IN THE COURT OF APPEAL **Appeal Ref:**

ON APPEAL FROM

THE QUEEN'S BENCH DIVISION

ADMININSTRATIVE COURT

[2019] EWHC 2057 (Admin)

Singh LJ and Holgate J

B E T W E E N:

THE QUEEN

on the application of

THE NATIONAL COUNCIL FOR CIVIL LIBERTIES ("LIBERTY")

Appellant

- and -

(1) SECRETARY OF STATE FOR THE HOME DEPARTMENT

(2) SECRETARY OF STATE FOR THE FOREIGN, COMMONWEALTH AND DEVELOPMENT OFFICE

Respondents

- and -

NATIONAL UNION OF JOURNALISTS

Intervener

GROUNDS OF APPEAL ON THE ECHR CLAIM

References to the judgment of the Grand Chamber in *Big Brother Watch v United Kingdom* (Application Nos 58170/13, 62322/14, 24960/15, Grand Chamber, 25 May 2021) ("*BBW GC*") take the form *BBW* §*para*.

References to 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), take the form J §*para*.

GROUND 1: ABSENCE OF ADEQUATE JOURNALISTIC / WATCHDOG SAFEGUARDS[1]

1 The Court erred in holding (J §§293–352) that the IPA provides sufficient safeguards to protect journalistic materials. The absence of adequate journalistic safeguards is incompatible with Articles 8 and 10 ECHR.

2 In particular, the Court erred (at J §§320–337 and 340–347) in that Articles 8 and 10 ECHR require that:

(1) There must be prior authorisation, by a judge or another independent body, of searching of data obtained or retained (that is, of selection for examination or acquisition of communications data) using search terms (or selectors) that 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 (alternatively probable), whether or not the searching intelligence service wishes or intends to identify a journalistic source (see *BBW GC* §§448–450, 525–528).

(2) The search (i.e. the use of the proposed search terms or other identifying details) in those circumstances must be "*justified by an overriding requirement in the public interest*", and the prior authorisation must include the judge or other independent body itself considering whether this is so and, in particular, whether a less intrusive measure might suffice (see *BBW* §448).

(3) Where it becomes apparent at any point during examination that CJM has been (or is likely to have been or to be) selected for examination, even if the search terms were not intended or thought likely to lead to this, continued use and retention must be (i) justified by an overriding requirement in the public interest and (ii) authorised by a judge or another independent body, with power to determine whether that criterion is satisfied (see *BBW* §450).

3 None of Parts 3–4,[2] Part 5, Part 6 Chapter 1, Part 6 Chapter 2, Part 6 Chapter 3, and Part 7

---

1 References herein to "journalists" and "journalistic" encompass campaigning / watchdog organisations such as Liberty, which J §351 held must be accorded the same protections as journalists and media organisations.

2 As to Part 3, while independent authorisation is always required under the s 60A power, it is not required under the s 61 power, save as provided by s 77. Section 77(1)–(1A) require independent authorisation only where a request is made "*for the purpose of identifying or confirming a source of journalistic information*". They accordingly do not accord the required protections in all circumstances Articles 8 and 10 require.

(and the associated Codes), including when read with the definitions of "*journalistic material*" and "*confidential journalistic material*" in s 264, contains the requirements set out above (at least in all circumstances) and, to the extent it does not, each power is incompatible with Articles 8 and 10.

4 The Court erred in holding (J §352) that the exclusion of material that was "*created … with the intention of furthering a criminal purpose*" from the safeguards for journalistic materials in the IPA is compatible with Articles 8 and 10 ECHR. This exception (which would apply, for example, to a document disclosing gross incompetence or misconduct by a senior government official that was copied and provided to a journalist, assuming the copying and provision to be unlawful) means that the protection required by Articles 8 and 10 is not provided.

GROUND 2: ABSENCE OF SAFEGUARDS IN THE BULK REGIMES AND PART 5

5 The Court erred in failing to hold that Article 8 ECHR requires independent authorisation of the categories of search terms (or selectors) at the point of initial authorisation of secret surveillance (see *BBW GC* §§353–355, 381–383, 416, 425). Article 8 so requires, none of Part 5, Part 6 Chapters 1–3 and Part 7 or the associated Codes contains such a requirement, and they are to that extent incompatible with Article 8.

6 The Court erred in failing to hold that Article 8 requires separate and objective internal authorisation and verification of the proportionality of the use of strong selectors (i.e. search terms) linked to identifiable individuals, before they are applied (and a record of the justification for their use to be kept) (see *BBW GC* §§353–355, 382–383, 416, 425). Article 8 so requires, there is no provision for this in Part 5, Part 6 Chapters 1–3 and Part 7 or the associated Codes, and they are to that extent incompatible with Article 8.

7 The Court erred (J §§171–178, 228–234) in failing to hold that the provisions below are incompatible with Article 8 because the distinction they draw between "content" and "communications data" (or similar concepts), or their different treatment of these, is not "*objectively and reasonably justified*" (see *BBW GC* §423):

(1) Part 6 Chapter 1 and Part 6 Chapter 3, insofar as they distinguish between "*content*" and "*secondary data*"/non-"*protected material*" and the British Islands safeguard does not apply to the latter;

(2) Part 6 Chapter 2 (bulk acquisition warrants), insofar as it does not contain a British Islands safeguard; and

(3) Part 7, insofar as it does not contain a British Islands safeguard, including for selection for examination of content.

GROUND 3: ABSENCE OF SAFEGUARDS IN RELATION TO SHARING MATERIAL WITH OVERSEAS AUTHORITIES

8 The Court erred in failing to hold that Article 8 ECHR requires a secret surveillance regime to have the following safeguards where material may be shared with overseas authorities, that none of Part 5, Part 6 Chapters 1–3 and Part 7 contains such requirements, and that each of those provisions is to that extent incompatible with Article 8 (see *BBW GC* §362):

(1) the material shared had been collected and stored in a Convention-compliant manner;

(2) the circumstances in which such a transfer may take place are clearly set out in domestic law;

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

(4) heightened safeguards are necessary where "*material requiring special confidentiality*", such as CJM, is transferred; and

(5) transfer of material to foreign intelligence partners is subject to independent control.

9 In particular, the Court should have held that:

(1) The sections governing provision of material to "*overseas authorities*" in Part 5 and Part 6 Chapters 1–3[3] and the associated Codes permit the Secretary of State, in her discretion, to determine that material may be provided without any safeguards.

(2) Part 7 and the associated Code make no provision in relation to provision of BPDs to overseas authorities.

---

[3] Sections 129(2), (5), (9)–(10), 130 (Part 5), 150(2), (5) and (7)–(8), 151–152 (Part 6 Chapter 1), 171(2), (5), (7)–(10) and 172 (Part 6 Chapter 2), 191(2), (5), (7)–(8), 192–193 (Part 6 Chapter 3).

(3) None of Part 5, Part 6 Chapters 1–3 and Part 7 and the associated Codes contains the provisions required by Article 8 as explained in *BBW GC*.

GROUND 4: IMPERMISSIBLY BROAD BULK PERSONAL DATASETS REGIME (PART 7)

10 The Court erred (J §§223–224) in failing to hold that the statutory requirements as to what is authorised to be retained in a Part 7 BPD and the circumstances in which a BPD warrant may be issued (in ss 199(1), 204(3) and 205(6)), that is, the scope of application of Part 7, do not satisfy the Convention requirement of foreseeability and Part 7 is accordingly incompatible with Article 8.

11 The Court further erred (J §§223–224) in that:

(1) It failed to make any finding as to whether and why the scope of application of the provisions is sufficiently defined.

(2) It held that the scope of application of the provisions was sufficiently defined because a Judicial Commissioner was unlikely to approve the retention of a particular BPD whose retention would have been unlawful. Article 8 requires that State databases of private information be sufficiently well defined in legislation or other binding measure.

GROUND 5: ABSENCE OF ADEQUATE SAFEGUARDS FOR LAWYER–CLIENT COMMUNICATIONS

12 The Court erred in holding (J §§271–292) that Article 8 ECHR does not require a secret surveillance regime to require as safeguards (i) prior independent authorisation of selection for examination of legally privileged material, and (ii) an overriding requirement in the public interest to justify such selection for examination (determined by the independent authoriser), (iii) in all cases where (a) the communications of someone known to be a lawyer are accessed, (b) it is likely (alternatively probable) that that lawyer–client communications will be accessed or (c) it becomes apparent that such material is being examined. The Court ought to have held that Article 8 requires substantially identical safeguards in a secret surveillance regime for lawyer–client communications as for journalistic materials (see *Szabó and Vissy v Hungary* (2016) 63 EHRR 3 §77) and, accordingly, that these safeguards are required, that Parts 3–4, Part 5, Part 6 Chapters 1–3

or Part 7 do not require these safeguards (or do not require them in all circumstances where this is required) and that each is to that extent incompatible with Article 8.

13 Further, the Court ought to have held that any difference in the treatment of lawyer–client communications (or related communications) in different provisions must be objectively justified (see *BBW GC* §§416–423), that Part 6 Chapter 1 and Part 6 Chapter 2 treat the same lawyer–client communications (or related data) differently, that there is no objective justification for this, and that for this reason also these provisions are incompatible with Article 8.

GROUND 6: THE INEFFECTIVENESS IN PRACTICE OF THE IPA TO ENSURE CONVENTION COMPLIANCE

14 The Court erred in holding (J §§353–392) that serious defects in MI5's systems from 2010 onwards that were disclosed in April 2019, which indicated that MI5 had failed to observe safeguards as to (at least) retention, review and destruction of large amounts of data and made false statements to Judicial Commissioners about its systems (all of which was not properly disclosed to the Secretary of State or oversight bodies until March 2019): (i) were not relevant to its assessment of whether the impugned provisions were "in accordance with the law" (J §§387–388); and (ii) did not demonstrate that the safeguards were not effective in practice (§389).

15 The Court ought to have held that: (i) it was required, as a matter of principle, to consider the effectiveness of the safeguards in practice in considering their compatibility with Articles 8 and 10 ECHR (see *BBW GC* §360); (ii) the matters disclosed (alternatively, taken with the subsequent disclosure in *Liberty and Privacy International v Security Service* (IPT Claim No IPT/20/01/CH))[4] demonstrate that the safeguards in the IPA are not effective in practice; and (iii) for this reason also, the impugned provisions are not "*in accordance with the law*" or "*prescribed by law*" under Articles 8 and 10.

BEN JAFFEY QC
DAVID HEATON
SOPHIE BIRD

BHATT MURPHY

20 May 2022

[4] Liberty has been given permission by the IPT to use these materials for the purposes of this claim.