is incorrect applying *Watson CJEU*.

96 The DC's reasoning is also inconsistent with its finding that Parts 3–4 still fail to comply with the requirement for prior independent authorisation precisely because access by MI5, MI6 and GCHQ was not (separately and) independently authorised: 2022 J §§121–132.

97 The failure of the bulk provisions to provide for prior independent authorisation of access is thus incompatible with retained EU law. For the avoidance of any doubt, for the reasons in paragraph 86 above, this applies also to Part 7 as there set out.

(5) EU Ground 3: At Least Equivalent Protection under the Charter to the ECHR

98 Charter Art 52(3) provides that EU law confers at least equivalent protection to equivalent ECHR rights. Where the IPA is incompatible with the ECHR, there is also a

---

[56] See ss 138(1)(d), 158(1)(c), 178(1)(d), 204(3)(c), 205(6)(c). As to operational purposes, see, eg, s 142.

breach of the corresponding EU law rights under Art 7 and 11 of the Charter. The DC erred in holding otherwise.

(a) Incompatibilities with the ECHR

99 Rs have conceded in light of *BBW GC* that:

99.1 Part 6 Chapter 1 is incompatible with Arts 8 and 10 ECHR for its failure to provide adequate journalistic protections pursuant to *BBW GC*: see paragraph 19 above.

99.2 Part 6 Chapter 1 is incompatible with Art 8 ECHR because it does not require prior internal authorisation for use of strong selectors linked to identifiable individuals.

100 There is no sensible basis for the refusal to make these concessions in relation to Part 6 Chapters 2 and 3, Part 7 and Part 5 and (in relation to journalistic protections) Parts 3–4: see paragraphs 21–23 above and the Annex. Further, as set out in Part B, the IPA is incompatible with the ECHR in the respects identified by ECHR Grounds 1–5.

(b) Equivalent protection under the Charter

101 To the extent the Court accepts that the IPA is incompatible with the ECHR, it follows from Art 52(3) of the Charter (and equivalent aspects of EU law general principles) that those provisions are also unlawful under Charter Arts 7 and 11 and corresponding general principles of EU law.

102 The correspondence between ECHR Art 8 and Charter Art 7 was well established well before IP completion day. For example, in Case C-400/10 PPU *McB v LE* [2011] Fam 364 [53] the CJEU said:

> "Moreover, it follows from article 52(3) of the Charter that, in so far as the Charter contains rights which correspond to rights guaranteed by the ECHR, their meaning and scope are to be the same as those laid down by the ECHR. However, that provision does not preclude the grant of wider protection by European Union law. Under article 7 of the Charter, 'Everyone has the right to respect for his or her private and family life, home and communications'. The wording of article 8.1 of the ECHR is identical to that of the said article 7, except that it uses the expression 'correspondence' instead of 'communications'. That being so, it is clear that the said article 7 contains rights corresponding to those guaranteed by article 8.1 of the ECHR. Article 7 of the Charter must therefore be given the same meaning and the same scope as article 8.1 of the ECHR, as interpreted by the case law of the European Court of Human Rights: see, by analogy, *Varec SA v Belgium (Diehl Remscheid GmbH & Co intervening)* (Case C-450/06) [2008] ECR I-581, para 48." [emphasis added]

103 Article 52(3) of the Charter expressly requires that Arts 7 and 11 provide the same level

of protection as ECHR Arts 8 and 10. Indeed, the CJEU has generally gone significantly further in its jurisprudence than the ECtHR.

104 Given the admitted breaches of the ECHR, there was also a breach of EU law. The DC rejected this argument: 2022 J §§149–158. It was wrong to do so. The four reasons given are not applicable in this appeal (in light of *BBW GC* in particular) or are incorrect:

104.1 First, 2022 J §151 said it was not appropriate for the DC to act on *BBW GC* in circumstances where it had reached contrary views in the 2019 J. It concluded that: "*What view the Court of Appeal will take is not a matter for us.*" This leaves matters open for this Court to consider.

104.2 Secondly, 2022 J §§152–155 contains an analysis of whether the CJEU was technically bound by *BBW GC*. That is at best a distraction: the relevant point is what the content of Charter Arts 7 and 11 is and whether they confer at least the same protection as ECHR Arts 8 and 10.

104.3 Thirdly, 2022 J §156 pointed out that, if *BBW GC* were a judgment of the CJEU, it would not bind the High Court, as it was handed down after IP completion day. But Parliament's choice was to retain the obligations in the Charter in the circumstances of this case.

104.4 Fourthly, 2022 J §158 said:

> "Finally, we bear in mind that the Government has already stated that it intends to amend the IPA in order to address the defects which were identified by the Grand Chamber in *Big Brother Watch*: see the written Ministerial Statement of 31 March 2022. In those circumstances, it would not be appropriate for this Court to anticipate exactly how the Government and Parliament of the UK must act in order to comply with the judgment in *Big Brother Watch*."

The fact the government has announced that it expects to amend legislation in the future does not excuse the Court from identifying legal defects in existing legislation that is currently in force and in daily use. In any case, this is not a substantive reason directed at the content of Charter Arts 7 and 11.

105 In short, the relevant rights under EU law are at least as extensive as those under the ECHR, as is well-established. Article 52(3) of the Charter in terms so requires. The DC was therefore wrong not to find any breach of EU law on this basis.

106 Further, if and to the extent that this Court accepts that there are further incompatibilities with the ECHR, as Liberty submits to be the case (see Part B), these give rise to a retained EU law remedy on the same basis.

D RELIEF

107 It is likely to be convenient to address relief once this Court's decision on the substance of both the ECHR and EU law grounds is known. In general terms, Liberty submits that:

107.1 It is appropriate to allow the appeal and declare that the IPA is incompatible with retained EU law, and with Arts 8 and 10 ECHR, in the respects identified above.

107.2 If and insofar as any legislative change is introduced and in fact cures an incompatibility, it is nonetheless appropriate to make a declaration as to the position prior to amendment.

107.3 The Court has power in respect of EU law issues to briefly suspend the effect of any declaration it makes if real harm to the public interest would otherwise occur, as the DC did in relation to the declaration of incompatibility with EU law that it made.[57]

108 The parties have agreed that there should be no order as to the costs of the appeal (save in certain exceptional and presently irrelevant circumstances).

BEN JAFFEY KC
DAVID HEATON
SOPHIE BIRD

BHATT MURPHY **7 October 2022**

[57] DC's Reasons on Remedies and Permission to Appeal dated 22 July 20 [2]–[4].

ANNEX: ECHR GROUND 1 — JOURNALISTIC PROTECTIONS — DEFECTS

A.1 The provisions of the IPA are incompatible with Art 10 (and Art 8) in the following respects:

A.2 For **Part 6 Chapter 1** (bulk interception) and **Part 6 Chapter 3** (bulk equipment interference):

A.2.1 The IPA provides only, in ss 154 and 195, that, where CJM obtained under a bulk warrant is retained following examination, the Investigatory Powers Commissioner ("**IPCr**") must be informed. The Codes of Practice provide only that, where an authorised person intends to select for examination intercepted content (only, not secondary data) "*in order to identify or confirm a source of journalistic information*" or "*which the [agency] [equipment interference authority] believes is confidential journalistic material*" (and no targeted examination warrant is required), a senior official is notified.[58] That is inadequate.

A.2.2 These provisions fail to require independent authorisation of selection for examination (i.e. searches) in any of the circumstances identified in paragraph 16.1 above, except where it so happens that a targeted examination warrant must be sought under Part 2 Chapter 1 (see s 15(3)) or Part 5 (see s 99(1)(b), (9)). This is not triggered by anything to do with CJM. That requirement arises only where (i) search criteria referable to an individual who is in the British Islands are used and (ii) the purpose of their use is to identify that individual's communications or information (i.e. the 'British Islands safeguard'): see ss 152(1)(c), (3)–(4) and 193(1)(c), (3)–(4)[59] (and ss 15(3) and 99(1)(b), (9)).

---

58 Interception Code of Practice §§9.84–9.87; Equipment Interference Code of Practice §§9.81–9.84.

59 If either condition is not met, there is no need for a targeted examination warrant and so no independent judicial authorisation. Thus, for example, there will be no judicial commissioner or other independent approval where it is sought to select using criteria referable to J, a journalist who is in the British Islands, in order to identify the communications of S, J's source (who is not (known to be) in the British Islands).

A.2.3 Even then, these provisions fail to require an overriding requirement in the public interest (assessed by the independent decision-maker) in any of the circumstances identified in paragraph 16.1 above (even where the purpose of the search is to identify a journalistic source), again except where both (i) it so happens that a targeted examination warrant must be sought (that is, where the British Islands safeguard applies, as explained immediately above) and (ii) a purpose of the warrant is "*to determine the source of journalistic information*".[60]

A.2.4 Further, neither Part 6 Chapter 1 or Part 6 Chapter 3 (or their Codes of Practice) requires independent authorisation justified by an overriding requirement in the public interest for continued use and retention where CJM is identified when the results of a search are examined (i.e. in the circumstances identified in paragraph 16.3 above).[61]

A.3 For **Part 7** (BPDs) and **Part 6 Chapter 2** (bulk acquisition of communications data), no statutory or code provision requires independent authorisation of selection for examination (save, under Part 7, in relation to privileged items):[62] see ss 221 and 172 respectively. The relevant Codes do provide that "*[w]here the intention is to select for examination data in order to identify a source of journalistic information*" there must be

---

60 Interception Code of Practice §9.74; Equipment Interference Code of Practice §9.76. Both Codes are clear that this applies only (relevantly) where a targeted examination warrant is sought.

For completeness, while ss 28–29 and 113–114 make further provision, they only require that (i) warrant applications for a purpose of identifying or confirming a source of journalistic information or for obtaining material which the applicant believes to be CJM must state that purpose and (ii) a warrant may only be issued where the person to whom the application is made believes that "*specific arrangements for the handling, retention, use and destruction*" of such material exist. These thus do not require prior independent authorisation or an overriding requirement in the public interest.

61 Interception Code of Practice §9.88 and Equipment Interference Code of Practice §9.84 merely require reporting to the IPCr, which is manifestly inadequate.

62 As to which see ss 222–223.

an overriding requirement in the public interest.[63] The only requirement in the Code for Part 7 where CJM is identified in search results is to inform the IPCr;[64] there is no equivalent requirement in the Code for Part 6 Chapter 2.[65] These provisions are thus inadequate: they do not require independent authorisation, and do not require an overriding requirement in the public interest (assessed by the independent authoriser) in all the circumstances identified in paragraphs 16.1 and 16.3 above, for example, where a search uses terms known to be connected to a journalist, where selection of CJM is likely (irrespective of whether the intention is to identify or confirm a source) or where CJM is identified when the results of a search are examined.

A.4 For **Part 5** (thematic equipment interference), while thematic equipment interference warrants must be independently authorised (ss 102(1)(d)), 103(1)(e), (2)(e), 104(1)(d), 106(1)(d), (3)(d), 108), there is a need for an overriding requirement in the public interest (as assessed by the independent authoriser) only where a purpose of the warrant is "*to determine the source of journalistic information*".[66] Again, the only requirement where CJM is identified is to inform the IPCr.[67] These provisions are again inadequate: they do not require an overriding requirement in the public interest (assessed by the independent authoriser) in all the circumstances identified in paragraphs 16.1 and 16.3 above.

A.5 For **Parts 3–4** (communications data acquisition and retention):

A.5.1 For acquisition of communications data under s 60A, where a public authority's access request must be independently authorised by the Investigatory Powers Commissioner (which in practice occurs via the Office of Communications Data Authorisation), there is necessarily independent authorisation (under s 60A itself), but the requirement in s 77 for there to be "*another overriding public interest*" (in s 77(6)(b)) apples only where the authorisation is "*for the purpose*

63 Bulk Personal Datasets Code of Practice §7.45 (emphasis added); Bulk Communications Data Code of Practice §6.25.

64 Bulk Personal Datasets Code of Practice §7.48.

65 Compare Bulk Communications Data Code of Practice §§6.25–6.31.

66 Equipment Interference Code of Practice §9.76. See footnote 60 above on ss 113–114, which do not meet the Art 10 requirements as set out in *BBW GC*.

67 Equipment Interference Code of Practice §9.84.

of identifying or confirming a source of journalistic information" (s 77(1A)(a)). The requirement for an overriding public interest (assessed by the independent authoriser) is therefore not accorded in all the circumstances identified in paragraphs 16.1 and 16.3 above.

A.5.2 For acquisition of communications data under s 61, which permits MI5, MI6 and GCHQ to self-authorise access to communications data generally, s 77 does require independent approval (s 77(2)) and "*another overriding public interest*" (s 77(6)(b)), but again only where a request is made "*for the purpose of identifying or confirming a source of journalistic information*" (s 77(1)(a)). Accordingly, for s 61 acquisition, there is neither independent authorisation nor a requirement for an overriding public interest in all the circumstances identified in paragraphs 16.1 and 16.3 above.