IN THE INVESTIGATORY POWERS TRIBUNAL

Claim No. IPT/15/110/CH

B E T W E N:

PRIVACY INTERNATIONAL

Claimant / Applicant

- and -

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS

(2) SECRETARY OF STATE FOR THE HOME DEPARTMENT

(3) GOVERNMENT COMMUNICATION HEADQUARTERS

(4) SECURITY SERVICE

(5) SECRET INTELLIGENCE SERVICE

Respondents

Claim No. [ ]

(1) LIBERTY

(2) PRIVACY INTERNATIONAL

Claimants

- and -

(1) SECURITY SERVICE

(2) SECRETARY OF STATE FOR THE HOME DEPARTMENT

Respondents

GROUNDS OF CLAIM AND

APPLICATION TO AMEND AND RE-OPEN CLAIM NO. IPT/15/110CH

IN RELATION TO THE SECURITY SERVICE

References to the attached bundle take the form [**B/*tab*/*page***].

A SUMMARY

1 Liberty and Privacy International ("**PI**") bring a new claim, and PI also applies to amend its existing claim in Claim No. IPT/15/110/CH (the "**Existing BPD/BCD Claim**") so as

to put before the Investigatory Powers Tribunal (the "**IPT**" or the "**Tribunal**") the Security Service's ("**MI5**'s") non-compliance, over an extended period, with the basic statutory safeguards in the Investigatory Powers Act 2016 ("**IPA**") and their equivalents in predecessor legislation, regulations and statutory and non-statutory arrangements, in particular the non-statutory arrangements for bulk communications data ("**BCD**") and bulk personal datasets ("**BPD**").

2 These longstanding and serious failings — which were withheld from the Investigatory Powers Commissioner ("**IPCr**") and his predecessors until February 2019 — began to emerge piecemeal through PI's Existing BPD/BCD Claim in the Tribunal, which commenced in November 2015. Such failings were disclosed more fully in Liberty's challenge to the IPA before the Divisional Court (the "**IPA Challenge**"), in detail that raises the obvious question as to why this material was not disclosed in the Existing BPD/BCD Claim. The Defendants to the IPA Challenge first indicated on 17 April 2019 that as a matter of candour they needed to disclose this material. It was first disclosed in heavily redacted form in OPEN, after consideration by Special Advocates (but without their agreement on redactions), on 7 June 2019 (the "**Initial MI5 Disclosure**"), shortly before the substantive hearing on 17–21 June 2019. Slightly less redacted documents were later disclosed.[1]

3 The disclosures indicate that there have been significant intrusions into individuals' privacy, contrary to domestic law and without any justification, at a systemic level, due to the creation and continued use, over a significant period, of inadequate systems for data retention, management and destruction.

4 The conduct of the Secretary of State for the Home Department ("**SSHD**") and MI5 in relation to the grant of warrants and the obtaining, retention and destruction of potentially sensitive data under them has been unlawful, both under domestic judicial review principles and under the Human Rights Act 1998 ("**HRA**").

5 In broad summary:

(1) The SSHD and MI5 have acted unlawfully as a matter of domestic law, including by failing to follow mandatory statutory requirements under the IPA and the Regulation

[1] This is the form of documents that are enclosed to this pleading.

of Investigatory Powers Act 2000 ("**RIPA**") relating to the obtaining, retention, use and destruction of personal data, as well as failing to follow policies (including codes of practice), in particular for handling bulk and other intercept material and possibly material obtained via equipment interference or otherwise.

(2) MI5 appears to have led Ministers, the IPCr and Judicial Commissioners to grant warrants (and the SSHD to grant directions for acquisition of BCD under section 94 of the Telecommunications Act 1984 ("**TA**")) on a false basis as to its arrangements for the retention, review and destruction of personal data obtained by bulk and other means over an extended period.

(3) In consequence, MI5 and the SSHD have obtained, processed and retained potentially highly intrusive personal data in ways that are: (i) *ultra vires*, unlawful and invalid under domestic law; (ii) not "*in accordance with the law*" or "*prescribed by law*" and disproportionate under Articles 8 and 10 of the European Convention on Human Rights ("**ECHR**"), thus contrary to s 6 of the HRA; and (iii) not "*prescribed by law*" under Articles 7, 8 and 11 (read with Article 52) of the EU Charter of Fundamental Rights ("**CFR**") nor effected by a "*legislative measure*" under Article 15 of the Directive 2002/58/EC (the "**ePrivacy Directive**").[2] MI5 and the SSHD's actions are unlawful for each of these reasons.

(4) Further, the Tribunal is respectfully invited to consider, once it has conducted appropriate investigations and has all relevant material, in full, whether the material disclosed demonstrates that the RIPA and IPA regimes were and are themselves not "*in accordance with the law*" or "*prescribed by law*" under Articles 8 and 10 ECHR (and Articles 7, 8 and 11 CFR), or not necessary in a democratic society, as they demonstrate that, even if the regimes otherwise contain sufficient safeguards to meet these requirements, those safeguards are not effective in practice.

(5) The Claimants are victims for the purposes of the ECHR as they reasonably consider that they are likely to be victims of the unlawful conduct, which is likely to have affected large numbers of persons including NGOs. PI's privacy rights have been

[2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201/37.

breached: the IPT has already found that the Security and Intelligence Agencies unlawfully collected, retained and processed bulk data relating to PI (see paragraph 99 below). Other NGOs such as the South African Legal Resources Centre and Amnesty International have previously been found by the Tribunal to have been victims of unlawful conduct by the UK intelligence agencies: Amended Open Determination dated 22 June 2015 [2015] UKIPTrib 13_77-H_2. More generally, Liberty and PI are users of telecommunications systems in the UK, so are subject to the regimes. The test in *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) for victim status is therefore satisfied. In any event, the Claimants have standing to complain about the breaches of domestic law pleaded below as a result of their belief that they have been the subject of unlawful conduct by MI5.

6 Liberty and PI both bring a new claim in the Tribunal, as set out in summary form in Forms T1 (human rights) and T2 (judicial review) (the "**New Claim**") and in further detail below.

7 PI in addition, seeks permission to amend its Existing BPD/BCD Claim and for the Tribunal to re-open its judgments into MI5's compliance with Article 8 ECHR and the legality of its BPD/BCD regime (the "**Amendment Application**"). It does so in circumstances where it appears that the material referred to below ought to have been disclosed in that claim and is material to the Tribunal's conclusions reached to date.

8 Procedurally, both PI's Amendment Application and the New Claim ought to be case managed together, and with the Existing BPD/BCD Claim. They raise overlapping or (at least) related issues. The extent of any overlap is likely to become clearer if and when proper disclosure is given.

9 The Tribunal is invited, for the New Claim, to instruct the existing Counsel to the Tribunal in the Existing BPD/BCD Claim, given the overlap with the Existing BPD/BCD Claim.

10 For convenience, Liberty and PI are referred to herein as the "**Claimants**", although PI is also an applicant in relation to the Amendment Application.

B THE FACTS

11 The facts relevant to this challenge begin with those set out in the Divisional Court's judgment of July 2019 in relation to Liberty's challenge to the IPA under the ECHR: *R (Liberty) v Secretary of State for the Home Department* [2019] EWHC 2057 (Admin),

[2020] 1 WLR 243 [353]–[392] (the **"IPA Judgment"**). An extract from the IPA Judgment, upon which the Claimants rely, is attached: [**B/15/283-293**].

12 That factual section of the IPA Judgment was based on the Initial MI5 Disclosure, that is, documents disclosed, in heavily redacted form, in the IPA Challenge. The Initial MI5 Disclosure is attached: [**B/1-10/69-130**]. The Divisional Court considered that it was able to determine the IPA Challenge without seeing the unredacted versions of those documents or of the July 2019 Compliance Improvement Review (see paragraph 48 below).[3]

13 The Claimants respectfully invite the Tribunal to obtain and consider, *inter alia*:

(1) unredacted versions of all the documents referred to below (and potentially documents referred to in the redacted parts, of which the Claimants have no knowledge);

(2) previous versions of those documents,[4] which may assist in understanding the manner in which disclosures were made by MI5 to the IPCr; and

(3) all documents referred to in those documents, in particular MI5 Board Papers, its corporate registers, and similar materials, as these are likely to shed light on MI5's corporate knowledge.

14 The Initial MI5 Disclosure documents referred to below are included in Appendix 2 below. A list of previous versions and documents referred to in the Initial MI5 Disclosure documents, insofar as the Claimants are able to identify them from the Initial MI5 Disclosure, is attached as Appendix 3.

(1) The Initial MI5 Disclosure

15 The Initial MI5 Disclosure shows in summary that:

---

3 The Claimants address the Divisional Court's findings on the conclusions to be drawn from this material in Part C below.

4 For example, the First Inspection Report (as defined below) is "Version 2, issued 29 March 2019" [**B/2/74-90**]. Version 1 was requested by the Special Advocates but never disclosed (on the basis of its asserted irrelevance) in the IPA Challenge.

(1) From as early as 2014,[5] MI5 persistently and knowingly failed to comply with the safeguards in s 15 of RIPA and later with the equivalent IPA provisions;[6]

(2) MI5 was unable to carry out proper disclosure searches for proceedings in the IPT (thus undermining its effectiveness as a route of challenge and a means of ensuring lawful conduct); and

(3) The UK's regime for oversight of secret surveillance failed to identify these serious systemic problems, even when raised at MI5 Board level in January 2018.

16 The MI5 disclosure therefore demonstrates that the IPA and RIPA safeguards relating to examination, use, storage and destruction, and oversight arrangements, have not been effective in practice in certain — apparently extensive — instances. More specifically, it shows that MI5 has not in practice observed the central safeguards under the RIPA s 8(4) regime and the associated Code of Practice, and under IPA Part 6 Chapter 1 (at least), relating to:

(1) Access control for material obtained under warrants;

(2) Copying of material obtained under warrants;

(3) Review, retention and destruction ("**RRD**") of "*operational data*"[7]; and

(4) Identification and review, retention and deletion of lawyer–client communications subject to legal privilege.

The evidence further shows that the oversight mechanisms — the Commissioner and the Tribunal under RIPA and the IPCr, the Tribunal and the Judicial Commissioners under the IPA — did not identify this systemic issue, and also that MI5 was not able (or otherwise failed) properly to carry out disclosure searches for proceedings in the Tribunal.

---

5 The subsequently-disclosed Compliance Improvement Review of Sir Martin Donnelly (June 2019) states at §16 that "*compliance failure risk had been reported to the Management Board as early as 2010*".

6 The bulk interception regime under the IPA commenced in full on 27 June 2018. As the new evidence relates to non-compliance dating from at least 2014, the Applicants understand that non-compliance to extend to material obtained and held under the RIPA s.8(4) bulk interception regime.

7 Fulford LJ, Generic Warrants Decision (5 April 2019), §3 [**B/4/97**].

17 It further follows that the SSHD and MI5 breached their duties of candour in relation to the Existing BPD/BCD Claim: either by failing to disclose the matters set out in the chronology in Appendix 1 hereto (and summarised in paragraphs 15–16 above) or by failing to disclose that MI5 was not in fact in a position to confirm whether it had properly given disclosure.

18 The disclosed documents[8] are as follows:

(1) A letter from MI5's Director of Policy, Compliance, Security and Information to the Investigatory Powers Commissioner's Office ("**IPCO**") dated 11 March 2019 (the "**MI5 11 March 2019 Letter**") [**B/1/69-73**];

(2) IPCO's *Inspection Report* issued 29 March 2019 (the "**First Inspection Report**") [**B/2/74-90**];

(3) A new Annex H — Section II to the MI5 Handbook for Judicial Commissioners issued 1 April 2019 ("**Annex H**") [**B/3/91-96**];

(4) The IPCr's "generic" decision on safeguards dated 5 April 2019 (the "**Generic Warrants Decision**") [**B/4/97-105**];

(5) A letter from Sir Andrew Parker, Director General of MI5, to the Home Secretary dated 24 April 2019 (the "**Parker 24 April 2019 Letter**") [**B/5/106-108**];

(6) A letter from the IPCr to Sir Andrew Parker dated 26 April 2019 [**B/6/109-110**];

(7) IPCO's "*Inspection Report: [Technology Environment] follow up inspection, 15–16 April 2019"* dated 26 April 2019 (the "**Second Inspection Report**") [**B/7/111-121**];

(8) A letter from "The Oversight and Errors Team" at MI5 to IPCO dated Friday 3 May 2019 [**B/8/122-125**];

(9) A letter from the IPCr to Sir Andrew Parker dated Wednesday 8 May 2019 (the "**IPCO 8 May 2019 Letter**") [**B/9/126-127**]; and

---

[8] The documents have been disclosed with redactions made for reasons of national security. The tracked changes represent further disclosure given in consequence of discussions between Special Advocates appointed to represent Liberty's interests and the Defendants. The colours of the tracked changes are not of any relevance.

(10) A letter from "The Oversight and Errors Team" at MI5 to IPCO of 15 May 2019 [**B/10/128-130**].

19 In the **Generic Warrants Decision** of 5 April 2019, which drew on the documents listed above prior to that date, Fulford LJ, the then IPCr, considered whether he would continue to grant MI5 warrants under the IPA, in light of the serious and systemic issues that had been discovered. He summarised the systemic failure at §10 [**B/4/99**]:

> "MI5 has inadequate control over where data is stored; [REDACTED]; and the deletion processes which applied to it."

Specific errors Fulford LJ identified include the absence of proper mechanisms for review, retention and destruction of retained data and an absence of effective safeguards relating to lawyer–client communications ("**LPP**" material): see at §§12, 19 [**B/4/99, 101**].

20 Fulford LJ referred at §10 [**B/4/99**] to "*the undoubted unlawful manner in which data has been held and handled*", and gave "*file shares*" and "*data stores*" (two ways in which MI5 processes material obtained under warrants) as examples of this. (The First Inspection Report further makes clear (§1.3 [**B/2/75**]) that the key risks are "*file shares*" and "*data stores*", that is, as the Claimants understand it, circumstances in and/or methods by which data is retained and shared without adequate controls.)

21 Other errors include "*Copying of Data*" and "*Access Controls*": see at §12 [**B/4/99-100**]. This appears to refer to non-compliance with safeguards that require MI5 to minimise the extent of copying of material obtained, the number of copies made, and the number of persons to whom and extent to which the material is disclosed or to whom access to the material is given, and to store such material securely.

22 Fulford LJ, on the basis of the material before him, made clear that these serious and systemic failings: (i) had existed unremedied after MI5 first identified them in 2016; and (ii) <u>still</u> persisted in relation to data obtained prior to the Generic Warrants Decision on 5 April 2019.

23 Further, when the significant issues described above and below were (eventually) disclosed to Fulford LJ, they were underplayed by MI5: at §9 [**B/4/99**].

24 Fulford LJ referred to the MI5 11 March 2019 Letter admitting that MI5 had identified the non-compliance in question "*as early as January 2016*": at §12 [**B/4/99**].

25 Fulford LJ held that warrants had been issued to MI5 on a basis that MI5 knew to be incorrect and, under the IPA, Judicial Commissioners[9] were given false information. He said at §3 [**B/4/97**]:

> "By January 2018 at the latest, the Management Board at MI5 had a clear view of serious problems with the manner warranted data is held in [the Technology Environment ("**TE**")]. These have been referred to as 'compliance risks' e.g. the effective Review, Retention and Destruction ('RRD') had not been implemented, with risks of non-compliance; [REDACTED]; and there was a real possibility that the destruction of material was not being implemented appropriately. I consider that these were understood to a level that MI5 should have considered the legality of continuing to store [REDACTED] operational data in [the TE]. Given the risks were evident by this stage, they ought to have been communicated to me — indeed, the recommendation in the paper before the Management Board in January 2018 was to 'update Whitehall stakeholders (particularly the Home Office), through the QR process' and yet there is no indication that this was contemplated by the Board."

Similarly, at §6 [**B/4/98**], Fulford LJ said:

> "It seems to me that to have provided assurances to the Secretary of State regarding safeguarding warranted data that, in hindsight, did not comply with MI5's obligations under the various safeguarding sections amounts to an error of notable gravity. As soon as MI5 became aware of this, it should have reported the matter and explained what it intended to do by way of rectification. <u>In short, MI5 did not have the option of seeking privately to devise a strategy before reporting the matter. Moreover, it is impossible sensibly to reconcile the explanation of the handling arrangements the Judicial Commissioners were given in briefings and the JC Handbook with what MI5 knew over a protracted period of time was happening.</u>" [emphasis added]

At §44 [**B/4/104**], Fulford LJ stated:

> "Albeit not strictly relevant to the present application, it is clear that for warranted material in [TE] there has been an unquantifiable but serious failure to handle warranted data in compliance with the IPA for a considerable period

---

9 Under IPA s 138 in Part 6 Chapter 1 (and cognate provisions), prior approval by Judicial Commissioners is required to issue a bulk interception warrant and other forms of bulk warrants, applying a judicial review standard to the Secretary of State's decision to issue the warrant.

> of time, and probably since IPCO first became operational. Assurances that have been made to the Secretary of State and the Judicial Commissioners of such compliance were, in hindsight, wrong and should never have been made. Warrants have been granted and judicially approved on an incomplete understanding of the true factual position. Indeed, I am concerned that on this important subject we were incompletely briefed during the Commissioners' induction programme, including that most recently provided to Lord Hughes and Sir Colman Treacy. To date, therefore, MI5's retention of the warranted material in [TE] cannot be shown to have been held lawfully and the failure to report these matters timeously to IPCO is a matter of grave concern which I will be addressing separately."

26 Fulford LJ further states at §4 [**B/4/97**] that an MI5 Executive Board paper in October 2018 "*set out many of these problems in greater detail*" and "*included a stark assessment of the compliance risks*", namely, that:

> "Effective RRD has not been implemented across all data stores in the [TE], potentially including warranted material … [this could] lead to successful IPT challenges, loss of confidence of ministers/JCs and consequently restrictions in warrants or reputational damage."

Fulford LJ observed at §46 [**B/4/104-105**] that, going forward, it would be necessary for inspectors to be afforded "*direct access to members of staff*" at MI5 and that it would not be acceptable for them to "*rely on hearsay accounts of internal conversations between members of MI5*". This seems to indicate that, hitherto, inspections and audits had been conducted <u>without</u> such access, but this had somehow been treated as sufficient.

27 At §49 [**B/4/105**], Fulford LJ concluded:

> "This is a serious and inherently fragile situation. …. <u>Without seeking to be emotive, I consider that MI5's use of warranted data in [TE] is currently, in effect, in 'special measures' and the historical lack of compliance with the law is of such gravity that IPCO will need to be satisfied to a greater degree than usual that it is 'fit for purpose'</u>. It is of importance to add by way of postscript that now this problem has been ventilated, MI5 appear to be using every endeavour to correct the failings of the past and to secure compliance. The organisation has cooperated in every way with the inspection we recently conducted and the questions that I posed." [emphasis added]

28 By way of summary only, the key points to emerge from the other documents mentioned above, summarised below in chronological order, are as follows.

29 The **Parker 24 April 2019 Letter** [**B/5/106-108**] contains a frank admission from Sir Andrew Parker to the then Home Secretary that MI5 failed to recognise the seriousness of its legal non-compliance (at §§3 and 5):[10]

> "I very much regret that we had not fully appreciated the significance of the issues in the [TE]. With the understanding we have now developed, off the back of much detailed work, I clearly wish MI5 had moved more quickly to bottom out some of the risks in play, and that we had brought our developing understanding to your attention and that of the Investigatory Powers Commissioner at an earlier stage. …
>
> … it is a bitter pill now to realise that in the case of the [TE], we have been slow to appreciate properly some of the risks manifesting within that complex environment."

30 The **MI5 11 March 2019 Letter** reveals that an MI5 compliance team identified in January 2016 that "*data might be being held in ungoverned spaces in contravention of our policies*" (emphasis added): §10 [**B/1/70**]. It says that the risk was reported to the Management Board and regularly reported on from early 2018. It "*became apparent that the task of examining the [TE] was too large* [for the legal compliance programme] *as it had to remain focussed on the urgent changes needed to be complaint with the Investigatory Powers Act*": §10 [**B/1/70**].

31 The existence of what MI5 itself calls "*ungoverned spaces*" in which it holds and uses large volumes of private data is a serious failure of governance and oversight, especially when mass collection of data of innocent people is concerned.

---

[10] The letter sought to argue at §6 [**B/5/107**] that the MI5 Board had not as at January 2018 understood "*the full extent and severity of the issues in [TE], and therefore had not appreciated their full significance from a legal compliance perspective*". In the IPCO 8 May 2019 Letter [**B/9/126-127**], Fulford LJ responded as follows: "*Separately, thank you for sending me a copy of your letter to the Home Secretary of 24 April, which, inter alia, sets out your position as to the extent to which Ml5's Board understood and responded to the compliance risks in [the TE] as corporate knowledge of these evolved. I would welcome a discussion with you and/or members of your staff before I decide whether to add any further detail on this question for the Home Secretary and ultimately the Prime Minister — focusing in particular on the information which was available to the Board in January 2018 and to four of Ml5's Directors in October 2017. There may be some additional remarks that I can properly make to set this in its proper context.*" No further documents or information have been disclosed in the IPA Challenge to suggest that Fulford LJ's findings of MI5's awareness of the situation by very senior officers as at October 2017 or January 2018 was in any way qualified or, indeed, that the findings in the Compliance Improvement Review of MI5 Board level knowledge of the risk of non-compliance as at May 2013 (see paragraph 50(1)–(2) below) are other than entirely correct.

32 Fulford LJ became aware of MI5's non-compliance only in very late February 2019,[11] and only because MI5 itself disclosed this to him. Even then, as he explains, the non-compliance was made intelligible only when a written briefing was provided on 11 March 2019.[12] His inspectors did not identify the problem during their audits of MI5's systems. An inspection was ordered: Generic Warrants Decision §12 [**B/4/99**].

33 That inspection led to the **First Inspection Report**. It finds in §3F [**B/2/76**] that, "*by January 2018 if not earlier, MI5 had a clear view of some of the compliance risks around [the TE], to the extent that they should have carefully considered the legality of continuing to store and exploit operational data in [the TE]. The risks were also sufficiently clear that they should have been communicated to the IPC.*"

34 In the First Inspection Report at §4.2.6 [**B/2/78**], a "Red Amber Green" rating is included in respect of "[Data Type 1]", as follows:

4.2.6 [*REDACTED*]

[THE REDACTIONS IN COLUMN 1 OF THE TABLE BELOW INCLUDE LPP, COPYING OF DATA AND ACCESS CONTROLS, BUT NOT NECESSARILY IN THAT ORDER]

IPA safeguard	RAG rating	Rationale
[*REDACTED*]	GREEN	[*REDACTED*]
[*REDACTED*]	AMBER	[*REDACTED*]
Review, retention, and deletion (RRD)	RED	[*REDACTED*]
[*REDACTED*]	AMBER	[*REDACTED*]
[*REDACTED*]	RED	[*REDACTED*]

It is therefore apparent that there is a "*RED*" rating against an "*IPA safeguard*" (which may be "*LLP*", "*copying of data*" or "*access controls*" — the public are apparently not permitted to know which of these fundamental requirements of the IPA have been breached), in addition to the "*RED*" RRD (review, retention and deletion) rating. There are also amber ratings for another two areas. At §4.1.6 [**B/2/77**], the Report explains that a red rating indicates "*serious compliance gaps*" and amber indicates "*some compliance*

[11] The MI5 11 March 2019 Letter summarises a briefing to Fulford LJ on 27 February 2019: see Generic Warrants Decision §7 [**B/4/98-99**].

[12] Generic Warrants Decision §§9, 11 [**B/4/99**].

gaps". Thus the First Inspection Report identified that, in relation to one datatype, MI5 is not complying with four out of five IPA safeguards.

35 The First Inspection Report contains five further such tables, apparently relating to different "[Data Types]" (or means of obtaining or holding data) [**B/2/78-83**]. Liberty and PI infer from the report that each of these tables refers to a different technique, such as bulk personal datasets, bulk interception material, and so forth. Across those five tables, there are a further 10 "*RED*" ratings and 4 "*AMBER*" ratings.

36 The First Inspection Report also contains, in Chapter 7, a summary of the development of MI5's knowledge of the serious failures to comply with statutory safeguards now revealed:

(1) In January 2016, a senior lawyer in MI5 identified the problems (see §7.1.2 [**B/2/85**]): "*Allowing uncharted material to remain* [in the TE] *presents considerable legal risk ... We may fall foul of our duty under the SSA* [Security Service Act 1989] *to only hold material for as long as is necessary for our statutory functions – but auditing* [the TE] *manually has proven extremely resource intensive, and the work is not complete.*" As explained at §§7.1.3–7.1.4, as a mitigation, the paper recommended that MI5 should "*ask staff to claim that material they require for current use and then delete everything else without resorting to further audit*". Due to "*the complex way in which data was used*" within "*TE*", however, "*this recommendation was not capable of being implemented*". (The Claimants note the clear parallel to the breach found to exist by the ECtHR in *Catt v United Kingdom* (App No 43514/15, 24 January 2019, First Section).[13])

(2) In October 2016, MI5 concluded there was "*a high likelihood of relevant material not being discovered, or being discovered when it should have been deleted, in a disclosure exercise leading to substantial legal or oversight failure*" (§7.1.5 [**B/2/85**]). This issue had "*first been identified as being relevant to disclosure exercises in 2014*" and there had been concern that insufficient progress had been made to reduce the risk (§7.1.6 [**B/2/85**]).

---

[13] See, in that connection, *Catt v United Kingdom* (App No 43514/15, 24 January 2019, First Section) [127]: "*In general terms the Court would add that it would be entirely contrary to the need to protect private life under Article 8 if the Government could create a database in such a manner that the data in it could not be easily reviewed or edited, and then use this development as a justification to refuse to remove information from that database.*"

(3) The October 2016 paper, produced for Directors of MI5 and others, concluded (§7.1.8 [**B/2/86**]): "*There is significant risk around the absence of compliance with relevant legislation, Codes of Practice and Handling Arrangements.*"

(4) In October 2017, MI5 knew that it might not make proper disclosure in legal proceedings due to the TE. As an update paper produced for four Directors of MI5 in October 2017 put it: "*The main legal risk here remains one of disclosure in that we may not find relevant material which is held [REDACTED] on [the TE].*" Yet, the same update paper stated: "*we continue to build some* [systems] *without*" the capability to review, retain and destroy data properly (§§7.1.11–7.1.12 [**B/2/86**]). It is thus apparent that MI5 continued not only to use, but to build, systems that MI5 knew did not comply with statutory and other legal requirements, and further that this was known at Director level. MI5 knew that it was breaking the law, but decided to proceed anyway, in secret. Such deliberate unlawful conduct by a public body, conducted in secret, raises the most serious questions of propriety, culture and governance.

(5) The October 2017 paper concluded (§7.1.14 [**B/2/86**]): "*we need a new plan that prioritises hard on the top compliance risks and sets out a realistic target state. This plan needs to focus in on the management and use of warranted data (or [some] forms of it if this is still too big a problem) as its first step.*" Notwithstanding this recognition at senior levels, there is no suggestion that any recommendation for any disclosure or reporting, within MI5 or externally to oversight bodies or the IPT, was made.

(6) By January 2018, based on a paper on compliance risk to MI5's Management Board of that date, the First Inspection Report concluded that, by this time, MI5 had "*a clear view of some of the compliance risks around [the TE], to the extent that they should have carefully considered the legality of continuing to store and exploit operational data in [the TE]*", and that these risks "*were also sufficiently clear that they could have been communicated to the IPC*", but MI5's Management Board did not take this step and, apparently, did not contemplate doing so (§7.1.16 [**B/2/87**]). The January 2018 Board Paper (as extracted in the First Inspection Report) is striking: it lists in terms (insofar as not redacted) the ongoing breaches of the statutory requirements in relation to data obtained under warrants, relating to "*RRD*" and "*LPP*" — one further error is redacted in its entirety (the basis for which is not readily comprehensible): §7.1.15 [**B/2/86-87**].

(7) Even in October 2018, MI5 failed promptly to report to the IPCr, the IPT[14] or the Intelligence and Security Committee ("**ISC"**) what it had recognised internally to be serious breaches of the legislative regime (§§7.1.20 – 7.1.22 [**B/2/87-88**]). Notwithstanding recognition at Board level of widespread non-compliance with statutory requirements, no report was made for over four months, until an oral briefing of Fulford LJ on 27 February 2019, made comprehensible on 11 March 2019 (see paragraph 32 above). It appears that MI5 continued to apply for warrants, which continued to be granted in ignorance of MI5's systemic non-compliance with RIPA and the IPA.

37 This summary in Chapter 7 is said to be "*illustrative, as we have not reviewed all of the relevant paperwork*": §7.1.1 [**B/2/85**]. It is therefore possible that any enquiries and disclosure directed by the Tribunal might unearth significant further material that bears on the institutional knowledge of MI5 of these defects.

38 Chapter 8, a brief conclusion, notes in §8.2 [**B/2/88**] that "*Ml5 will be producing forms of words to summarise the compliance risks of [the TE] and proposed mitigations, which will inform decisions as to whether to approve these warrants*". No such material was disclosed in the IPA Challenge, but the Tribunal may well find it helpful to understand how MI5 described the errors, particularly in the context of warrant applications.

39 The Claimants note that it was around the same time that the IPCr published Notice 1/2018, which emphasises that warrant applications attract a duty of full and frank disclosure.

40 On 1 April 2019, MI5 issued **Annex H** (an attachment to the Handbook for Judicial Commissioners) [**B/3/91-96**], which set out the "*mitigations*" MI5 had implemented and explained on what basis MI5 considered that warrants could lawfully be issued to it. Annex H stated at §§49–53 [**B/3/95**] that the First Inspection Report had rated compliance with LLP safeguards as an "*AMBER*" risk in relation to some data. It recorded that:

---

[14] In any case before the IPT in which disclosure of these defects was not made (which appears to be all such cases, at least as to 29 March 2019), the IPT will have made its decision on an erroneous basis, not least because the relevant warrants or authorisations will not have been lawful under domestic law or compliant with the Convention. MI5 will in such cases also have breached its duty of candour. See, in particular, the discussion in Sections D and H below relating to the Existing BPD/BCD Claim.

(1) There was a risk that "*while there is a manual system in place for deleting LPP material if required to do so, given the compliance gaps in relation to RRD there can be very little assurance that [REDACTED] any conditions imposed by a Judicial Commissioner on the use or retention of such material have been complied with*" (Annex H §50);

(2) There were two further "*compliance risk*[s]" that relate to requirements to mark LLP material (once it has been identified as privileged): some systems within the "*TE*" did not allow LLP material to be flagged at all and, additionally, where a "*file share*" was used it was "*possible*" that flags would not be carried over — MI5 did not know whether or not this was the case and "*are working to establish the extent of this risk and the extent to which it can be addressed through specific guidance and the new naming convention for file shares*" (Annex H §§52–53).

It accordingly appeared to be the position, as at April 2019, that MI5 had only manual processes for deleting LPP information, some systems could not flag it, and MI5 did not know whether flags were carried across where "*file shares*" were used. No further disclosure in relation to this issue was given in the IPA Challenge. Full disclosure should be given in this challenge.

41 There was then a **Second Inspection Report** [**B/7/111-121**] of 26 April 2019. This states that there are two "*RED*" recommendations ("*critical recommendation: affects compliance status if not addressed*") and a further three "*AMBER*" recommendations ("*core recommendation: improvements must be made*") (see the table at §3.1.1 [**B/7/113-115**]), the majority of which remain entirely secret. Again, no further disclosure was given in the IPA Challenge.

42 The **MI5 3 May 2019 Letter** [**B/8/122-125**] sets out preliminary error reports by MI5:

(1) Page 2 states [**B/8/123**] that, in addition to the areas identified, MI5 is "*in the earlier stages of understanding issues associated with [other areas], but we anticipate there will be cases where material has been handled in error for one or more of the reasons above.*" Nothing of the issues relating to "*[other areas]*" has been disclosed.

(2) Page 2 also refers to "*selection for examination*", a statutory process applying only to bulk powers, which indicates that the defects extend to bulk data.

(3) Page 2 in §4 indicates that MI5 continued (as at May 2019) to investigate "*potential issues related to [two areas of another technology environment: TE2]*". The Letter suggests MI5 has little idea of what data it holds and, even today, cannot access or audit it. Thus on page 3 [**B/8/124**] the Letter says of "*TE2 Area 1*" and "*TE2 Area 2*":

> "Our initial scans of [Area 1] have been completed and we have identified files which may contain warranted material. [It is a complex area and is challenging to investigate. We have therefore only been able to scan some of the files and are working towards scanning other files. We may also need to use dip sampling in some areas]".

In short, MI5 is still unable to document the current and historic state of its bulk data holdings and how those holdings have been or will be processed. In such circumstances, there has not been and cannot be a Convention-compliant system of retention, use and destruction by MI5. RIPA and Codes of Practice, and the subsequent IPA regime, have proven inadequate to ensure compliance with the basic statutory requirements for proper handling of private information obtained by MI5.

43 The **IPCO 8 May 2019 Letter** [**B/9/126-127**] shows Fulford LJ's concern about further errors that had emerged towards the end of April or in early May 2019:

> "Unsurprisingly, I am concerned that these two potential errors, which seemingly indicate a similar set of underlying problems in [TE2] to those which we have been considering in [the TE], have surfaced in this way, on two counts.
>
> First, it appears that MI5 has been aware of a 'compliance risk' in [Area 1] and [Area 2] since 2016. I am concerned, therefore, that this information was not included in either the original briefing concerning [the TE] on 27 February 2019 or the full prose description setting out the nature of the problem dated 11 March 2019. I need an immediate briefing on this issue, supported by a prose description of the problem that is similar in layout to the one we helpfully received on 11 March 2019. …
>
> Second, to the extent that [Area 1] or [Area 2] contain warranted data, it would be helpful to understand whether MI5's use of either area is in breach of the IPA's safeguards. From the limited information so far provided it seems highly likely that this is the case, but I would welcome the earliest information on this point from MI5's perspective. If that assumption is correct, this raises the question as to whether MI5 has the capability to handle warranted data in an IPA-compliant fashion." [emphasis added]

44 **The MI5 15 May 2019 Letter** [**B/10/128-130**] responds to Fulford LJ. It discloses that MI5 did not know what data is held on "*TE2*" nor the associated "*working practices*" under which the data is held and processed, saying at §5 [**B/10/128**]:

> "We completed an initial scan of approximately [REDACTED]% of [Area 1] in April 2019. We are about to commence further scanning of [Area 1] to ensure we have a full understanding of the data. The full scan has been challenging to action [REDACTED]. We have also been seeking to understand working practices within [Area 1] so that we can take comprehensive action to improve assurance of our compliance with relevant safeguards. This will include issuing new guidance to users [REDACTED]."

If those within MI5 responsible for compliance — let alone the Commissioner / IPCO or the IPT — do not know the relevant working practices or what data is stored, there cannot have been proper oversight or an effective system of control.

45 So far as the Claimants are aware, there has never been any disclosure in any IPT claim of this material or information. In particular, this information was not disclosed in the Existing BPD/BCD Claim.

46 Liberty and PI understand that at no point was any disclosure made[15] by an employee or officer of MI5 pursuant to the "whistle-blowing" provision in IPA s 235(6).[16] The ultimate mechanism to ensure that the IPCr was aware of unlawful conduct failed to operate. Further, MI5 committed a serious breach of the Code of Practice by failing to report the conduct to the IPCr promptly:

(1) All "*Relevant error[s]*" must be disclosed by MI5, MI6 and GCHQ to the IPCr (IPA s 231(9)). An element of that definition is that an error is of a kind defined in a Code of Practice.

---

15 Liberty and PI do not know whether any staff member of MI5 or in the Home Department considered making such a disclosure and was prevented or discouraged from doing so. This may be an area on which the Tribunal considers it appropriate to order disclosure.

16 Remarkably, the reason advanced for this in submissions in the IPA Challenge was that it is necessary to report and deal with such matters in line with reporting structures within the SIAs. The purpose of s 235 is to enable precisely the opposite to occur.

(2) The current Interception of Communications Code of Practice[17] sets a timescale for, and the circumstances in which, reporting is required in §10.17. That period is 10 working days. The errors were not disclosed within that period.

(3) The previous Interception Codes of Practice under RIPA of 2010 and 2016 also required any person aware of a breach of safeguards to report this to the Interception of Communications Commissioner (the IPCr's predecessor).[18]

(4) MI5 was aware of the errors at a senior level for a number of years before the errors were disclosed in late February/March 2019.

(5) The current Code of Practice emphasises that MI5, MI6 and GCHQ should not sit on problems — as soon as it is established that there is a problem it should be reported, even if there is no solution to report.[19]

47 The Claimants have not been informed as to whether any person has been disciplined or investigated in relation to the existence and subsistence of, and concealment of and failure to disclose in litigation, such breaches, and MI5 is requested to confirm the position. The absence of such a step, and the concomitant indication that such conduct is not treated as a form of breach or misconduct, would be a further indictment of systemic failures within MI5.

(2) The findings of the Compliance Improvement Review

48 After the conclusion of the hearing in the IPA Challenge, the Defendants in that claim disclosed on 15 July 2019, and published online,[20] the "**Compliance Improvement**

---

17 Home Office, Interception of Communications Code of Practice (March 2018) §10.17: "*When a relevant error has occurred, the public authority that made the error must notify the Investigatory Powers Commissioner as soon as reasonably practicable, and no later than ten working days after it has been established by appropriate internal governance processes that a relevant error has occurred. … Where the full facts of the error cannot be ascertained within that time, an initial notification must be sent with an estimated timescale for the error being reported in full and an explanation of the steps being undertaken to establish the full facts of the error.*"

18 Home Office, Interception of Communications Code of Practice (2010) §§6.1; Home Office, Interception of Communications Code of Practice (March 2016) §§7.1, 7.18, 10.3.

19 See footnote 17 above.

20 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/816768/20190709_CIR_summary_for_publication.pdf

Review Summary", which is a summary of the independent review[21] into MI5's serious, systemic and longstanding failure to observe statutory safeguards on access control, copying, review/retention/destruction and lawyer–client communications for information obtained under warrants. This summary included strongly worded criticisms of MI5.

49 The Defendants to the IPA Challenge eventually (on 15 August 2019) provided the full report of the Compliance Improvement Review (i.e. the full document and supporting material from which the summary was extracted) to the Special Advocates who had been appointed in the IPA Challenge with a view to an appropriately redacted version being provided to Liberty. The Special Advocates provided comments to the Defendants to that claim on 3 October 2019. A redacted version of that full report has not yet been disclosed to Liberty.[22] It is therefore not admitted that the summary report is a fair reflection of the full report nor that it would not be possible to disclose more. The Tribunal in the present claim should be provided with the full report immediately, and a redacted version should also be disclosed in OPEN promptly.

50 Nevertheless, the Compliance Improvement Review Summary makes the following clear:

(1) **Defects existed for even longer than previously suggested:** Compliance risks were first identified in 2010, recommendations made in 2011, and in May 2013 the MI5 Board discussed "*a paper setting out serious information management risks …, which clearly had implications for legal compliance*" (§§3–5 [**B/13/273**]). The IPCO Inspection Reports did not mention this, and no explanation for the omission in those reports was provided. It therefore seems to be the case that, even from February 2019, MI5 has not been candid about its unlawful conduct.

(2) **There is an ingrained institutional culture of accepting and permitting unlawful conduct in MI5:** Compliance with the IPA and previous legislation "*never became a mission-critical priority for the senior leadership, nor therefore for MI5 staff; and consequently was not properly resourced*" (§8 [**B/13/274**]). MI5 had a "*lack of*

---

21 By Sir Martin Donnelly, a former Permanent Secretary: see the Home Secretary's written statement made on 15 July 2019 to the House of Commons at <https://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Commons/2019-07-15/HCWS1722/>.

22 The long delay before this occurred has not been properly explained. It is understood that the Special Advocates sent back comments and proposed alterations on 3 October 2019; on 25 November 2019, Liberty was informed that the relevant person dealing with redactions for the Government had been absent.

urgency in reducing the legal risks" and systems lacking essential safeguards were expanding (§11 [**B/13/274**]). There was "*a sustained organisational failure to appreciate the extent of the compliance problem and its consequences*" (p 3 [**B/13/275**]).

(3) **MI5 failed to inform the Commissioners and Home Office of its systemic non-compliance and unlawful conduct:** Despite Management Board awareness from May 2013, MI5 failed to inform the Secretary of State and Home Office, and the Commissioners, of its systemic inability to comply with statutory requirements (§13 [**B/13/274**]). It instead sought and obtained warrants, knowing that it was unable or unwilling to comply with the requirements for holding data obtained under such warrants. The only point the reviewer makes in MI5's favour is that MI5 did not "*attempt … to hide information*" (§12 [**B/13/274**]). But he qualifies this, stating that "*the information shared was insufficient to highlight the increasingly urgent problems caused by continuing compliance difficulties*". In the context of secret state surveillance, where effective oversight depends not just on the accuracy of information MI5 (carefully) chooses to give the Secretary of State and Commissioner, but on that information being complete and thus not creating a misleading impression, it is difficult to understand the conclusion that information was not in substance "hidden".

(4) **There was no prospect of MI5's compliance in the near future:** A striking recommendation (p 9 [**B/13/281**]) is that "*MI5 must ensure that all its data can be shown to be held in accordance with legal compliance requirements by June 2020.*" The reviewer considered that the issues (it is inferred with TE or TE2) had not been resolved: p 3 [**B/13/275**]. No explanation for the June 2020 deadline was given. It appeared to be aspirational (the reviewer says that it is "*ambitious*"), not based on an understanding of the detail of changes required to MI5's systems. (p 6 [**B/13/278**]). The Claimants do not know whether (notwithstanding the matters described at paragraph 52 below) that ambitious deadline is likely to be met, or what issues remain outstanding at present. MI5 is requested to confirm the position.

(5) **Fundamental change was required to comply:** Recommendations 1–14 seek the creation of a "*compliance culture*" in MI5 (p 5 [**B/13/277**]). This requires a

fundamental "*step change*" (p 9 [**B/13/281**]) to comply with the IPA. Recommendations include:

(a) staff and contractors are given "*urgent … training on MI5's statutory obligations in respect of handling warranted data*" (Recommendation 1, p 5 [**B/13/277**]);

(b) "[r]*esources for MI5's compliance function need to be increased substantially*", and lawyers are deployed within MI5 to ensure compliance (Recommendation 4, p 6 [**B/13/278**]);

(c) the area in the Home Office overseeing MI5 should "*take a more proactive approach to their oversight role*", *inter alia* to ensure that its own staff have the technical expertise to engage with MI5 on compliance risks (Recommendation 9, p 7 [**B/13/279**]); and

(d) MI5's Legal Director becomes a full Management Board member, "*to provide an authoritative legal voice on all governance issues in Board discussions*" and to provide a quarterly statutory compliance report (with the Home Office Chief Legal Adviser) to the Permanent Secretary and Director General (Recommendations 10–11, p 7 [**B/13/279**]).

51 The findings and recommendations in the Compliance Improvement Review Summary show that the safeguards under the IPA — which as MI5 rightly thought "*did not substantively change the existing legal provisions with regard to warranted data handling*" (§7 [**B/13/273-274**]) — failed to ensure in practice in many cases that data was held consistently with Articles 8 and 10 ECHR. The oversight mechanisms under the IPA (the ISC, the IPT and the Commissioner) failed to detect <u>any</u> of these issues or the need for a battery of recommendations amounting to fundamental cultural, systems and attitudinal change in MI5, from the top down, with a view to achieving <u>legal</u> compliance by (it was then thought) June 2020.

(3) Subsequent developments

52 On 21 October 2019, Sir Brian Leveson was appointed as the IPCr. On 22 October 2019, the IPCr announced that IPCO had concluded a series of targeted inspections of MI5, over

a six-month period, and concluded that "*MI5's use of the IT system in question is now fit for purpose*" [**B/16/294**].[23]

53 Once more, the Claimants invite the Tribunal to request the documents evidencing the inspections that led to this announcement. They are likely to assist the Tribunal insofar as they may show: (i) the systems that MI5 ought at all times to have had in place; and (ii) how such systems could be implemented. As has occurred previously, it is also possible that, on a forensic examination, and in light of any further disclosure or enquiries it directs MI5 to carry out, the Tribunal may take a different view of the extent to which the previous, systemic and long-standing failings have been remedied or the robustness of any fixes. One of the important functions of the Tribunal is to examine whether the oversight provided by the IPCr has in fact been effective.

C THE DIVISIONAL COURT'S DECISION AND ITS RELEVANCE TO THIS CLAIM

54 The Divisional Court rejected Liberty's challenge to the IPA: [2019] EWHC 2057 (Admin).[24] The question of an appeal has been stayed pending judgment of the Grand Chamber of the ECtHR in the *Big Brother Watch* case (App Nos 58170/13, 62322/14 and 24960/15) and the preliminary reference to the CJEU in Case C-623/17 *Privacy International*, the reference made in the Existing BPD/BCD Claim.[25]

55 Before the Divisional Court, Liberty had relied on the disclosure summarised above to submit that, contrary to the requirements in ECtHR jurisprudence,[26] the safeguards in question were not adequate and effective in practice, but instead were illusory and theoretical, such that the scheme of safeguards in the IPA and associated codes of practice was not "in accordance with the law".

---

23 IPCO, "Compliance inspections of MI5 complete" (22 October 2019) available at <https://www.ipco.org.uk/Default.aspx?mid=4.32>.

24 In light of the pending decision of the Grand Chamber of the ECtHR, the Divisional Court extended the time for appeal until events including the handing down of that judgment. Accordingly, Liberty should not be taken, by any reference in this pleading to the Divisional Court, to accept for the purposes of any appeal the correctness of any finding of the Divisional Court.

25 See the Tribunal's decision to make the reference: *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* [2017] UKIPTrib IPT_15_110_CH (8 September 2017) and its Order for Reference dated 18 October 2017. The Advocate-General delivered his opinion in Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* ECLI:EU:C:2020:5 on 15 January 2020, as to which see footnote 38 below.

26 See in particular the summary at [378] and [380].

56 The Divisional Court:

(1) summarised the evidence referred to above and acknowledged the seriousness and concerning nature of MI5's systemic failings (at [361]–[372]); but

(2) ultimately considered that those failings did not demonstrate that the system created by the IPA, as a whole, was not effective in practice and thus not in accordance with the law (at [378]–[392]).

57 At [387] the Divisional Court adverted to possible proceedings before the IPT in which the lawfulness of instances of conduct relating to the failings that were the subject of disclosure in the IPA Challenge could be considered. It is that claim that the Claimants now bring. The Divisional Court emphasised: "*Nothing we say in this judgment should be taken to anticipate in any way what might be said in any such future litigation.*"

58 The Divisional Court made a further finding of present relevance. The Defendants to the IPA Challenge adduced a Witness Statement of MI5 Witness dated 4 February 2019, made by a "*Deputy Director in the Security Service*" who in §1 stated that:

> "I manage the Information and Legal Compliance teams at Ml5. Prior to my current role, I was acting Director for Policy, Compliance and Information and before that I was Programme Director for an IT and Business Change programme to implement new legislation. Prior to taking up that role, I was the Ml5 Deputy Legal Adviser. In total, I have been employed by Ml5 for 25 years. This is the first witness statement that I have made in these proceedings. I have previously given a witness statement to the Hay Barn Inquiry in 2018 and I have also given a witness statement in the case of Privacy International –v- Secretary of State for Foreign and Commonwealth Affairs and Others [2018] UKIPTrib IPT-15-110-CH. My witness statement in the latter proceedings was dated 8 October 2018."

Having outlined the various Handling Arrangements that MI5 had used under RIPA, that witness went on to state at §§14–15:

> "It can be seen from the documents in Ml5 1 and those exhibited to the witness statements of the SIS and GCHQ witnesses [which had provided those organisations' Handling Arrangements] that the intelligence services have each taken a different approach to the production of written arrangements under the Act. As separate legal entities, and as agencies with different statutory functions which are given effect by different internal operating models, the intelligence

services each produced their own written arrangements to reflect their own ways of working and to ensure compliance with the requirements of the Act.

… I am satisfied that MI5's Handling Arrangements, taken together with the range of internal handling arrangements and policies referred to therein and the information provided in each warrant application, comply with the requirements of the Act." [emphasis added]

59 This Witness Statement was given before the disclosure by MI5 to the IPCr at the very end of February 2019 had taken place. At the 11 June 2019 directions hearing in the IPA Challenge, Liberty by its counsel gave notice that it considered that, in the absence of any evidence to explain how this statement came to be made, the Claimants were minded to criticise the candour of this statement.[27] No further statement was adduced.

60 The Divisional Court referred to this evidence as follows at [371]–[372] of its Judgment:

"Before leaving the documentation we should note what was said in a witness statement filed in these proceedings before this Court on 4 February 2019 by a witness on behalf of MI5, whose identity for understandable reasons has not been disclosed. That witness is a Deputy Director at MI5. The witness manages information and legal compliance teams at MI5 and previously was the MI5 Deputy Legal Advisor. At para 15 the witness informed the Court that:

> "… I am satisfied that MI5's Handling Arrangements, taken together with the range of internal handling arrangements and policies referred to therein and the information provided in each warrant application, comply with the requirements of the Act. …"

Clearly, in the light of the documents that have subsequently been disclosed, that statement has turned out to be wrong, although it is not clear to this Court that it was inaccurate to the knowledge of the witness at the time that it was made. It is to the credit of those acting for the Defendants that they have complied with their duty of candour and co-operation with the Court since that time but it is (to say the least) unfortunate that such disclosure was not made at the time when evidence was filed in these proceedings just a few weeks before the briefing given to the IPC. We do not know the full circumstances and so we say no more about it here."

---

[27] Liberty in this regard drew a contrast between the apparently careful language used by the MI5 Witness, set out above, and that of in the Witness Statement of SIS Witness dated 4 February 2019, who had simply said at §8: "*I am satisfied that SIS's Handling Arrangements fully comply with the requirements of the Act.*"

61 Liberty and PI submit that the circumstances in which a very senior officer of MI5 came to make this statement, and the knowledge of the individual in question, ought to be the subject of investigation in these proceedings. It may, for example, be material to any findings the Tribunal must make about MI5's past conduct that a person in the senior position of the MI5 Witness in the IPA Challenge would knowingly make such a statement or would do so without a proper basis for it, including undertaking all relevant investigation so as to ensure the statement was complete, not misleading, and candid.

D THE EXISTING BPD/BCD CLAIM

62 These developments in the IPA Challenge must be seen alongside the stance of MI5 and the evidence and disclosure it gave in the Existing BPD/BCD Claims. At the heart of those claims were two key issues:

(1) The legality of orders made at the instigation of and for the benefit of MI5 (amongst other agencies) under section 94 TA to require telecommunications providers to provide certain bulk telecommunications data to MI5; and

(2) The legality of MI5 policies, practices and procedures for handling bulk personal datasets, including but not limited to bulk communications data.

63 Appendix 1 contains a chronology that demonstrates how MI5's awareness of the issue of non-compliance, as now revealed by the Initial MI5 Disclosure and the Compliance Improvement Review, sits chronologically with its evidence to the IPT in the Existing BPD/BCD Claim. That evidence is summarised in brief outline below. This comparison reveals a substantial failure in MI5's duty of candour, leading to both PI and the Tribunal being misled, and leading the Tribunal to reach findings on an incomplete and materially inaccurate understanding of the situation.

64 As far as Liberty and PI can see from the redacted version of the Respondents' CLOSED letter to the Tribunal of 7 June 2019, there has been no attempt to provide a reasoned explanation of why these matters were not disclosed. The Respondents simply assert that the ECHR phase of the proceedings had closed and that no disclosure exercise will be perfect. That cursory and self-serving explanation fails to grapple with the systemic and serious nature of the defects explained above and the knowledge of MI5, including at Board Level, as found by Fulford LJ in the Generic Warrants Decision and further revealed

in the Second Inspection Report. How the Respondents were able to reach the conclusion in their 11 June 2019 letter to PI that nothing disclosed in the IPA Challenge fell to be disclosed in the Existing BPD/BCD Claim is also not explained. Nor is it apparent how that conclusion could credibly be reached.

65 References in this section to the "Respondents" are to the Respondents to the Existing BPD/BCD Claim, as will be apparent from context. In all instances this includes the SSHD and MI5.

(1) MI5's evidence to the Tribunal

66 In the Respondents' Amended Open Response (19 February 2016), the Respondents (including the SSHD and MI5) relied in particular on the existence of Handling Arrangements in relation to BPD for the purposes of compliance with Article 8 ECHR. For example, §175 provided: "*if some version of the list of 'safeguards' in eg §95 of Weber applies to the BPD Regime, the present regime satisfies the requirements for such 'safeguards', insofar as it is feasible to do so*" (and see §185 in respect of BCD). The Respondents also relied upon the oversight mechanisms, including the Intelligence Services Commissioner (eg at §§177, 187).

67 The Respondents pleaded various assertions as to the compliance, in fact, with the safeguards set out in the BPD Handling Arrangements. For example, in the context of "*Review of Retention and Deletion*" (§82), they stated:

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

68 In the OPEN version of the Respondents' (initially CLOSED) response to the Claimant's request for further information and disclosure of 15 January 2016 (the OPEN version itself dated 30 March 2016), MI5 was specifically asked to state the number of instances of non-compliance that have been detected with the Handling Arrangements. The Respondents reported six instances of non-compliance with the BPD Handling Arrangements, and 47 instances of non-compliance in relation to BCD Handling Arrangements, in respect of the

period 1 June 2014 to 9 February 2016. No reference was made to either of the "Technology Environments".

69 Further, in the OPEN version of the Respondents' (initially CLOSED) pleaded Response (11 April 2016), the Respondents, including the SSHD and MI5, relied upon the existence of the BPD Closed Handling Arrangements[28] and the steps set out therein. For example, at §§76–81, they said:

> "The retention and use of BPD in MI5's possession is reviewed by MI5's Bulk Personal Data Review ("BPDR") Panel (§7.1.3). …
>
> In addition to satisfying themselves that the level of intrusion is justifiable under Article 8(2) of the ECHR, the BPDR panel must also be satisfied that it complies with the requirements of the Data Protection Act 1998 (§7.1.2). If at any time, including on a review, it is judged that MI5's retention of BPD is no longer necessary and proportionate 'all copies must be deleted or destroyed.' (§7.1.2).
>
> …
>
> The BPDR panel considers recommendations for each dataset under review and decides whether to retain or delete it (§7.1.5). …
>
> When a dataset is retained, it is given a retention review period of six to 24 months 'in accordance with the level of intrusion and risk posed by the retention and use of the dataset' (§7.1.5). …
>
> When a decision has been reached to delete BPD, its destruction is tasked to technical teams responsible for retention and deletion. Confirmation of complete deletion must be recorded with the data governance team and an update provided to the next BPDR panel meeting. Information specialists provide technical reassurance surrounding the deletion and destruction of the dataset (§7.2.1)."

70 MI5 also relied upon the oversight provided by the Intelligence Services Commissioner, and drew attention (at §85) to the obligation at §8.3.4 of MI5's Closed BPD Handling Arrangements:

> "The Service must provide to the appropriate Commissioner all relevant documents and information such that he can exercise the oversight described above. …"

---

[28] As a result of the claim, these were disclosed in part. References to "Closed Handling Arrangements" in this section are therefore to Handling Arrangements that have been disclosed or gisted.

71 The Respondents, including the SSHD and MI5, further stated to the Tribunal (at §219) that:

> "In particular there are detailed internal arrangements which provide comprehensive safeguards in terms of the authorisation for BPD activities and the use, storage of, access to, retention, and disclosure of any material obtained as a result of such activities."

72 Similar submissions were made by the Respondents, including the SSHD and MI5, in relation to MI5's treatment of BCD. They said, for example, that BCD's retention and deletion must be reviewed every six months (§252) and that, "*where a decision is taken to delete data, MI5 must task the technical teams responsible for Retention and Deletion with a view to ensuring that any retained data is destroyed*" (§258). The Respondents asserted that "[i]*n particular there are detailed internal arrangements which provide comprehensive safeguards in terms of the authorisation for Section 94 activities and the use, storage of, access to, retention and disclosure of any material obtained as a result of such activities*" (§311).

73 In the Respondents' Amended Open Response to the Claimants' Supplemental Request for Further Information and Disclosure dated 10 June 2016 (itself dated 14 July 2016), the Respondents responded to specific questions about instances of non-compliance with the Handling Arrangements and about Commissioner oversight (pp 24–27). No reference was made to breaches in respect of any "Technology Environment".

74 The Amended Witness Statement of the MI5 Witness dated 8 July 2016 explained that the witness is a "*Deputy Director in the Security Service since 2010 and a member of the senior management group since 2004*" (§1). The witness stated (§§42–43):

> "In view of: the increasing use and value of BPD within MI5; recognising BPD as a category of data in its right; and, in particular, because we proposed that some of our BPD would be made more generally available to investigators, we concluded that we ought to formalise the policy process by which datasets of this type were acquired and held, and reviewed, by MI5. I refer further below (under 'Safeguards') to the regime we instituted in 2006 in order to achieve this. …".

75 At §59, in discussing those "safeguards" introduced from 2006, the witness states:

> "The review process was another key way to ensure that we were only retaining BPD where there was a genuine need to do so. In particular, over the period from 2006 onwards, at every 6 monthly review of BPD, each of the BPDs then held by MI5 was reviewed."

76 The witness described the cross-SIA BPD policy and Handling Arrangements from February/November 2015 at §§79 ff. The witness further stated (§81): "*I confirm that these internal MI5 Handling Arrangements set out and describe our current practice and procedure in relation to the acquisition, use, retention, review, deletion and oversight of BPD*" (emphasis added).

77 In respect of retention and review, the witness informed the Tribunal (§84):

> "All new acquisitions will be subject to an initial review by the BPD Review Panel at the first meeting after acquisition. If a decision is taken to retain the dataset, then a review period of between 6 months and 24 months will be set, and continued retention will then be considered at the meeting after that period."

78 The witness further gave evidence (at §86) that:

> "… at the end of the retention period, data of a certain age (within that dataset) will be scheduled for deletion (because it is not considered necessary and appropriate to continue to hold that data). …"

79 As to the systems on which BPD is held, the witness stated (§92):

> "Criteria which will inform decision-making as to the system onto which the dataset will be loaded will include: whether there is any particular sensitivity in relation to the data or the source of the dataset, and whether it is necessary for the data to be made available to all investigators."

80 In respect of independent oversight, the witness asserted (at §99): "*MI5 keeps the Home Secretary appraised, on an annual basis, of its BPD holdings and key matters in relation to its policy relating to, and use of, BPD.*" And (at §100) he said: "*The* [Intelligence Services] *Commissioner has exercised oversight of BPD throughout the period since October 2010. On a twice yearly basis we have provided to the Commissioner a full list of all BPD then currently held by us.*"

81 Specifically in relation to BCD, the witness stated (§130): "*BCD in the database is currently retained for 1 year … since December 2008, the database has not held data that is more than 365 days old. Since November 2009, the database has held data for 365 days*

(automatically deleting any data that is older than 365 days)". And, in relation to the BCD Handling Arrangements (§132): "[save for specific described instances of non-compliance], *these set out and describe our current practice and procedure in relation to the acquisition, use, retention, review, deletion and oversight of BCD"* (emphasis added).

82 As is now apparent from the Initial MI5 Disclosure summarised above, this evidence to the Tribunal was materially misleading. No effort has been made by the Respondents, who adduced this evidence, to identify these statements, nor to explain how this came about.

83 The Respondents, including the SSHD and MI5, in the Respondents' Skeleton Argument for OPEN Preliminary Issues Hearing 26–29 July 2016 dated 20 July 2016, addressed the position in relation to MI5 at §§104–123 (BCD) and §§151–160 (BPD). The Respondents stated at §§115–116:

> "… MI5 is, and throughout the material period, has been obliged not to keep data, including BCD, for longer than is necessary having regard to the purposes for which the data has been obtained and are being retained / used.
>
> The appropriate retention period was initially six months, before being revised upwards, and then fixed in November 2009 at one year. Any data that is older than one year was automatically deleted: see Appendix A, §86."

They relied upon the Handling Arrangements at §§100–101, 121 and Appendix A §§74–117. At Appendix A §40, the Respondents relied upon the fact that the Commissioner's oversight was extended in 2015 to cover "*MI5's storage and destruction arrangements for the data*". Accordingly, at §123, the Respondents asserted that the MI5 BCD regime was in accordance with Article 8(2) ECHR.

84 In relation to retention/review/destruction of BPD, the Respondents in their Skeleton informed the Tribunal that (§155):

> "MI5 was also obliged to comply with the fifth data principle, as set out in respect of GCHQ at §138 above. In addition, the relevant Codes of Practice and MI5's internal arrangements included safeguards in relation to retention/review/destruction, as did the joint SIA BPD Policy in force from February 2015: see Appendix B, §§75, 94-99 and 120."

The Respondents relied upon the Handling Arrangements at Appendix B §§85–100, 124–125, 128–160. Accordingly, at §170, the Respondents asserted that the MI5 BPD regime was in accordance with Article 8(2) ECHR.

(2) The Tribunal's First BPD/BCD Judgment

85 On 17 October 2016, the Tribunal issued its judgment in relation to, inter alia, the compliance with Article 8 ECHR of MI5's BPD and BCD regime (the "**First BPD/BCD Judgment**"). In summarising the jurisprudence it was applying at §62, the Tribunal noted:

> "(i) … We must be satisfied that there exist adequate and effective guarantees against abuse. …
>
> (vi) The degree and effectiveness of the supervision or oversight of the executive by independent Commissioners is of great importance, and can, for example in such a case as *Kennedy*, be a decisive factor."

86 In respect of the period post-avowal, the Tribunal accepted the Respondents' assertions as to the effectiveness of the measures in place to provide safeguards over the BPD and BCD regimes: see §§65–66, §§85–101. Indeed, the Tribunal reproduced the Respondents' appendices to their skeleton argument as appendices to its own judgment, and concluded (§88):

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

(3) The Respondents' Report on Searches

87 In light of the Tribunal's conclusion that the BPD and BCD regimes were unlawful before they were publicly acknowledged to exist and procedures relating to them were publicly disclosed (i.e. "pre-avowal"), the Respondents, pursuant to the Order of the Tribunal, provided a Report on Searches dated 17 February 2017. That report initially stated that MI5 did not hold data relating to PI (the Claimant in the Existing BPD/BCD Challenge) in its BCDs in the period when the BCD regime was unlawful.

88 On 6 October 2017, the Respondents provided a Re-Amended OPEN Response to the Claimants' Request for Further Information Relating to Searches dated 22 February 2017. In that document, §§3A–3C and 26 provide:

> "3A. In July 2017 the MI5 team dealing with the BPD/BCD case established that MI5 held a category of data, in the form of 'workings' that officers conducting investigations may have saved, and that this data could be relevant to the accuracy of the searches undertaken in January 2017. In particular, it was established that, in an area known as ['Workings'], officers could (if they needed to do so) save the results of their analysis (arising from a particular investigation) and that these saved 'workings' could include (amongst other things) the results from searches that they had undertaken, including the results of searches of MI5's BPD holdings and MI5's BCD database.
>
> 3B. Because of the possibility that the data that had been saved into 'Workings' could potentially be the result of a search of a BPD database or the BCD database, MI5 concluded that it should search 'Workings' for any data in relation to the search terms provided by the Claimant. The results of these searches (carried out in August and September 2017) relating to the Claimant's search terms, are reflected in the re- amendments below, and are described in more detail in CLOSED.
>
> 3C. The search results from 'Workings' also caused MI5 to review its corporate record search results.
>
> … 26. The results of the corporate record and BCD searches conducted by MI5 show that data from MI5's BCDs relating to the Claimant was either accessed or examined during the pre-avowal period."

89 Accordingly, the Report on Searches was amended on the same date to state that MI5 did unlawfully hold data relating to the Claimant in its BCDs prior to avowal.

90 At paragraph 9F of MI5's Amended Report on Searches (which was gisted to PI on 14 September 2018), it was stated that "*there is no existing review, retention and deletion … period prescribed for the data (officers' workings, including the results of searches) that has been saved in Workings*".

91 This issue of "Workings" appears to be distinct from the issue disclosed in the Initial MI5 Disclosure. After Liberty suggested in the IPA Challenge in its Skeleton Argument of 9 June 2019 for a directions hearing on 11 June 2019 (at §§18–23) that the issue of "Workings" and those that are the subject of the Initial MI5 Disclosure appeared to be

linked, the Defendants to that claim submitted at the hearing that the issues were distinct. Were it otherwise, the SSHD (as a party to the IPA Challenge) and MI5 would no doubt have clarified, in light of these submissions, that the two issues were in fact one and the same.

(4) The Tribunal's Third BPD/BCD Judgment

92 In the Tribunal's third judgment in the Existing BPD/BCD Claim dated 23 July 2018 ([2018] UKIPTrib_IPT_15_110 CH) (the "**Tribunal's Third BPD/BCD Judgment**"), the Tribunal recognised the ability to re-open its First Judgment in light of further information that had been disclosed subsequent thereto (§98):

> "It is common ground between the parties that, if our Judgment was flawed, based upon materially inaccurate evidence, ie if evidence, which was material to our decision, was materially inaccurate, we would reopen the Judgment, at least to the extent of reconsidering the issues in the light of all the evidence. It is clear that no such reopening of a concluded Judgment would occur unless such material evidence was fresh evidence, that is evidence which neither was nor could reasonably have been known to the Claimant at the time of the original Judgment."

93 The Tribunal acknowledged at §6(i):

> "It is not irrelevant that this Tribunal is called the Investigatory Powers Tribunal, because, in addition to reaching a number of judicial conclusions, it has been constantly necessary, in this case in particular, for the Tribunal, at the instance of the Claimant, but very often at the instance and with the assistance of the Counsel to the Tribunal, to probe and to consider fresh problems and lacunae."

94 The subsequent disclosure of additional information revealing inaccuracies in the GCHQ Witness's evidence concerning unlawful delegation of section 94 directions[29] led to the Tribunal re-opening its conclusion from the First BPD/BCD Judgment that GCHQ's regime under section 94 TA was in accordance with Article 8 ECHR since 4 November 2015: Tribunal's Third BPD/BCD Judgment §§58, 97.

95 In respect of PI's further proposed basis for re-opening the judgment, on the ground that Sir Stanley Burnton (when Interception of Communications Commissioner) was not

[29] See the Tribunal's Third BPD/BCD Judgment at §§12-16.

properly appraised of the true facts in relation to his review of the section 94 directions, the Tribunal:

(1) concluded at §106 that "*all relevant documents were made available to* [Sir Stanley Burnton]" and there was accordingly no basis for re-opening the First BPD/BCD Judgment; and

(2) was additionally persuaded by the fact that: "*There is and has been a genuine determination both on the part of the Commissioners and the Agencies themselves to get things right*" (§112).

In light of the Initial MI5 Disclosure, the first conclusion, and the second conclusion in respect of MI5 (at the time it was reached), are now untenable.

96 The Tribunal additionally considered the proportionality of MI5's BPD and BCD regimes. The Tribunal held at §§92–94:

> "It is significant that there is no criticism by the Claimant of the safeguards set out in Appendix 2 to this Judgment, especially at paragraphs 29, 80 and 81, relating to the regular consideration of proportionality by the Agencies at each stage of acquisition of and access to BCD and BPD and the reduction of intrusiveness by the filtering out of irrelevant material. We have set out in our CLOSED Judgment our conclusions about the way in which the system has operated in practice. It is quite clear that the Commissioners were extremely diligent in chasing up and questioning compliance by the Agencies with regard to proportionality. …
>
> We are satisfied that consideration of proportionality is inbuilt into the Agencies' systems, and that there is regular consideration, at both the stage of acquisition and of access, of whether there are any practical alternative measures that could be taken.
>
> In the circumstances which we have considered in open and in closed, we consequently resolve the issue of proportionality, reserved by paragraphs 16(d) and 102 of our First Judgment, in favour of the Respondents."

In light of the Initial MI5 Disclosure, those conclusions are now likewise untenable in respect of MI5.

97 Following the Tribunal's Third BPD/BCD Judgment, PI submitted to the Tribunal (Skeleton Argument on behalf of the Claimant for the Hearing on 25 September 2018 dated 19 September 2018) at §2:

> "The Claimant invites the Tribunal to apply its findings on the legal position re Article 8 ECHR (the position on EU law awaiting the reference from the CJEU) as set out in its judgments dated 17 October 2016 (Privacy International [2017] 3 All ER 647, [2016] HRLR 21) and 23 July 2018 ([2018] UKIPTrib IPT_15_110_CH) to the facts. In order to achieve that, the Tribunal will need to ensure that as much as possible has been disclosed to the Claimant, and make findings of fact as to the nature and extent of the breaches that have occurred."

98 Notwithstanding that substantive issues remained outstanding, the Tribunal on 26 September 2018 at the request of all parties issued a Determination pursuant to s 68(4) RIPA (the "**Determination**") to "*enable submissions to be made at some later stage as to what remedies, if any, should be ordered*" (§3).

99 In respect of MI5, the Tribunal determined in the Determination (§5(c)–(d)):

> "MI5 held BPD data related to the Claimant in the pre-avowal period [i.e. prior to 11 March 2015]. As a consequence of our findings in the judgments referred to in paragraph 2 above that data was unlawfully held. MI5 has accessed or examined such data, as it accepts (see paragraph 11 of the Respondent's Re-Amended OPEN Response to the Claimant's Request for Further Information which was served on 6 October 2017 ("the RFI")).
>
> MI5 held BCD data related to the Claimant in the pre-avowal period [i.e. prior to 4 November 2015]. As a consequence of our findings in the judgments referred to in paragraph 2 above that data was unlawfully held. MI5 has accessed or examined such data, as it accepts (see paragraph 26 of the RFI)."

100 On 16 April 2019, the Tribunal issued its OPEN reasons for the Determination. At §§5–12, the Tribunal addressed MI5's decision to delete the data contained in "Workings" the day prior to the Tribunal's hearing. The Tribunal endorsed IPCO's conclusion that MI5's decision to delete the data was "*regrettable*" but "*legitimate*" (§10).

(5) The Response to the Initial MI5 Disclosure in the Existing BPD/BCD Claim

101 On 4 October 2019, it was disclosed into OPEN in the Existing BPD/BCD Claim that, upon the Initial MI5 Disclosure being made in the IPA Challenge (in which Lord Justice Singh was presiding), the Respondents wrote to Lord Justice Singh, as President of the

Tribunal, by letter dated 7 June 2019 in relation to the Existing BPD/BCD Claim (the **"7 June 2019 Letter**").

102 In the 7 June 2019 Letter, the Respondents asserted that: "*... we do not consider that this matter is relevant to any issue which remains for consideration by the Tribunal*". They alleged that "[t]*he claim in respect of Bulk Personal Data ("BPD") has concluded*" and that, regarding the claim in respect of BCD, the claim "*has concluded insofar as the Claimant alleged that the BCD regime was unlawful as a matter of domestic law and the European Convention on Human Rights ('ECHR')*". They further stated:

> "Relevance to Current IPT Proceedings
>
> As set out above, (a) these proceedings alleged that the pre-Investigatory Powers Act 2016 regimes for BCD and BPD were unlawful; and (b) the claim in respect of BPD has concluded as has the claim in relation to BCD save for issues of EU law. Given that procedural position, the [issues that have arisen] are not relevant to the extant proceedings. We make the following points in this regard.
>
> [REDACTED]
>
> (ii) As to BPD
>
> [REDACTION]
>
> In any event, this part of the claim has now concluded …
>
> The searches carried out for the purposes of these proceedings were conducted at a fixed point in time and could never have been given complete assurance about the historical position. …"

103 These are extraordinary statements for the Respondents to have made. The proceedings are still extant (with a decision as to remedies outstanding, as well as the application of the CJEU's ruling in the matter referred to it). That, in and of itself, means that the Respondents' duty of candour remained and remains engaged. Further, the Tribunal has already shown itself properly willing to re-visit conclusions in circumstances where further information has subsequently been disclosed. The claim is also not, in respect of BPD, limited to the position prior to the IPA. The Respondents' position is therefore at best wrong and at worst disingenuous. Further, the basis for the extensive redactions in the correspondence is unclear. There appears to Liberty and PI to be no good reason for them, and disclosure of an unredacted or less redacted version of the letter is requested.

104 By letter dated 11 June 2019, the Respondents sent an OPEN letter to PI, stating:

> "Following the Written Ministerial Statement of the Home Secretary on 9 May 2019 … concerning compliance issues at the Security Service, we have considered whether anything falls for disclosure in this case, and have concluded that nothing falls to be disclosed."

105 For the reasons herein, that assertion — nowhere explained (save as above) — does not withstand scrutiny.

E STANDING

106 Liberty and PI meet the test for standing in this claim. Each has a sufficient interest in the subject-matter of the claim by virtue of (1) their objects and activities as organisations that seek to protect civil and human rights generally (Liberty) and privacy (PI), and (2) their belief that their communications or other information concerning them has been unlawfully intercepted or otherwise obtained, used and improperly retained (see below).

107 Liberty and PI are both also victims for the purposes of s 7 of the HRA in relation to unlawful bulk and other surveillance:

(1) As campaigning organisations, Liberty and PI have rights to respect for their correspondence and to freedom of expression under Articles 8 and 10 ECHR. Further, their staff, who enjoy all rights accorded under Articles 8 and 10 ECHR, use means of communication that rely on public telecommunications systems for their work activities, which may involve private, sensitive and/or journalistic information. The reality of bulk collection and processing mechanisms is that very large numbers of people are likely to be affected by unlawful conduct, including the Claimants. Liberty and PI's interests are therefore likely to have been affected by unlawful bulk or other unlawful surveillance by MI5 or unlawful use of the information thus collected. In any event, mere subjection to a system of secret surveillance containing the defects pleaded above is sufficient to make them victims.

(2) The Tribunal's current case law – *Human Rights Watch v Secretary of State for the Foreign and Commonwealth Office* [2016] UKIPTrib15_165-CH [46] – as to victim status for the purposes of bringing a complaint to the Tribunal is as follows:

> "whether in respect of the asserted belief that any conduct falling within subsection s.68(5)[30] of RIPA has been carried out by or on behalf of any of the Intelligence Services, there is any basis for such belief; such that the 'individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or legislation permitting secret measures only if he is able to show that due to his personal situation, he is potentially at risk of being subjected to such measures.'"

The citation is of *Zakharov* [171]. The Tribunal in *Human Rights Watch* (supra) described this as a "*low hurdle*".[31]

(3) Here, as set out above and more specifically below, the IPCr's reports establish that there has in fact been extensive unlawful retention, use and failure to destroy bulk and other personal data over a long period, from which it follows that warrants and directions were also obtained unlawfully (as set out below).

---

30 It may be that this should be a reference to RIPA s 65(5).

31 Liberty and PI submit that this aspect of the *Human Rights Watch* case law is wrong in principle, for two reasons:

(1) It is necessary, to ensure that the Tribunal's review regime operates compatibly with human rights, for there to be an unfettered right of access (subject to controls for truly vexatious cases), which is required by HRA s 3.

(2) The Court in *Zakharov* (supra) at [171] was dealing with the question of victim status for an application to the ECtHR where a person did not claim that secret surveillance measures had been applied to them (or there was any particular reason to suspect this). It held that a person would be a victim for this purpose where (a) there was no effective domestic remedy (in which case all actual or potential users of a telecommunications system were victims of a direct interference with their Article 8 rights) or (b) there was an effective domestic remedy in relation to alleged unlawful surveillance, in which case a person would be a victim only where the person could show that, due to their personal situation, they were at risk of being subjected to such measures. This approach becomes circular if applied by a domestic tribunal: the standard the domestic tribunal applied itself determines whether one is a victim for the purposes of an application to the ECtHR. In other words, in accepting this as an acceptable standard, the IPT has effectively assumed there is an effective domestic remedy even for those who have no basis for suspecting surveillance provisions have been applied to them, and who on the IPT's approach (requiring a basis for thinking surveillance measures have been applied) cannot bring a claim. Under both the previous RIPA regime and the IPA, they have no other means of finding out whether they have been unlawfully placed under surveillance. They therefore have no effective domestic remedy, by virtue of the standard the Tribunal has adopted for victim status.

The Claimants accept, however, that this approach represents the case law of the Tribunal and further that the Divisional Court approved the Tribunal's decision in *HRW* at [112] of the IPA Challenge. They therefore at this stage reserve this point for any appeal, should the Tribunal decide any aspect of the case by reference to standing and victim status.

(4) There is further at the very least a real risk of a breach of the privacy rights of Liberty and PI, arising from their nature as campaigning organisations and by virtue of the activities they conduct, not least given their particular focus on ensuring lawful use of interception and surveillance powers by the intelligence services and police/law enforcement bodies. As part of their work, the Claimants communicate with clients and others who may be of intelligence interest. The Claimants' communications are likely to have been collected and processed as a result.

(5) Indeed, this is clear from the Tribunal's previous determinations. The Tribunal's determinations to date demonstrate that organisations such as Liberty and PI have been the targets of (unlawful) surveillance and use of their information:

(a) The Tribunal has already found in the Existing BPD/BCD Claim that PI's data was collected, held and processed unlawfully, including by MI5 (see paragraph 99 above).

(b) In *Liberty v Secretary of State for Foreign and Commonwealth Office* [2015] UKIPTrib 13_77-H_2 (Amended Open Determination of 22 June 2015), the Tribunal found that:

(i) Amnesty International's emails had been lawfully and proportionately intercepted and accessed but had been unlawfully retained — it directed that the unlawfully retained emails should be destroyed (at §14); and

(ii) Emails of the Legal Resources Centre, an NGO in South Africa, had been intercepted and accessed, which the Tribunal held to have been done in breach of the internal procedures for selection for examination (at §15).

It therefore clear that the activities of highly respected NGOs, such as the Claimants, are subject to surveillance.

F THE LAW

(1) Relevant domestic law principles

108 It is trite law that:

(1) **Mandatory provisions:** Where a decision-maker fails to comply with provisions in legislation that may conveniently be termed "mandatory", their decision is unlawful and (at least in general) void *ab initio*: see, eg, *De Smith's Judicial Review* (8th ed 2018) [5-057] and the authorities there cited. Whether non-compliance with a legislative requirement has this effect is a question of construction, to be judged by reference to the text, context and object of the provision and statute in question.

(2) **Jurisdictional/precedent fact:** Where a statute requires a fact to exist in order to operate a decision-making power, where that fact does not exist but the power is purportedly exercised, its exercise will be unlawful and void: see, eg, *R v Secretary of State for the Home Department, ex parte Khawajah* [1984] AC 74 (HL).

(3) **Mistake as to established and relevant fact:** A decision taken on an incorrect understanding of an "*established and relevant fact*", where (i) the fact may be established, (ii) the applicant is not responsible for it, (iii) the mistake was material to (though not necessarily decisive in) decision-making, and (iv) the decision results in "*unfairness*", is unlawful and void: *E v Secretary of State for the Home Department* [2004] EWCA Civ 49, [2004] QB 1044.

(2) Convention requirements under Articles 8 and 10 ECHR

109 The obtaining, accessing, use, and/or retention of any data of the Claimants is an interference with their rights under Articles 8 and 10 ECHR.

110 Under the rubric of the requirement for an interference with rights to be "*in accordance with the law*" or "*provided by law*" under Articles 8 and 10, that interference must satisfy two conditions:

(1) First, the interference must itself be <u>in accordance with</u> domestic law, that is, it must comply with domestic statutes, regulations, codes of practice that apply to the conduct in question: see, eg, *Big Brother Watch v United Kingdom* (App Nos 58170/13, 62322/14 and 24960/15, 18 September 2018, First Section) [465]–[467] ("***BBW***") (UK statute not complying with EU law held to be not "in accordance with the law" under Article 8).

(2) Secondly, in the case of a secret surveillance regime, in light of the severity of the interference and dangers of secret surveillance, as the law stands, a secret surveillance regime must set out in detail the following as "*minimum safeguards*" to avoid abuse:

> "the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed …"

The ECtHR has stated this principle in these terms in cases including: *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [231]; *Szabó and Vissy v Hungary* (App No 37138/14, 12 January 2016, Fourth Section) [56]; *Weber and Saravia v Germany* (App No 54934/00, 29 June 2006, Third Section) [95].

In this context, *BBW* at [330] further establishes that, in the context of a bulk regime, the first two requirements (directed to the scope of application of the regime) require that "*the grounds upon which a warrant can be issued"* must be "*sufficiently clear*", the law must "*give citizens an adequate indication of the circumstances in which their communications might be intercepted*" and that "*domestic law gives citizens an adequate indication of the circumstances in which their communications might be selected for examination*".

(3) Similarly, in relation to state databases of material, as the Grand Chamber said in *S & Marper v United Kingdom* (2008) 48 EHRR 1169 [99] in relation to national databases of the fingerprints and DNA of criminal suspects:

> "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 … The Court notes, however, that these questions are in this case closely related to the broader issue of whether the interference was necessary in a democratic society."

111 A more onerous test for the requirement of foreseeability under Articles 8 and 10 exists in these contexts because surveillance measures and secret state databases are not open to

public scrutiny generally or by the individuals affected, so, as the Grand Chamber held in *Zakharov* (supra) at [229]–[230]:

> "especially 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 interception of telephone conversations, 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 …
>
> [I]t would be contrary to the rule of law for the discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference …"

112 Crucially for present purposes, however, whether the safeguards actually operate effectively in practice so as to ensure that Article 8 and 10 rights are respected — the "*actual operation*" of a secret surveillance regime — is critical to an assessment of its compliance with Articles 8 and 10: see *Zakharov* [284], [303].[32] The safeguards must be "*adequate and effective*" in practice to secure the Convention rights concerned, not theoretical and illusory: *Zakharov* [232]. Further, any review mechanism "*must be vested with sufficient powers and competence to exercise an effective and continuous control*": *Zakharov* [275]. As the Defendants submitted in the IPA Challenge: "*In assessing compatibility with the Convention, regard must be had to the actual operation of a surveillance system, including the checks and balances on the exercise of power and the existence or absence of any evidence of actual abuse: see Ekimdzhiev v Bulgaria app. 62540/00, 30 January 2008, at [92], BBW at [320]*."

113 Not every error will be such as to show that this requirement is not met. Some errors, and their prompt identification and correction, might show a system of regulation oversight that is working properly. Without more, if the IPCr identifies swiftly through audit a problem, investigates it, and resolves it, this may be said to show that the system of internal oversight works. That is, it may show that the system of guarantees is effective.

---

[32] See also *Catt v United Kingdom* (App No 43514-15, First Section, 24 January 2019) [120]–[123], referring to the "*absence of effective safeguards*", and *Gillan v United Kingdom* (2010) 50 EHRR 45 [84], referring to reports demonstrating the inappropriate and unlawful use of stop and search powers.

(3) EU law requirements

114 Liberty and PI submit that MI5's retention, review and destruction of data and other conduct set out above falls within the scope of EU law,[33] in particular the ePrivacy Directive (see Articles 1, 2 and 15 thereof).

115 Under EU law, these actions are subject to the following requirements:

(1) Article 15(1) of the ePrivacy Directive requires that derogations from the rights it confers, including (in Article 5(1)) to the confidentiality of communications transmitted by a public communications network and through publicly available electronic communications services, be effected via "*legislative measures*".[34]

(2) Articles 7, 8 and 11 **CFR** provide for the rights to respect for private and family life and communications, protection of personal data and freedom of expression. Articles 7 and 11 CFR provide at least equivalent protection to that of Articles 8 and 10 ECHR.[35] These provisions reflect general principles of EU law.

(3) Article 52(1) CFR requires that any limitation on the exercise of each of these rights must be *inter alia* "*provided for by law*" and proportionate. Article 8(2) provides, in relation to Article 8, that personal data "*must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law*". These provisions similarly reflect general principles of EU law.

116 Pursuant to general principles of EU law, reflected in Article 47 CFR, any person whose EU law rights have been violated has a right to an effective remedy for that violation.

---

33 Liberty and PI recognise that this is the question of EU law raised in the reference in the Existing BCD/BPD Claim, as to which see footnotes 25 above and 38 below, which remains pending. They therefore do not ask the Tribunal to determine this point without the CJEU's judgment. That is of course no reason to prevent the claim otherwise from moving forward.

34 See, as to this, Opinion of Advocate-General in *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:572 [150]–[151], applied by the CJEU in Joined Cases C-203/15 C/698-15 *Tele2Sverige and Watson* [2017] QB 771 [117] ("*a measure of that kind must be legally binding under domestic law*").

35 Explanations Relating to the Charter of Fundamental Rights [2007] OJ C 303/17 at 20–21, 33.

(4) The relevant statutory safeguards

117 The core of the statutory protection for privacy over warranted data once obtained is provided by the retention safeguards sections in the IPA, namely, ss 53 (targeted and thematic interception), 129 (targeted and thematic hacking), 150(2), (4)–(5) (bulk interception), 171 (bulk communications data) and 191(2), (4)–(5) (bulk hacking). (There is no equivalent provision in Part 7 of the IPA, which makes provision for the exercise by MI5, MI6 and GCHQ of their powers to retain bulk personal datasets.)

118 Equivalent provisions were formerly in s 15 of RIPA and, before that, s 6 of the Interception of Communications Act 1985.

119 The basic principles are, to take for example s 138 (bulk interception warrants under the IPA):

> "(1) The Secretary of State may, on an application made by or on behalf of the head of an intelligence service, issue a bulk interception warrant if — …
>
> (e) the Secretary of State considers that satisfactory arrangements made for the purposes of sections 150 and 151 (safeguards relating to disclosure etc.) are in force in relation to the warrant,
>
> …"

By s 141(1), "*decision to issue a bulk interception warrant must be taken personally by the Secretary of State*".

120 The matters which, to issue a bulk interception warrant, the Secretary of State must consider to be satisfactory under s 138(1)(e) include those under s 150. By s 150(1), relevantly:

> "The Secretary of State must ensure, in relation to every bulk interception warrant, that arrangements are in force for securing —
>
> (a) that the requirements of subsections (2) and (5) are met in relation to the material obtained under the warrant, and
>
> (b) that the requirements of section 152 are met in relation to the intercepted content or secondary data obtained under the warrant."

By section 150(2) and (4):

"(2) The requirements of this subsection are met in relation to the material obtained under a warrant if each of the following is limited to the minimum that is necessary for the authorised purposes (see subsection (3)) —

(a) the number of persons to whom any of the material is disclosed or otherwise made available;

(b) the extent to which any of the material is disclosed or otherwise made available;

(c) the extent to which any of the material is copied;

(d) the number of copies that are made.

…

(4) The arrangements for the time being in force under this section for securing that the requirements of subsection (2) are met in relation to the material obtained under the warrant must include arrangements for securing that every copy made of any of that material is stored, for so long as it is retained, in a secure manner.

(5) The requirements of this subsection are met in relation to the material obtained under a warrant if every copy made of any of that material (if not destroyed earlier) is destroyed as soon as there are no longer any relevant grounds for retaining it (see subsection (6))."

121 Thus, the effect of these provisions, and the equivalent provisions for bulk powers under Part 6 of the IPA, and for the so-called "targeted" and "thematic" powers under Parts 2 and 5, is that the Secretary of State must ensure that arrangements are in force that have the effect that, for any material obtained under a warrant:

(1) the number of persons, extent of any disclosure, extent of any copying and number of copies made are kept to the minimum necessary;

(2) the material must be stored in a secure manner; and

(3) each copy made of any material or data must be destroyed as soon as its retention is no longer necessary (which requires not merely the destruction of the initial intercept material, but also of any copy, extract or summary of <u>any</u> of the material made identified as intercept material: see, e.g., s 150(9)).

122 Similarly, under IPA Part 7, ss 204 and 205[36] require respectively that, for a class or specific BPD warrant to be issued, it must be the case that "*the Secretary of State considers that the arrangements made by the intelligence service for storing bulk personal datasets of the class to which the application relates and for protecting them from unauthorised disclosure are satisfactory*" (s 204(3)(d)) and "*the Secretary of State considers that the arrangements made by the intelligence service for storing the bulk personal dataset and for protecting it from unauthorised disclosure are satisfactory*" (s 205(6)(d)).

123 Liberty and PI submit that, on their proper construction, and having regard to their purpose (namely, minimising the extent of any interference with privacy that occurs through the interception and retention processes) the effect of these provisions is that:

(1) the requirement in s 138(1) and equivalent provisions are "jurisdictional" or precedent facts, that is, they must in fact be satisfied for the power to issue a warrant to exist and be capable of lawful exercise;

(2) if requirements that the Tribunal, in reviewing decisions to issue warrants, itself considers to exist and to be satisfactory do not in fact exist (that is, if the consideration of the Secretary of State does not reflect the actual existence of the arrangements required under s 150(2)–(5) and equivalent provisions or satisfactory arrangements under Part 7), then the Secretary of State may not issue a warrant.

124 PI and Liberty submit that the terms and purpose of the relevant provisions in RIPA (ss 15 and 16) are not relevantly different from those in the IPA.

125 In respect of section 94 of the TA, s 94(1) or (2) read with (2A) required the Secretary of State (him- or herself, that is, personally and not by delegation: see Third BPD/BCD Judgment §§42–45) to be satisfied that the direction was "*necessary*" and "*proportionate*", i.e. in accordance with EU law and/or ECHR requirements, before making a direction for BCD. It was accordingly necessary for the Secretary of State to be provided, by the Security Intelligence Agencies, with all information material to the exercise of his or her discretion.

---

[36] These must be read with the relevant functions of, relevantly, MI5 as set out in the Security Service Act 1989 s 1, whose exercise Part 7 conditions.

G MI5'S UNLAWFUL CONDUCT

126 The documents summarised in Part B above establish that:

(1) MI5 knew about a series of serious breaches with basic requirements for compliance with Articles 8 and 10 ECHR, and with fundamental statutory requirements imposed on it by Parliament for the issue of warrants (under both RIPA and the IPA);

(2) MI5 did not fix these issues;

(3) Notwithstanding knowledge at the highest levels of MI5, which on the documents and extracts from documents Liberty and PI have seen went back as far as May 2013 at MI5 Board level (see paragraph 50(1) above), MI5 did not itself report the issues for several years and, when it finally did report these matters to the IPCr in February 2019, MI5 was not frank and made at best a partial and incomplete report;

(4) The true nature of the problems was sufficiently serious that even MI5 itself did not understand the true scale and extent of the (systemic) problems — it now seems for years after the problems had been discovered — as Sir Andrew Parker admitted; and

(5) These problems were not separately identified by the IPCr (or his predecessor under RIPA) in its audit role.

127 The seriousness of these breaches is on the higher end, given in particular that: (1) Fulford LJ has found that MI5 made inaccurate statements to Judicial Commissioners (both in relation to their induction and to obtain the grant of warrants); (2) MI5 appears to have breached its duty of candour on warrant applications and in the obtaining of section 94 TA directions prior to March 2019; (3) MI5 has breached its duty of candour in the Existing BPD/BCD Claim; (4) these issues are of very long standing, and were known about at senior levels of MI5, for some years before any action was taken; and (5) the breaches themselves were extensive and serious. These conclusions are irreconcilable with the Tribunal's conclusions in relation to MI5 in the First BPD/BCD Judgment.

128 As the IPCr (Fulford LJ) himself concluded in his Generic Warrants Decision at §10 [**B/4/99**], MI5 had recently revealed to him "*the undoubted unlawful manner in which data has been held and handled*", giving "*file shares*" and "*data stores*" (two ways in which MI5 processes material obtained under warrants) as examples of this.

129 Liberty and PI do not have a full or clear picture of MI5's unlawful conduct, due to the extensive redactions in the documents. Liberty and PI will supplement these Grounds of Claim as required. The Respondents are reminded of their duty of candour, which includes disclosure of material that relates to any hitherto unappreciated grounds or areas of challenge.

130 Pending such disclosure and fuller investigation by the Tribunal of the circumstances in which incorrect statements appear to have been made to the Secretary of State and Judicial Commissioners by MI5, to their knowledge, Liberty and PI are not able to state more specifically the dates and decisions to which the submissions below apply.

(1) Domestic law claims

131 Warrants issued to MI5 under the IPA and RIPA and/or section 94 TA directions made in favour of MI5 in the circumstances set out above were unlawful and void.

(a) Failure to comply with mandatory provisions / Absence of "jurisdictional" or precedent fact

132 The requirements on the Secretary of State to ensure that various safeguards exist, and the condition that the Secretary of State be satisfied as to their existence before a warrant is issued, are:

(1) Mandatory provisions, so that failure to follow them vitiates any decision taken in those circumstances; and

(2) Precedent or "jurisdictional" facts to the exercise of the Secretary of State's power to issue a warrant, such that, unless the requirements in question do in fact and exist and are satisfactory, there is no power to issue a warrant.

133 Liberty and PI submit that, as Fulford LJ has in substance found, in the circumstances set out above MI5 did not in fact have arrangements in place that satisfied IPA s 150 and similar provisions (or the predecessor provisions under RIPA). Due to the widespread use of "TE1" and "TE2" within MI5, and their apparently systemic failings in relation to retention, review and deletion and LPP (and the other "*RED*" and "*AMBER*" areas the subject of the First Inspection Report and Second Inspection Report, which have not been disclosed), MI5's systems for material obtained under warrants did not ensure that: (1) the number of persons, extent of any disclosure, extent of any copying and number of copies

made are kept to the minimum necessary; or (2) each copy made of any material or data is destroyed as soon as its retention is no longer necessary.

134 It follows that, so far as RIPA and the IPA are concerned, all warrants issued to MI5 while this situation persisted — and persists — were and are unlawful, null and void.

(b) Mistake as to established fact

(i) Issue of individual warrants and directions in the absence of information as to MI5's compliance

135 Further or alternatively, for substantially the same reasons, insofar as the Secretary of State has decided to issue a warrant under the IPA or RIPA and, under the IPA, any Judicial Commissioner has approved such a decision, it appears that such decisions will have been based on a mistake as to an established fact. That fact was either (i) the actual condition of MI5's systems for retaining/reviewing/deleting warranted data itself or (ii) the existence of further evidence as to the condition of those systems that would be relevant to the decision to grant a warrant. Such analysis applies equally to section 94 directions issued by the Secretary of State on a mistaken understanding of the Article 8 ECHR and EU law compliance of MI5's ability to hold BCD/BPDs.

(ii) Issue of individual warrants and directions on the basis of misunderstandings due to misleading statements made to Judicial Commissioners in support of warrant applications and as part of initial briefing and training

136 Further or alternatively, Fulford LJ makes clear that MI5 has made incorrect statements that should not have been made, and further that such statements have been made, or allowed by senior officials at MI5 to be made, knowing that they were not true: see paragraph 25 above, in particular Fulford LJ's finding that "*it is impossible sensibly to reconcile the explanation of the handling arrangements the Judicial Commissioners were given in briefings and the JC Handbook with what MI5 knew over a protracted period of time was happening*" (Generic Warrants Decision §6 [**B/4/98**]).

137 Liberty and PI infer that it is on the basis of such false statements that MI5 has obtained warrants (or section 94 directions) that, as Fulford LJ found, should not have been issued.

138 This is a further reason why such decisions to issue warrants, and any decisions to approve the same, are unlawful.

(c) Unlawful conduct in respect of the Claimants

139 If and to the extent that (i) any warrant or authorisation is unlawful and data has been obtained, retained or used purportedly pursuant to it or (ii) there has been a breach of any of the statutory requirements above in relation to any data obtained or held by MI5 (whether or not any warrant or authorisation was itself lawful), the Claimants' data has been (in the case of PI) and is likely to have been (in the case of Liberty) unlawfully held or used. Any such conduct was unlawful.

140 Further or alternatively, Liberty and PI are not aware of the terms of the warrants and authorisations, which have not been disclosed. However, it is possible that those warrants and authorisations themselves require steps to be taken or are granted subject to conditions (for example, as to the retention or deletion of data). Liberty and PI submit that:

(1) Insofar as a warrant or authorisation was itself lawfully granted, the effect of the provisions and purpose of the RIPA, TA and IPA (as set out in paragraphs 117–125 above) is that any requirement the warrant/authorisation imposes is itself to be treated as a mandatory requirement.

(2) Accordingly, non-compliance with any such requirement has the consequence that the obtaining, retention and use (or continued obtaining, retention and use) of any data is unlawful.

141 Given the secrecy of the conduct, the Claimants cannot provide further particulars at present. The Tribunal is invited to direct at a minimum that any requirements as to the holding of data in warrants or authorisations are sufficiently disclosed in OPEN so that the present Claimants can make effective submissions.

(2) Convention and EU law claims

(a) ECHR: Grant of warrants and directions and data obtained/held under them

142 MI5 has, in relation to warrants obtained in the circumstances set out above, and any obtaining or retaining of data under them, acted in a manner that was "*not in accordance with the law*" and not "*provided by law*" under Articles 8 and 10. This is because in obtaining purported warrants it has failed to comply with domestic law.

143 Further, in relation to directions for the acquisition of BCD pursuant to section 94 TA granted to MI5, there was likewise no Convention-compliant basis for the direction to be issued and/or for data to be retained. Each such direction and/or retaining was therefore unlawful.

144 The Claimants were victims of the failures to comply with the statutory arrangements set out above.

(b) ECHR: Systemic challenge

145 In addition, the regimes under the IPA, RIPA and the TA appear themselves not to be "*in accordance with the law*" or "*prescribed by law*" under Articles 8 and 10 ECHR and/or disproportionate in all the circumstances (so that any obtaining or retaining of data under them will also have been unlawful), because the Initial MI5 Disclosure establishes that the safeguards in the statutory regimes (assuming those regimes otherwise to satisfy the requirements of Articles 8 and 10 ECHR)[37] are not effective in practice but are instead theoretical and illusory. Liberty and PI note that the Divisional Court considered this question in the IPA Judgment [353]–[392] in relation to the IPA and, on the OPEN materials before it, did not accept Liberty's argument (as set out above). The Tribunal is respectfully invited to consider this matter as to RIPA and, in relation to the IPA, to consider the argument afresh, on the basis of the additional and CLOSED material the Claimants anticipate the Tribunal will have before it in the present claim. In any event, the Claimants reserve their position on this point in the event of any appeal in the present claim or any claim for judicial review of the Tribunal's decision.

(c) EU law claim

146 The SSHD's and MI5's conduct set out above in granting and obtaining warrants and directions, and retaining data purportedly pursuant to them, is also in breach of EU law and unlawful for the reasons set out above, namely:

---

[37] Liberty and PI do not accept that this is the case. However, they recognise that this issue will be finally determined for RIPA by the Grand Chamber in *BBW* and that the Divisional Court has decided that the safeguards under Parts 6 and 7 of the IPA do meet these requirements in the IPA Judgment. The time for appeal of the IPA Judgment has been extended until after the handing down of the Grand Chamber's decision in *BBW*. For the avoidance of any doubt, Liberty reserves the right to advance arguments on any appeal from the IPA Judgment decision that those requirements are not satisfied.

(1) Those actions did not occur in accordance with domestic law, namely, the statutory powers that provide for them, again with effect that the interferences with the rights under Articles 7, 8 and 11 CFR (and the general principles they reflect) were not "*provided for by law*" (and, in the case of the rights under Article 8 CFR, "*laid down by law*") nor is their basis "*legislative measures*" under Article 15 of the ePrivacy Directive.

(2) Further or alternatively, those actions occurred pursuant to a system that did not meet the requirements of Articles 8 and 10 ECHR that an interference be "*in accordance with the law*" and thus *a fortiori* one that does not satisfy Articles 7, 8 and 11 CFR (and the general principles they reflect) and Article 15 of the ePrivacy Directive. For the same reasons, there was a disproportionate interference with rights.

147 It follows Liberty and PI have a right to an effective remedy in respect of the breaches under Article 47 CFR and the general principle of EU law it reflects.

H APPLICATION TO AMEND EXISTING BPD/BCD CLAIM AND RE-OPEN FINDINGS OF COMPLIANCE WITH ARTICLE 8 ECHR

148 It appears that at least part of the conduct disclosed by the Initial MI5 Disclosure occurred in relation to BPD and/or BCD. Accordingly, PI seeks the Tribunal's permission to amend its claim relating to BPD and BCD to include the above facts and matters, and requests the Tribunal to re-open the question of the compliance with Article 8 ECHR of MI5's BPD and BCD regimes for the period from respective avowal (the regime already being recognised to be unlawful prior to those dates).

149 As set out in Section D above, the pleadings, evidence and skeletons presented to the Tribunal in respect of MI5's BPD and BCD regime made no reference, in breach of MI5's duty of candour, to the matters that have now been disclosed. Nor has any proper explanation of this been attempted, as set out above.

150 The Tribunal recognised, in its First BPD/BCD Judgment, that the assessment of Article 8 ECHR compliance required safeguards that were actually effective and not merely illusory — see the jurisprudence summarised at paragraph 112 above and First BPD/BCD Judgment [60]–[62] (see especially [62(i)]). On the basis of the inaccurate and materially misleading information presented to the Tribunal by MI5, the Tribunal concluded that such

safeguards were in existence in relation to MI5. The new disclosure falsifies that conclusion, not only in relation to the effectiveness of the Handling Arrangements for ensuring the Convention-compliant treatment of BPD and BCD, but also the system of oversight by the Commissioners. For example, Sir Stanley Burnton's review of section 94 directions was carried out in ignorance of the potential and/or actuality that bulk data would remain in "TE1" (and perhaps also "TE2") without any, or alternatively any adequate, safeguards.

151 Furthermore, in addition to the systemic undermining of the safeguards, the new disclosure indicates that there has in fact been unlawful selection and storage of BPD/BCD by MI5 officers, where that data has been held indefinitely, with no period for its review and deletion — all of which constitutes a serious breach of Article 8 ECHR in relation to the data in question, and which further indicates in particular that the BPD/BCD regime does not satisfy the sixth *BBW* / *Weber* requirement for adequate and effective procedures under which information is reviewed and deleted.

152 It is no answer, as suggested by the Respondents, that the Tribunal has already delivered its First BPD/BCD Judgment. Various issues remain open in the Existing BPD/BCD Claim, including all questions of remedies and all questions of EU law in relation to BCD.[38] The Tribunal has already indicated, in the Third BPD/BCD Judgment, that it is appropriate in these ongoing proceedings to re-open matters that purport already to have been determined, in circumstances where material further information has been disclosed subsequent to its judgment.

153 The consequence of the additional matters now disclosed, revealing systemic and long-standing non-compliance with safeguards in relation to data, including bulk data, and the effective concealment of those issues from all aspects of the oversight regime (including the Tribunal), is that it is now untenable for MI5 to suggest that its BPD/BCD regimes were compliant with Article 8 ECHR unless and until such time as those matters are adequately addressed.

---

[38] On 20 January 2020, Advocate General Campos Sanchez-Bordona issued his Opinion in the preliminary reference made by the Tribunal to the CJEU in the Existing BPD/BCD Claim (Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* ECLI:EU:C:2020:5). The Opinion concluded that the Respondents' BCD regime was in scope of (§§28–33), and in breach of (§§37), EU law.

I CASE MANAGEMENT AND RELIEF

154 PI and Liberty submit that their New Claim should, as a matter of case management, be managed with the Existing BPD/BCD Claim (as amended) as the issues appear, at least in part, to arise out of the same facts and matters and there is considerable overlap.

155 PI and Liberty consider that it would be appropriate for the Tribunal to make immediate directions and/or orders for:

(1) The preservation by MI5 of all relevant data. No data identified pursuant to any of the steps below as having been unlawfully retained or potentially unlawfully retained should be destroyed prior to the conclusion of this claim and any appeal or period for appeal;

(2) The disclosure to the Tribunal without redaction of the items in Appendix 2 and Appendix 3 hereto and the disclosure (with appropriate redactions or gisting, if necessary, with regard to the scope of the present claim) of those materials to the Claimants;

(3) Investigation into and disclosure reflecting all RIPA and IPA warrants and section 94 directions issued to MI5 (or otherwise) on the basis of the Secretary of State and/or a Judicial Commissioner having an incorrect understanding of MI5's information management systems (that is, not being aware in full of the matters set out above as revealed by the Initial MI5 Disclosure or the availability of further information as to MI5's RRD and data handling processes), including in particular dates when and circumstances in which any unlawful conduct commenced or may have commenced; and

(4) Investigation into what material has been obtained, used and retained not in compliance with the statutory safeguards set out above and/or purportedly under any unlawful, void warrant or direction, including in particular the extent to which any data handled unlawfully has been or is now (subject to being held for the purposes of these proceedings) proposed to be permanently deleted.

156 Liberty and PI seek final relief that includes at least the following (which they will supplement and/or adjust as appropriate):

(1) The quashing of all warrants, authorisations and/or directions that were unlawfully issued and declaratory relief accordingly;

(2) Declarations that MI5 and/or the SSHD have unlawfully obtained, used, retained and failed to destroy material, because it has been obtained, used or retained other than in accordance with the statutory safeguards set out above and/or because it has obtained pursuant to unlawful warrants, authorisations and/or directions;

(3) Destruction of data that has been unlawfully retained;

(4) Damages and/or monetary compensation; and

(5) Such further or other relief as the Tribunal considers appropriate.

THOMAS DE LA MARE QC
BEN JAFFEY QC
DANIEL CASHMAN
DAVID HEATON

Bhatt Murphy
Liberty

APPENDIX 1 — CHRONOLOGIES

Date	MI5's awareness of the non-compliance	Existing BPD/BCD Claim	IPA Claim
2010	"*the specific IT environment was originally accredited in 2010*" (Compliance Improvement Review §3) "*Compliance failure risk had been reported to the Management Board as early as 2010*" (Compliance Improvement Review §16)		
2011	A 2011 review made a number of recommendations including mandatory training for users, and implementation of a retention and deletion policy (Compliance Improvement Review §3)		
May 2013	"*The MI5 Management Board discussed a paper setting out serious information management risks within the organisation … the work was under-resourced given the scale of the problem, and lacked urgency*" (Compliance Improvement Review §5)		
2014	"*This issue had first [been identified as being relevant to disclosure exercises in 2014]*" (First Inspection Report §7.1.6, including as gisted)		
2015	"*The [register] began development after our initial review of information management in the [TE] in 2015.*" (MI5 11 March 2019 Letter §20)	PI brings Existing BPD/BCD Claim	
January 2016	Legal paper on compliance risk produced by senior MI5 lawyer, recognising that "*allowing uncharted material to remain [in the TE] presents considerable legal risk …*		

Date	MI5's awareness of the non-compliance	Existing BPD/BCD Claim	IPA Claim
	We may fall foul of our duty under the SSA to only hold material for as long as is necessary for our statutory functions" (First Inspection Report §7.1.2) "[T]*he team conducting the compliance review …* [identified], *at a high level, that data might be being held in ungoverned spaces in contravention of our policies*" (MI5 11 March 2019 Letter §10)		
February 2016		19 February 2016: Respondents' Amended Open Response, relying upon the adequacy of oversight and handling arrangements in relation to BPD/BCD	
July 2016		Amended witness statement of MI5 witness, relying upon the adequacy of oversight and handling arrangements in relation to BPD/BCD First substantive hearing in the Existing BPD/BCD Claim, in which the Respondents relied upon MI5's compliance with the Handling Arrangements in relation to BPD and BCD compliance with Article 8 ECHR	
October 2016	TE review concluded there was "a high likelihood of relevant material not being discovered, or being	Tribunal's First BPD/BCD Judgment concluding that MI5's	

Date	MI5's awareness of the non-compliance	Existing BPD/BCD Claim	IPA Claim
	discovered when it should have been deleted, in a disclosure exercise leading to substantial legal or oversight failure" (First Inspection Report §7.1.5)	BPD and BCD regimes were compliant with Article 8 ECHR	
November 2016			IPA receives Royal Assent
December 2016			20 December 2016: Pre-action letter sent to Defendants (to which no substantive answer is ever provided)
February 2017			28 February 2017: Claim for judicial review issued
March 2017	Paper on "TE" risks, identifying "*significant risk around the absence of compliance with relevant legislation, Codes of Practice and Handling Arrangements. This includes categories of data for which there are [particular rules]*" (First Inspection Report §7.1.8)		
June 2017			14 June 2017: Permission granted on Part 4 EU law challenge
July 2017		19 July 2017: MI5 reports the retention of data in "Workings" to IPCO as an error	
October 2017	MI5 Paper on compliance in the "TE" provided to four MI5 Directors (First Inspection Report §7.1.10)	6 October 2017: MI5 updates its report on searches to take into account "Workings"	
January 2018	Risk from "TE" and "[another risk]" identified in paper to the MI5 Management Board by Director of Policy and		

Date	MI5's awareness of the non-compliance	Existing BPD/BCD Claim	IPA Claim
	Information and, from early 2018 reported in a dashboard (MI5 11 March 2019 Letter §10; First Inspection Report §7.1.15) By January 2018 if not earlier, "*MI5 had a clear view of some of the compliance risks around [the TE]*" (First Inspection Report §7.1.16) MI5 Management Board elevates the risk in its corporate risk register to "*RED*" and notes that an Audit Risk and Assurance Committee "*planned to carry out a deep dive review of compliance risk in June 2018*" (First Inspection Report §7.1.19)		
February 2018			First hearing, in relation to Part 4 / EU law
April 2018			27 April 2018: Divisional Court hands down first judgment, addressing EU law challenge to Part 4
July 2018		23 July 2018: Tribunal's Third BPD/BCD Judgment, re-opening its finding in relation to GCHQ's compliance with Article 8 ECHR, but otherwise not re-opening its First BPD/BCD Judgment	
September 2018		26 September 2018: Tribunal's determination under s 68(4) RIPA that MI5 unlawfully held BPD and	

Date	MI5's awareness of the non-compliance	Existing BPD/BCD Claim	IPA Claim
		BCD data related to the Claimant in the pre-avowal period	
October 2018	MI5 Executive Board Paper on "TE" compliance risks: "*The EB noted the scale of the challenges involving the [TE], endorsed the creation of a transformative programme … to address these risks, as well as supporting tactical mitigations already underway. The EB also formally agreed that we should brief IPCO …*" (MI5 11 March 2019 Letter §11; First Inspection Report §7.1.20) Paper stated: "*MI5 is unable to provide robust assurances to its oversight bodies*" (First Inspection Report §7.1.20)		
November 2018			27 November 2018: Permission granted on all other parts of IPA Challenge (in addition to the Part 4 EU law challenge), including ECHR grounds
February 2019	21 February 2019: Limited background provided by MI5 in a letter to IPCr (Generic Warrants Decision §7) 27 February 2019: MI5 briefs the IPCr orally about compliance risks which had been identified within the "TE" (Generic Warrants Decision §7)		4 February 2019: MI5 Witness makes witness statement asserting satisfaction that MI5's Handling Arrangements (taken with other matters) satisfy IPA requirements
March 2019	MI5 11 March 2019 Letter 18-22 March 2019: First inspection of the "TE"		

Date	MI5's awareness of the non-compliance	Existing BPD/BCD Claim	IPA Claim
	29 March 2019: First Inspection Report		
April 2019	1 April 2019: Note on the mitigations in place to deal with the compliance risks within the "TE" / Annex H 5 April 2019: Generic Warrants Decision 15–16 April 2019: IPCO further inspection of aspects of the TE 24 April 2019: MI5 letter to the Home Secretary 26 April 2019: IPCO Inspection Report: [Technology Environment] follow up inspection	16 April 2019: Tribunal's OPEN reasons for Determination	17 April 2019: Defendants indicate that a "*candour issue*" had arisen and that they will make application under Justice and Security Act 2013 s 6
May 2019	3 May 2019: MI5 letter to IPCO with summary of investigations into potential errors currently being progressed which bear on the "TE". Notes that "*knowledge of some compliance risk associated with [Areas 1 and 2] … was held by MI5 in 2016*". 8 May 2019: IPCO letter to MI5 concerning Areas 1 and 2 within the second technology environment. 9 May 2019: Written Statement of Secretary of State for the Home Department: "Investigatory Powers Act 2016: Safeguards Relating to Retention and Disclosure of Material: Written statement - HCWS1552". 15 May 2019: MI5 letter to IPCO concerning Areas 1 and 2 within the [Second technology environment ("TE2")]		
June 2019	Compliance Improvement Review concludes that "*MI5*	7 June 2019: Respondents inform	7 June 2019: Initial MI5

Date	MI5's awareness of the non-compliance	Existing BPD/BCD Claim	IPA Claim
	must ensure that all its data can be shown to be held in accordance with legal compliance requirements by June 2020"	the IPT, in a CLOSED letter, that the proceedings have concluded in relation to the ECHR and accordingly the identified compliance issues are not relevant to the extant proceedings. 11 June 2019: Respondents inform the Claimant that "*we have considered whether anything falls for disclosure in this case, and have concluded that nothing falls to be disclosed*".	Disclosure given 11 June 2019: Liberty reserves right to criticise MI5 Witness 17-21 June 2019: Hearing of the IPA Challenge insofar as based on the ECHR
July 2019			15 July 2019: Defendants disclose Compliance Improvement Review Summary 29 July 2019: Divisional Court's second judgment (addressing ECHR challenge to all challenged provisions of IPA)
October 2019	21 October 2019: Sir Brian Leveson appointed as IPCr 22 October 2019: the IPCr announced that "*MI5's use of the IT system in question is now fit for purpose*"		

APPENDIX 2 — TABLE OF ATTACHMENTS

Initial MI5 Disclosure		
1	A letter from MI5's Director of Policy, Compliance, Security and Information to IPCO (the "**MI5 11 March 2019 Letter**")	11 March 2019
2	IPCO's *Inspection Report* ("**First Inspection Report**")	29 March 2019
3	A new Annex H — Section II to the MI5 Handbook for Judicial Commissioners ("**Annex H**")	1 April 2019
4	The IPCr's "generic" decision on safeguards (the "**Generic Warrants Decision**")	5 April 2019
5	A letter from Sir Andrew Parker, Director General of MI5, to the Home Secretary (the "**Parker 24 April 2019 Letter**")	24 April 2019
6	A letter from the IPCr to Sir Andrew Parker	26 April 2019
7	IPCO's "*Inspection Report: [Technology Environment] follow up inspection, 15–16 April 2019*" (the "**Second Inspection Report**")	26 April 2019
8	A letter from "The Oversight and Errors Team" at MI5 to IPCO	3 May 2019
9	A letter from the IPCr to Sir Andrew Parker (the "**IPCO 8 May 2019 Letter**")	8 May 2019
10	A letter from "The Oversight and Errors Team" at MI5 to IPCO	15 May 2019
Other		
11	IPCr Advisory Notice 1/2018: 'Approval of Warrants, Authorisations and Notices by Judicial Commissioners'	8 March 2018
12	Interception of Communications Code of Practice	March 2018
13	Compliance Improvement Review Summary	June 2019
14	Home Secretary's written statement on Compliance Improvement Review	15 July 2019
15	Extract from *R (Liberty) v Secretary of State for the Home Department* [2019] EWHC 2057 (Admin), [2020] 1 WLR 243 [353]–[392]	29 July 2019
16	IPCr announcement: 'Compliance inspections of MI5 complete'	22 October 2019

APPENDIX 3 — PREVIOUS VERSIONS / DOCUMENTS REFERRED TO IN INITIAL MI5 DISCLOSURE

Document	Referred to / Existence apparent from
Report to Management Board of MI5 following January 2016 compliance review, which identified risk that "*data might be being held in ungoverned spaces in contravention of…policies*" and "*[another risk]*"	MI5 11 March 2019 Letter §10 [**B/1/70**]
Report in or before 2017 "*which raised concerns about [other potential] issues*"	MI5 11 March 2019 Letter §10 [**B/1/70**]
Operational Improvement Review	MI5 11 March 2019 Letter §20 [**B/1/71**]
MI5 "*[…register] in a standalone application*" (as relevant to the issues in this claim)	MI5 11 March 2019 Letter §20 [**B/1/71-72**]
Initial review of information management in the TE in 2015	MI5 11 March 2019 Letter §20 [**B/1/71-72**]
All reports of errors to IPCO and/or Home Office	MI5 11 March 2019 Letter §§22, 28(c) [**B/1/72-73**]
Form of words proposed for inclusion in MI5's warrants and "*accompanying detail*" for the Warrantry Handbook	MI5 11 March 2019 Letter §28 [**B/1/73**]
Version 1 of the First Inspection Report issued some time before 29 March 2019 (and any other versions of the First Inspection Report)	First Inspection Report is entitled in full: "*Inspection Report — MI5 (Audit of [the Technology Environment]) Version 2, issued 29 March 2019*". See also §9 "*Annex: list of updates*". [**B/2/74, 89**]
Letter from MI5 Director of Policy and Information to IPCr dated 21 February 2019	First Inspection Report §1.2 [**B/2/75**] Generic Warrants Decision §7 [**B/4/98**]
Legal paper on compliance risk, January 2016 (apparently also referred to as Legal Compliance Report to the Management Board)	First Inspection Report §§7.1.2–7.1.3 [**B/2/85**] Parker 24 April 2019 Letter §5 [**B/5/106**]
TE review, October 2016	First Inspection Report §§7.1.5–7.1.7 [**B/2/85**]

Paper on the TE risks, March 2017 (produced by the Information Central team for the Director of Strategy, four Directors and "*others*")	First Inspection Report §§7.1.8–7.1.9 [**B/2/86**]
Paper on compliance in the TE, October 2017 (produced for four MI5 Directors and "*others*")	First Inspection Report §§7.1.10–7.1.14 [**B/2/86**]
Documents setting out the TE Improvement Programme	First Inspection Report §§7.1.10 [**B/2/86**]
Management Board paper on compliance risk, including annex/attachments, January 2018 (produced by the Director of Policy and Information)	First Inspection Report §§7.1.15–7.1.19 [**B/2/86-87**] Generic Warrants Decision §3 [**B/4/97**] Annex is referred to in Parker 24 April 2019 Letter §6 [**B/5/107**]
Data store error letter / Report to IPCO dated 4 March 2019	First Inspection Report §7.1.17 [**B/2/87**] Generic Warrants Decision §10 [**B/4/99**]
MI5 Handbook for Judicial Commissioners, May 2018 (containing Ml5's summary of its handling arrangements for categories of warranted material)	First Inspection Report §7.1.18 [**B/2/87**]
MI5 corporate risk register (including as at January 2018, or such other time as the risk was elevated to "*RED*", and beforehand)	First Inspection Report §7.1.19 **[B/2/87]**
The results of any review conducted by MI5's Audit Risk and Assurance Committee in June 2018 (or at such time as the review was carried out)	First Inspection Report §7.1.19 [**B/2/87**]
Executive Board paper on the TE compliance risks, October 2018	First Inspection Report §§7.1.20–7.1.22 [**B/2/87-88**] Generic Warrants Decision §4 [**B/4/97-98**]
MI5's summary of its planned mitigations shared with the IPCr following the 22 March 2019 meeting	First Inspection Report §8.2 [**B/2/88**]
MI5's "form of words" to describe the risks of the TE and proposed mitigations	First Inspection Report §8.2 [**B/2/88**]
The "*Director General communication*"	Annex H §44 [**B/3/95**]

The guidance "*which requires users to seek the deletion of any LLP material they do encounter*"	Annex H §52 [**B/3/95**]
The "*[register]*"	Annex H §59 [**B/3/96**]
In relation to the new Annex H to the MI5 Handbook, April 2019: (1) IPCO's request to MI5 for "additional information" (2) MI5's response Any subsequent versions of Annex H to the MI5 Handbook	Generic Warrants Decision §28 [**B/4/102**]
Any report or other document containing the results of any inspection of MI5 carried out in May 2019	Letter from the IPCr to Sir Andrew Parker dated 26 April 2019 p 2 [**B/6/110**]
All documentation (such as the "*new policy and supporting guidance on the use of the [TE]*" and/or the "*[TE] Policy to be introduced*", other policies, summaries, IPCO updates, advice, etc.) produced or amended in implementing IPCO's recommendations or otherwise responding to the First Inspection Report, the Second Inspection Report, the Generic Warrants Decision or otherwise responding to reports or findings of IPCO in relation to TE1 and TE2	Second Inspection Report §3 [**B/7/113-115**] Annex H §§38, 48, 63 [**B/3/94-96**]
Accreditation of the specific IT environment in 2010	Compliance Improvement Review §3 [**B/13/273**]
2011 review that made recommendations including implementation of a retention and deletion policy	Compliance Improvement Review §3 [**B/13/273**]
May 2013 MI5 Management Board paper setting out "*serious information management risks*"	Compliance Improvement Review §5 [**B/13/273**]
Documents containing the "*concerns*" expressed by legal advisers "*about the robustness of the wider process*"	Compliance Improvement Review §10 [**B/13/274**]

MI5 Protocol governing relations with the Home Office	Compliance Improvement Review §12 [**B/13/274**]
MI5 Risk Register (relevant entries from at least 2010 onwards, including from October 2016 onwards when the compliance issues were flagged as "*red*")	Compliance Improvement Review §16 [**B/13/275**]
Any independent verification (or other evaluation) of the results of the change programme recommended, if and to the extent that MI5 has implemented this	Compliance Improvement Review p 6 (Recommendation 5) [**B/13/278**]
All minutes of MI5 Executive and MI5 Management Board meetings that mention the TE or the risks identified from 2010 onwards	Compliance Improvement Review p 6 (Recommendation 7) [**B/13/278**]
Any quarterly reports produced by the MI5 Legal Director to the Home Office Permanent Secretary and MI5 Director General, as recommended to be produced	Compliance Improvement Review p 7 (Recommendation 11) [**B/13/279**]