**IN THE INVESTIGATORY POWERS TRIBUNAL** **Claim No IPT/20/01/CH**

**B E T W E E N**

**(1) LIBERTY**
**(2) PRIVACY INTERNATIONAL**

**Claimants**

**- and -**

**(1) SECURITY SERVICE**
**(2) SECRETARY OF STATE FOR THE HOME DEPARTMENT**

**Respondents**

---

# CLAIMANTS' SKELETON ARGUMENT FOR THE SUBSTANTIVE HEARING LISTED TO BE HEARD 25 TO 29 JULY 2022

---

**References to the hearing bundle appear in the following format: "[vol/tab/page]"**
**References to the core bundle appear in the following format: "[Core/tab/page]"**
**References to witness statements are in the form "MI5 A1 §*" / "Hirsch 1 §*" etc**

**Certain issues are developed further IN PRIVATE. The Claimants have not served a separate IN PRIVATE skeleton argument. The existing materials IN PRIVATE set out the Claimants' position.**

## A SUMMARY

1 This skeleton argument is designed to introduce the documents and issues before the Tribunal. It will be supplemented by closing submissions once the oral evidence has been heard and opened up.

2 The Investigatory Powers Act 2016 ("**IPA**") and the Regulation of Investigatory Powers Act 2000 ("**RIPA**") provide for basic statutory safeguards for the acquisition and holding of personal data. These proceedings concern the Security Service's ("**MI5's**") systemic and systematic non-compliance, over an extended period, with these basic safeguards, and equivalent and related non-statutory arrangements (including for obtaining bulk communications data ("**BCD**") and bulk personal datasets ("**BPD**") and their handling).

3 MI5 continued to retain personal data, including "*a cut or selection*" from BPDs[1], in circumstances where MI5's technology environments had been known for years to have serious compliance faults – in MI5's own words, to be "*ungoverned spaces*" (January 2016, MI5 Legal Paper on Compliance Risk **[C2/54/11]**) and *"akin to the 'wild west' places [sic]"* (February 2017, 'TE Issues Minute' **[C2/65A/2]**). The holding of such data represents a serious interference with individuals' privacy, contrary to domestic law and without justification. The genesis of this breach was the creation and then continued use, over a significant period, of inadequate systems for data retention, review and destruction ("**RRD**"). MI5 has not in practice observed the central safeguards under:

3.1 the s.8(4) RIPA regime and associated Code of Practice;

3.2 IPA Part 6 Chapter 1 (at least); or

3.3 the procedures it devised for BCD and BPD that it obtained under s.94 Telecommunications Act 1984 ("**TA**") warrants or otherwise, contained in Handbooks designed to secure Article 8 European Convention on Human Rights ("**ECHR**") compliance,

relating to (i) access control for material obtained under warrants; (ii) copying of material obtained under warrants; (iii) RRD of operational data; and (iv) identification and RRD of lawyer-client communications subject to legal privilege.

---

[1] E.g. Report of Error Identified by MI5 (A2 Exhibit A22) §4 **[C4/196/1]**.

4 The existence of these defects (if not, perhaps, the full implications) was known to MI5 from an early date. More to the point, from an early stage it was identified that the unlawful holding of such data on such defective systems would produce or would risk producing potentially very serious consequences for oversight, warrantry and compliance with the law.

5 And, yet, MI5 repeatedly chose not to inform the Investigatory Powers Commissioner ("**IPCr**") or Judicial Commissioners of these serious failings until February 2019, which MI5 contends (to an implausible degree) was because it did not properly understand the problems with its own technology environments. Fulford LJ (the IPCr at that time), in light of the disclosure made to him in February/March 2019, considered MI5's position to have been "*inexcusable*" *and* "*outrageous*" **[C3/167/2]**. Even then the Investigatory Powers Commissioner's Office ("**IPCO**") was not fully informed; Fulford LJ was informed about the systemic failings in TE2 Area 1 and Area 2 only some months later: see the IPCO 8 May 2019 letter **[C3/174]**. Worse still, MI5 did not inform this Tribunal of the issues in ongoing litigation brought by Privacy International concerning the handling of bulk data (i.e. the "**Existing BPD/BCD Claim**"), instead actively relying before this Tribunal on its alleged full compliance with Handling Arrangements in relation to BPD and BCD, despite that litigation running in parallel since 2015. The IPT was seriously misled. And MI5 did not provide full and frank disclosure to the Secretary of State whose authorisation for warrants it was requesting. In turn, the Secretary of State was content to rely upon and trust the incomplete and inaccurate description it was obtaining from MI5 and made no material inquiries as to the extent of MI5's non-compliance. The result of this state of breach, and the accompanying systemic non-disclosure, is that (likely) hundreds of warrants or statutory authorisations were issued and implemented unlawfully.

6 Once one appreciates that evident *breaches* of legal requirements are routinely euphemistically described as "compliance risks" or such like in the Respondents' materials (terms the appropriateness of which the Tribunal is invited to focus upon in each document in which they are used, there being in most instances no sensible basis to contend that requirements have not been breached), all the evidence points to deliberate and protracted non-disclosure (or, in the case of disclosure to the Secretary of State, in

the later periods inadequate or incomplete disclosure) by MI5 of such serious breaches to:

6.1 MI5's oversight commissioners (the Interception of Communications Commissioner ("**IOCC**"), Intelligence Services Commissioner ("**ISC**"), and lately the IPCr);

6.2 the Secretary of State, in particular when: (a) exercising s.8(4) RIPA and other warrantry and analogous powers before the commencement of the IPA on his/her own; and (b) later, when acting as the "first lock" under the replacement IPA provisions;

6.3 Judicial Commissioners, acting as the "second lock" under the scheme of the IPA to approve key warrants formerly governed by RIPA (BCD/BPD warrants, equipment interference warrants etc);

6.4 this Tribunal, notably in the original *Liberty* proceedings (concerned with the legality of use of s.8(4) RIPA powers), proceedings which also produced false/misleading facts which the ECtHR considered in *Big Brother Watch v United Kingdom* (Application Nos 58170/13, 62322/14, 24960/15, 25 May 2021) ("***BBW***") and in the Existing BPD/BCD Claim;

6.5 other Courts and Tribunals, in particular in the context of disclosure, including in (i) criminal courts (notably those handling terrorism charges, particularly those in the Terrorism List) in the preparation of pre-trial disclosure and consideration of PII issues, (ii) civil litigation (such as the *Belhaj* case), and (iii) inquests/inquiries/reports, notably those in relation to terrorist attacks, such as the Litvinenko Inquest and then Inquiry (which reported in 2016), or the ongoing inquiry into the Manchester Arena bombing (commenced on 22 October 2019); and

6.6 Parliament and Parliamentary oversight committees (i.e. the Intelligence and Security Committee ("**ISC**")), particularly in the course of debating the safeguards required in the IPA in 2015 and 2016, a debate which appears to have occurred

without highly germane material being made available. As explained in the Commons Library briefing, the third of the key issues raised by the Bill/IPA was:[2]

> *"the trust that should be placed in the agencies and Government not to abuse powers that have the potential to be deeply intrusive."*

Such non-disclosure started at the latest (and that would be a conservative assessment) in 2012 and continued until 2019.

7 The illegality of MI5's approach is admitted, at least in part and for a period, by the Respondents in these proceedings. However, the nature, extent, scale and effect of the breaches remain in dispute. No shortcomings on the part of the Secretary of State, once informed of the problems that existed, are admitted. The important function of these inquisitorial proceedings is to allow fact-finding light to be shone into these ungoverned spaces, to understand the legal implications that should follow from such systemic breaches, and to address what these systemic failures, most obviously on the part of MI5 but also on the part of the Secretary of State (current and former), demonstrate about whether the schemes that permitted such circumstances are really fit for purpose and effective in practice. The Claimants' core case is that the conduct here shows that the arrangements for safeguarding data are not effective in practice and have been, apparently deliberately, breached for many years.

8 Astonishingly, after this unprecedented catalogue of protracted and serious failures (failures which were they to occur in any other regulated context would produce a national scandal, with at least disciplinary and other consequences at the most serious end of the scale), the Respondents' primary position is to invite the Tribunal to note (some of) the breaches of the law but grant no relief, or nothing but "*limited declaratory relief*" **[A1/11/31] [Core/7/31]** on the basis that the *"purpose of the warrantry provisions of the IPA (and RIPA) is not to disentitle the Intelligence Agencies from doing their vital work"* **[A1/6/18] [Core/5/18]**. The Tribunal should, respectfully, decline that invitation. The Intelligence Agencies' 'entitlement' is only to discharge their functions lawfully, faithfully applying the safeguards required by Parliament. The importance and difficulty of their job is already amply recognised by the heavily modified regulatory context in

---

2 https://commonslibrary.parliament.uk/research-briefings/cbp-7518/

which they operate, with the conferral of extraordinary powers accompanied by reduced safeguards (when compared to other actors, public or private).

9 But it cannot be the law that when the Intelligence Services flout even these carefully tailored and reduced safeguards they should be immunised from legal consequence because of their functions. If this Tribunal's response to such unlawfulness was that there are no legal consequences, that would not only be legally unprincipled (the agencies are governed by law), but it would also most starkly demonstrate the failure of the oversight system and the practical futility of litigation in this Tribunal. The statutory protections would be meaningless – capable of being breached with impunity – if it were sufficient to rely upon the breaches having been concealed and so only discovered after the event, and having occurred in the national security context, as an excuse. Instead, the Tribunal is asked to grant the declaratory, quashing and remedial relief set out at Amended Grounds of Claim ("**GoC**") §156 **[A1/5/59] [Core/4/59]** and to declare that the relevant statutory schemes, by reason of the demonstrated ineffectiveness of their safeguards in practice, were and are incompatible with the ECHR.

10 This hearing is listed for five days, with the first two days intended to be in OPEN. There will be cross-examination of Witness A and Witness C in CLOSED. The Tribunal has directed that there must be arrangements in place to "*enable rapid transcription and gisting of the evidence*" to the Claimants. The Tribunal has indicated that it will receive closing submissions in writing.

## B FACTUAL BACKGROUND

11 The following narrative is the best the Claimants can construct from the redacted and incomplete materials that have been presented to them in a highly fragmented (and non-chronological) fashion, largely as result of the tireless work of Counsel to the Tribunal to open material up or secure gists. Documents that should never have been put in CLOSED have been opened up; gists that should always have been provided have been provided belatedly. Fields of disclosure that were always of relevance have been belatedly investigated. Because of the chronology of these disclosures, the important revelations such documents contain are often unaddressed by the witness evidence filed by the Respondents, much of which pre-dates the disclosure of such documentary materials and thus the witness evidence does not address the obvious questions the

materials raise. Save where witness evidence is available and on point, the Tribunal will have little choice but to proceed from what is evident from the documents and (in the absence of evidence) make the inferences that such documents support. These documents will doubtless need close consideration in CLOSED.

12 That being so, the picture built from the OPEN materials is an arresting one; and one that calls at every stage for candid explanation by the Respondents, an explanation that is in many respects lacking.

## (1) Events prior to the briefing of the IPCr of compliance errors relating to TE

### *(a) 2010 to 2013*

13 Systemic compliance risks and/or instances of non-compliance in MI5's data holding systems were first identified as early as 2010. An MI5 Management Board Paper prepared for discussion on 16 April 2010 stated that "*in MB [REDACTED] we identified that there were '... very significant deep rooted Information Assurance*[3] *risks for the Service, (which) [a department] (was) not currently staffed to address'.*"[4] It noted that "*[c]urrent priorities are to reduce the risks of* intelligence failure *and* compliance failure *to acceptable levels, by ensuring that users can – with a high degree of confidence – retrieve information relevant to investigations and disclosure exercises where necessary.*"[5] The MI5 Management Board Minutes recorded that "*[t]he Board recognised the significant risks being carried in Information Assurance*", with the matter raised as early as December 2009; the issue was described as a "*major residual risk*" requiring "*a culture shift*".[6]

14 On 13 September 2010, "*[A Director]*" issued a paper, 'Recent Compliance Failures in [a department]', which raised a number of issues relating to the handling of data.[7] The "*Key points*" included:

---

3 "*Information Assurance*" is defined as "*the practice of identifying, assessing and mitigating risks to our information assets*": Management Board Paper (CIR/3), Annex A §2 **[C1/6/5]**.

4 Management Board Paper (CIR/3), §1 **[C1/6/2]**.

5 Management Board Paper (CIR/3), §2 **[C1/6/2]**.

6 Management Board Minutes (CIR/2), p.1 **[C1/5/1, 5]**.

7 [REDACTED] Minute: Recent compliance failures in [a team] (CIR/9) **[C1/11/1]**; [a department] and Compliance (CIR/9) **[C1/12/1]**; CIR §17 **[C4/185/5]**.

14.1 "*[a department]'s principal vulnerability is some new and serious compliance error and no strategic compliance framework in place to help mitigate the risk*";

14.2 "*Underlying this risk is, in some areas of [a department] activity, an imperfect understanding of current processes and the scale of risk they entail. This manifests itself at various levels, including among senior managers who may have little first-hand experience of the detail of current working practices*"; and

14.3 "*[a team] have traditionally held the lead for giving advice on warrantry / authorisation compliance (with advice from [a team]). [REDACTED] Whoever's fault indeed it was [REDACTED] we need to ensure that in future relevant advice is sought at the appropriate time, shared with all those who need to know and acted on.*"

15 The paper set out recent compliance failures which had been reported to the IOCC and ISC, "*as well as emerging findings about a further compliance breach in [a team]*", which it is assumed had not been so reported.[8] It identified six separate classes of compliance error, each of which was said to be different "*in nature, cause and scale*" (§3)[9] and that "*[s]ome at least of the causes of errors derive from broader trends in [a department] activity*" (§5)[10]. The errors themselves are entirely redacted in OPEN.

16 On 25 October 2010, a discussion paper produced within MI5's "*[a team]*" identified the "*controls required to ensure that the access to and handling of [the data to which the [a team] has access] is appropriate*."[11] Annex B set out a "*Suggested model for [TE2 Area 1] governance*"[12] and Annex C set out a "*Suggested method for cleansing the [TE2 Area 1]*"[13] (emphasis added).

17 It is therefore apparent that from at least 2010: (i) there were widespread compliance problems with MI5's data holdings and their handling; and (ii) so far as is discernible from the redactions, such failings required data to be "cleansed" from TE2 Area 1; and (iii) MI5 was aware of the data held in TE2 Area 1 and that it required "*cleansing*".

---

8 [a department] and Compliance (CIR/9) **[C1/12/1]**.
9 [a department] and Compliance (CIR/9) **[C1/12/2]**.
10 [a department] and Compliance (CIR/9) **[C1/12/3]**.
11 The scope of [a team] compliance (RFI/1) **[C1/13/1]**.
12 The scope of [a team] compliance (RFI/1) **[C1/13/6]**.
13 The scope of [a team] compliance (RFI/1) **[C1/13/7]**.

18 The TE is described by the Respondents as "*an MI5 technology environment*" (it appears to be explained in further detail in CLOSED in MI5 A2 §§17-41 **[B/2/3-5] [Core/9/3-5]**). The TE was granted interim accreditation in 2010 as a "*[system that holds restricted information]*." The accreditation process identified a number of "*HIGH*" rated risks.[14] All of the risks are redacted in the '[TE] Residual Risk Register', which states: "*[The table includes a risk related to the lack of policies that mandate how the TE is utilised, managed and supported]*."[15] In short, it was an ungoverned space built and then operated without thought as to the legal controls its existence and use required.

19 On 7 March 2011, "*[a department]'s [compliance group]*" had its first meeting.[16] The paper, '[a team] RIPA Compliance Update', noted that since the previous month there had been "*two more errors and three near-misses*"[17] (none of which has been disclosed or explained to the Claimants, despite the Claimants' request[18]).

20 In May 2011, "*[a department]'s Compliance Group*" issued a report, '*Audits and Investigations into [a team] compliance incidents of summer 2010 and emerging conclusions and recommendations.*' The report assessed the compliance of a number of systems on the TE, including "*TE fileshares*" (later known as "*fileshares*"). When the report was issued, the assessment of "*TE fileshares*" was incomplete, with its RAG (i.e. "red/amber/green") status yet to be determined.[19]

21 On 21 October 2012, there was a security audit of TE "*to determine what the [TE] is being used for today, what exists within the [TE] and practices that are followed by [TE] users*". The 'TE Security Review' contained "*ten findings in total that are risk-rated*", all of which are redacted.[20]

---

14 CIR §19 **[C4/185/6]**.
15 [TE] Residual Risk Register (CIR/11) **[C1/15/4]**.
16 CIR §21 **[C4/185/6]**.
17 [a team] RIPA Compliance Update (CIR/12) **[C1/16/2]**.
18 See paragraphs 20 and 23 in the Claimants' second letter to the Respondents dated 8 February 2022 **[D2/199/416-417] [Core/23/6-7]**.
19 CIR §23 **[C4/185/6-7]**; Audits and investigations into the [a team] compliance incidents of summer 2010 and emerging conclusions and recommendations ([A]2 doc 3) **[C1/17/15]**.
20 [TE] Security Review 2012 (CIR/13) **[C1/21/3]**.

22 In 2012, the TE was re-accredited as a "*[restricted] system*". The 'TE Security Case' noted that there were "*'HIGH' risks as a result of [REDACTED] as well as various other risks including [REDACTED]*."[21] All of the risks related to the TE are redacted.[22]

23 As early as 2012, MI5 has been aware of RRD compliance risks and/or instances of non-compliance in TE2 Area 2 (in addition to the problems in TE2 Area 1 above). TE2 is another technology environment, which appears to be described in CLOSED in further detail in MI5 A2 §§42-47 **[B/2/5-6] [Core/9/5-6]**. A 'Minute' prepared by "*[a department]*" in 2012 recorded that "*[i]nitial investigation has revealed that numerous individuals across the Service are saving information in the [areas within TE2 Area 2] instead of, or in addition to, [REDACTED]*" and this gave rise to the risk that "*corporate information is being stored outside the 'searchable framework'. Hence, it is possible that information is not being seen by those with a need to know (including the [REDACTED] team).*"[23] It also noted that "*no rules have been historically applied to [TE2 Area 2]*" and that TE Area 2 was "*being mis-used to: Store documents indefinitely which should ideally [be stored elsewhere]; share files which should be restricted. Issues: [REDACTED]; and an inability to determine which files can be safely deleted*."[24]

24 In 2012, the 'general [team] Data Retention Policy' was superseded by a system-specific data retention policy, which identified the "*[risk]*" arising from "*[a type of data] stored in [areas]*." The policy recommended that, as a mitigation, "*structures and processes must be put in place to ensure all this data is accounted for and can be routinely deleted in line with policy*."[25] The policy does not appear to have been disclosed in OPEN. It is therefore not known whether the "*[risk]*" identified was in relation to TE Area 2.

25 In May 2013, there was a MI5 Management Board meeting which appears to have discussed the RRD problems with TE and perhaps beyond. But no minutes of this Management Board meeting have been disclosed; the Claimants know of this meeting and its content from oblique references in later documents summarised below.

---

21 CIR §25 **[C4/185/7]**.
22 RMADS – [TE] Security Case 2012 (CIR/14) **[C1/22/6]**.
23 [Minute] **[C1/23/1]**.
24 [Minute] **[C1/23/2, 6]**.
25 CIR §28 **[C4/185/8]**.

26 A flavour can perhaps be gleaned from the Management Board Paper from June 2013, which provided an update from the 'Information Management Transformation Programme' on "*information risks*". The "*plenty of anecdotes of problems*" are redacted (§7). However, the paper noted: "*we are in the worst possible position on information discovery. [staff] searching for information…may well fail to find key [information]…*" (§8).[26] The need for a cultural shift is also noted: "[i]*t is clear that our organisational culture and behaviours do not make good IM* [information management] *practice a high enough priority…the overall picture is bleak*" (§3).[27]

27 By letter dated 14 August 2013, Sir Anthony May, the then IOCC, requested that each of the law enforcement and intelligence agencies which undertake warranted interception of communications under Part I Chapter 1 of RIPA under IOCC governance should provide him with "*full and systematically organised information about the retention, storage and deletion of the product of interception.*"[28] Sir Anthony asked for the information to be provided "*for all classes of interception material ... with particular reference to every generic database in which intercepted material is for a time stored.*"[29]

28 On 24 October 2013, the MI5 Deputy Director General responded. The OPEN version of the letter does not identify TE, TE Area 1 or TE Area 2, or any compliance concerns with RRD in those systems, notwithstanding the compliance risks and/or instances of non-compliance identified between 2009 to 2013 and summarised above. Indeed, the Respondents confirmed to the Claimants that "*MI5 did not inform Sir Anthony May about the RRD issues with TE/TE2.*"[30] So, in the face of an explicit request for this very type of information, MI5 failed to disclose the nature and implications of known RRD problems in TE and TE2 Areas 1 and 2. No explanation of this is given in the Respondents' evidence. The most reasonable inference seems to be that this was the beginning of a pattern of deliberate non-disclosure to oversight bodies in relation to these areas.

---

26 Management Board Paper: IMTP Update (RFI/3) **[C1/24/2-3]**.
27 Management Board Paper: IMTP Update (RFI/3) **[C1/24/2]**.
28 Letter from Sir Anthony May (May/1) **[C1/26/1]**.
29 Letter from Sir Anthony May (May/1) **[C1/26/2]**.
30 Letter from the Respondents to the Claimants dated 16 September 2021 **[D2/130/284] [Core/21/1]**. This letter was sent in response to the Claimants' letter to the Respondents dated 9 September 2021, which requested information on whether MI5 informed Sir Anthony of the TE/TE2 RRD issues in light of this not being apparent from the Respondents' evidence or disclosure (which indeed was given late on this issue, in August 2021) **[D2/127/280-281] [Core/20/1-2]**.

29 Later in the same month, on 8 October 2013, the MI5 Director General, Andrew Parker, gave a speech about the proposed Investigatory Powers Bill, stating:[31]

> "I welcome this reform and the enhanced confidence it can give to the public. The fact that much of this oversight necessarily happens out of public hearing leads some commentators to mistake silence for weakness. That is plain wrong. From my experience, I know that all of the bodies I have mentioned and their supporting staff pursue their responsibilities very fully, professionally and conscientiously."

30 On 16 December 2013, the Head of Oversight of the National Security Unit ("**NSU**"), prepared a note for the Home Secretary ahead of a meeting between Sir Anthony May, the Home Secretary and himself on 18 December 2013.[32] The note recorded that one of Sir Anthony's "*key findings*" following an inspection of the Home Office's warrantry processes on 3 December 2013 was that "*MI5 have [compliance problems] where they are retaining material for too long and deletion is not always effected.*"[33] Given the Respondents had not informed Sir Anthony about the TE/TE2 issues, it is apparent that the issues which were in fact reported to Sir Anthony extended to areas outside TE/TE2. Also, by this stage at the latest, the Home Secretary was apprised of at least some of MI5's compliance issues and/or non-compliance with RRD requirements. The Claimants requested that the Respondents disclose any response from the Home Secretary. By email of 8 December 2021, they stated: "*The Respondents can confirm that they have undertaken a search for any response from the Home Secretary to the Sir Anthony May Briefing and that no further material falls for disclosure.*" **[D2/186/388]** No explanation was provided of (1) what, if any material was identified; and (2) if any material was identified, why it does not fall to be disclosed.

31 On 19 December 2013, Sir Anthony wrote to Andrew Parker, MI5 Director General. The letter noted that "*certain themes*" had emerged from Sir Anthony's review of RRD of intercept material (most of which are redacted in OPEN) and contained the following summary of his concerns:[34]

> "To summarise:

---

31 <https://www.mi5.gov.uk/news/the-enduring-terrorist-threat-and-accelerating-technological-change#sthash.xo0XeJFf.dpuf>

32 Note to Home Secretary: Annual Bilateral with Interception Commissioner **[C1/28A/1]**.

33 Note to Home Secretary: Annual Bilateral with Interception Commissioner **[C1/28A/2]**.

34 Letter from Sir Anthony May to Director General (May/3) **[C1/29/8, 10]**.

MI5 appears to have [multiple systems] which retain intercepted material for various retention periods and there seems to be illogicality about the retention, storage and destruction of intercepted material. ...

(iv) MI5 acknowledges that the interception landscape needs to be tidied up and recognises that there are some difficulties with regard to compliance with the section 15 safeguards particularly around retention periods and deletion of intercept material.

(v) At the time of the inspection, MI5 were in the process of mobilising their Information Management Transformation Programme (IMTP), a long term complex programme of work to ensure that MI5 manages its information properly.

(vi) I recognise that it would be totally impractical to suggest that MI5 significantly adjust their current systems in the interim. ...

(vii) Although I regard some of the retention periods to be excessively long and some of the deletion process to be inadequate, on the face of it, MI5 does not appear to hold large amounts of untargeted intercept material. The vast majority has been collected because it relates to a warranted subject of interest or is relevant to a specific investigation and as such the nature of the intercept material is not untargeted. Nevertheless, MI5 still needs to move towards a position of full compliance with Section 15 of RIPA."

*(b) 2014*

32 On 24 March 2014, the TE was re-accredited as a "*[restricted] system*" notwithstanding that "*[A number of risks were noted]*"[35] and the risks (all of which have been redacted) were assessed as "*HIGH*" and "*MEDIUM-HIGH*".[36]

33 A report prepared for the MI5 Management Board recorded the following risk: "*[RISK: Risk of staff misusing access]*".[37] This is understood to be referring to risks relating to the extent to which the material is disclosed or to whom access to the material is given. It also recorded a further risk: "*[Risk 1]: MI5 is unable to create, store or retrieve information in a secure, legally compliant and accessible way due to the inadequacy of information handling application*" ("**Risk 1**"), which was rated "*AMBER*".[38] A second report recorded that Risk 1 remained "*AMBER*".[39]

34 A 'Minute' was prepared on 18 November 2014, which is entirely redacted in OPEN. However, the gist states as follows: "*[The document identifies a risk of incorrect or*

35 CIR §31 **[C4/185/9]**.
36 [TE] RMADS Risk Acceptance Statement #002 (CIR/15) **[C1/31/2]**.
37 REDACTED] 2014/2015 Management Board [REDACTED] Performance Report (CIR/16) **[C1/32/10]**.
38 CIR §33 **[C4/185/9]**; REDACTED] 2014/2015 Management Board [REDACTED] Performance Report (CIR/16) **[C1/32/11-12]**.
39 CIR §34 **[C4/185/9]**; [REDACTED] Performance Report for Management Board [REDACTED] 2014/2015 (CIR/17) **[C1/34/8-9]**.

*partial disclosure in legal proceedings. There are issues with data within MI5 that include a failure to link some data to a searchable record, and that the record, retain and delete policy is inconsistent and is not applied to much of MI5's data, in that a vast amount of data is kept that is not needed. ...]*"[40] (emphasis added). These are fundamental breaches as:

34.1 the problem was the lack of control/centralisation of data holdings, such that RRD policies were not being applied to "*much of MI5's data*" and a "*vast amount of data*" was being kept in breach of RRD policies; and

34.2 MI5 was identified as being unable to comply with its obligations in legal proceedings (whether before the IPT, in inquests, in criminal proceedings, in judicial reviews or otherwise).

35 The Compliance Improvement Review ("**CIR**") noted that the "*first major compliance issue with the [TE]*" was identified in 2014, and that subsequent internal reviews recorded that there were three major causes: (i) "*[A failure to create a type of record on another TE]*; (ii) "*A failure to apply review, retention and disposal (RRD) policy to the repository of data on the [TE]*"; and (iii) "*A failure to understand what data was held on the [TE].*"[41]

36 On 26 November 2014, the Interception of Communications Commissioner's Office ("**IOCCO**") Inspection Report was published. The report noted that the IOCC had been provided with a briefing on RRD arrangements. It stated that MI5 had prioritised (amongst other things) (i) "*[Data] – automated review retention and disposal has now been built into the [REDACTED]. By the end of 2014 MI5 anticipate that all [material] older than [REDACTED] will have been deleted*"; and (ii) "*[Material] – compliance is difficult due to [reasons]. MI5 is now compliant in relation to deletion of all material acquired in error.*"[42] It also noted that the IOCCO had been briefed on "*matters arising from the [error] and are satisfied that all material has now been destroyed.*" It appears that the IOCCO was not notified of any RRD compliance risks or non-compliance relating to TE, TE2 Area 1 or TE2 Area 2. The MI5 Deputy Director General provided IOCCO with further information following the inspection on 23 December 2014. An

40 Minute (MI5 Core Doc 1) **[C1/38/1]**.
41 CIR §35 **[C4/185/9-10]**.
42 IOCCO Inspection Report (May/4) **[C1/39/11]**.

updated spreadsheet enclosed with the letter, detailing the systems on which intercept material is stored, is fully redacted.[43]

*(c) 2015*

37 In 2015, the MI5 Management Board Performance Report 2014/15 was published. Having noted that a RRD policy had been reviewed, it stated: "*This marks a significant improvement in our ability to comply with [particular] handling arrangements, although there is still a significant way to go to achieve full compliance on [a type of data] RRD, an issue which is compounded by increasing focus on RRD issues by Commissioners and Government*" (emphasis added).[44] Risk 1 remained "*AMBER*". It stated "*there [was] a growing issue [REDACTED] arising from the Service acquiring and holding more data [REDACTED] which was considered by the [data review panel] and mitigations are being explored.*"[45] A "*further MI5 report*" was issued in 2015 and discussed by MI5 around the same time. Risk 1 was rated "*AMBER*".[46]

38 A "*further report*" produced in 2015 was discussed by the MI5 Management Board. The report proposed a new corporate risk: "*[Risk 3]: There is a risk that as a result of its systems, working practices or individual errors, MI5 is held to be failing to comply with its statutory obligations attracting adverse criticism or rulings from the Investigatory Powers Tribunal and/or oversight bodies (current or future) leading to substantial legal and/or reputational damage. This applies especially, but not exclusively, to information handling and record keeping*" ("**Risk 3**").[47]

39 In March 2015, Sir Anthony's 'Report of the Interception of Communications Commissioner' was published. Under the heading "*Retention, Storage and Deletion*", it noted that the IOCCO made 22 recommendations in 2013 and 11 recommendations in 2014 for interception agencies to review or shorten their retention periods and/or destroy intercepted material and/or related communications data where there was no persuasive justification provided for its ongoing retention (§6.64). It also stated:

---

43 Letter from Deputy Director General to Sir Paul Kennedy (May/5) **[C1/40/2]**.
44 Management Board Performance Report 2014/2015 (MI5 Core Doc 2) **[C2/41/4]**.
45 CIR §36 **[C4/185/10]**; Management Board Performance Report 2014/2015 (MI5 Core Doc 2) **[C2/41/8]**.
46 CIR §38 **[C4/185/10]**; Management Board Performance Report 2014/2015 (MI5 Core Doc 3) **[C2/42/9]**.
47 CIR §40 **[C4/185/11]**; Management Board Performance Report 2015/2016 (MI5 Core Doc 4) **[C2/43/4]**.

> "I can report that all of the recommendations were accepted by the interception agencies. The large majority have already been fully implemented. This has caused a significant amount of intercepted material and related communications data to be destroyed, and in some instances entire systems have been decommissioned. In other cases the maximum retention periods have been halved. Those agencies which have not yet managed to implement the recommendations in full are waiting on significant technical changes to be made to IT systems. I have made clear that future retention and destruction policies should not be dependent on broad assumptions about the value of the material or data. Reviews should be conducted regularly, informed by profiling exercises to ensure that the retention and destruction policies are not arbitrary. I welcome the progress made and my office will continue to monitor this area of the process." (§6.65)[48]

40 The Management Board Performance Report 2015/16 recorded that MI5's priorities were "*scoping the scale of the RRD challenge (with an RRD action plan agreed).*"[49] As to Risk 1, it noted that there were risks that (i) information was not disposed of appropriately; (ii) MI5 failed to deliver a long-term strategy for handling information; and (iii) poor compliance and information management practice would result in a loss of the confidence of oversight bodies. Risk 3 was included but not scored. It also stated that "*the Board acknowledged that a cultural change towards compliance was needed to make staff realise that it is a critical element of their job*" (§11).

41 On 13 October 2015, a 'Minute' was prepared for "*[two MI5 directors]*" concerning an "*Update on [TE]*". It recorded that "*[Information Risks were identified in 2014 in relation to legal proceedings. Immediate steps were taken to establish and mitigate the wider litigation risk]*" and "*[Work was commenced on an improved information register. The work focussed on the TE first]*."[50] It also stated that the "*legal risk*" from information holdings in the TE had been reduced but not eliminated and that the "*remaining legacy risk is naturally deteriorating*."[51]

42 The Management Board Performance Report 2015/16 recorded that Risk 3 "*now has a fully fleshed out set of subsidiary risks (arising from the risks articulated in the recent Compliance paper to MB), as well as a [REDACTED] RAG score (currently RED)*." It is apparent that that at least by this stage these "risks" had been identified by MI5 at the highest level. The risk was allocated to "*[the legal department]*".[52]

---

48 Sir Anthony May, "*Report of the Interception of Communications Commissioner*" **[C2/44/16]**.
49 Management Board Performance Report 2015/2016 (MI5 Core Doc 7) **[C2/48/6]**.
50 Minute (MI5 Core Doc 8) **[C2/49/1]**.
51 Minute (MI5 Core Doc 8) **[C2/49/2]**.
52 Management Board Performance Report 2015/2016 (MI5 Core Doc 11) **[C2/52/9]**.

43 Stepping back, it is impossible to see how this state of affairs was consistent with the demands of s.8(4) of RIPA or other warranting/authorisation safeguards; still less how it could begin to be consistent with the forms of warrantry under discussion in the Investigatory Powers Bill (as eventually adopted in November 2016 and commenced on 21 May 2018). This form and level of non-compliance always required disclosure on the application for the warrant.

*(d) 2016*

44 On 27 January 2016, a 'Minute' was prepared for "*[a deputy director]*" in relation to TE2 Area 1. It noted that "*[a director] chair of the Bulk Data Review Panel (BDRP) commissioned a review of the [TE2 Area 1] in November 2015 with a view to disposing of legacy material*." The review "*identified a lack of governance across the [TE2 Area 1]*"[53] and a number of risks associated with the TE2 Area 1 (§8). It stated that:[54]

44.1 "*Undertaking an audit of the [TE2 Area 1] is the most complex requirement of the review. Currently [MI5 is not able to complete this in] a simple or expedient manner, [REDACTED] [TE Area 2]*" (§3). Such a statement is consistent only with a vast data holding;

44.2 "*[TE2 Area 1] contains BPD, [some of which is managed effectively (in that it is subject to review and disposal), and some of which is not]*" (§4). This suggests that TE2 Area 1 is some form of federated database (i.e. a type of meta-database management system which maps to and draws from multiple autonomous database systems), drawing upon BPDs that MI5 holds; and

44.3 "*[A team] consulted across MI5 [REDACTED] to identify current use of the [TE2 Area 1]. Whilst a number of [teams] use the [TE2 Area 1] the only respondents who have indicated that they provide any level of guidance on the use of the [TE2 Area 1] are [teams] within [team].*" (§7).

45 In January 2016 (that is 10 months before the IPA was adopted, and some two years and 10 months before it came materially into force), the Legal Paper on Compliance Risk was prepared by "*[a senior lawyer]*" and constituted "*legal advice to the MI5*

---

53 [Minute] **[C2/53/1]**.
54 [Minute] **[C2/53/2]**.

*Management Board*".[55] Part of the paper has been unredacted following an application by the Claimants for specific disclosure arising from a waiver of privilege. The paper identified (i) "*Continued RRD risks in relation to some TE systems*"; (ii) "*The risk arising from data in ungoverned spaces on the TE in terms of legal obligation to disclose material in court cases]*"; and (iii) *"New Investigatory Powers Commissioner oversight*" with the "*scrutiny of MI5 … likely to concentrate on the handling of the product from warrants and authorisations.*"[56] Under the heading "*Ungoverned spaces*", it stated:

> "[The redacted text describes some areas of the TE as 'ungoverned spaces' and details the work being carried out to uncover and marshal such spaces.]
>
> Allowing uncharted material to remain presents considerable legal risk [REDACTED] someone might recall something requiring disclosure mid-court case. [REDACTED] we may fall foul of our duty under the SSA 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."[57]

46 The 'Legal Compliance Principles for [TE]', published following the Legal Paper on Compliance Risk, noted that the "*biggest risks*" were likely to be "*Consistency between RRD on the [TE] and other [technology environments]*" and "*Managing new requirements under the IP Act for managing any BPD on the [TE]*".[58]

47 The Legal Paper on Compliance Risk was presented to the Management Board in February 2016. There were *"no formal actions arising from this meeting"*.[59] The relevant reference to the report appears to be at §15: *"The Board was pleased to see dynamism in the process and the inclusion of [a new legal compliance risk], … addressing areas of greatest concern to MI5".*

48 On 8 August 2016, the MI5 Management Board Minutes recorded that Risk 3 was scored as "*RED, reflecting the need for MI5 to address the vulnerabilities to legal challenge identified in the Compliance Review delivered to the Management Board in February 2016.*"[60]

---

55 Legal Paper on Compliance Risk **[C2/54/1]**.
56 Legal Paper on Compliance Risk **[C2/54/2, 4]**.
57 Legal Paper on Compliance Risk **[C2/54/11]**.
58 Legal Compliance Principles for [TE] (MI5 Core Doc 25) **[C2/73/2-3]**.
59 Management Board Meeting (MI5 Core Doc 12) **[C2/55/1]**.
60 Management Board Meeting (MI5 Core Doc 14) **[C2/57/3]**.

49 Privacy International brought the Existing BPD/BCD Claim in June 2015, and in February 2016 – shortly after the 'Minute' referred to in paragraph 45 above – the Respondents filed their Amended OPEN Response in that Claim, actively relying upon the adequacy of oversight and Handling Arrangements in relation to BPD/BCD. See Amended Grounds of Claim §§66-67 **[A1/5/27] [Core/4/27]**. See further the various other statements made by the Respondents to this Tribunal in the same period, again actively relying on their compliance with Handling Arrangements as to the treatment of BPD/BCD, quoted at Amended Grounds of Claim §§68-84 **[A1/5/27-32] [Core/4/27-32]**, in the period until the first substantive hearing of the claim before the Tribunal in July 2016. The relevant part of the Tribunal's judgment, accepting the Respondents' submissions and therefore being satisfied as to adequate and effective guarantees against abuse and effective supervision, is summarised at Amended Grounds of Claim §§85-86 **[A1/5/32] [Core/4/32]**.

50 On 14 October 2016 (a month before the IPA received Royal Assent), a 'Minute' prepared following a review of the TE stated that "*our understanding of the evidence is not as complete as we would wish*"; that "*the current level [REDACTED] is still not acceptable*"; and that enough had not been done to ensure that "*this 'legacy' risk doesn't increase and resolution of identified issues feels as though it is stalled*."[61] The review reported three key findings, one of which 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*."[62] The remaining two findings have been redacted.

51 On 15 December 2016, just over two weeks after the IPA received Royal Assent (it did not come into force until 31 December 2016), the 'MI5 Quarterly Performance Report: Q2' was prepared for the Home Secretary. The report noted at §8 that:

> "MI5's corporate risk register flags that it is currently carrying a risk that MI5 is not compliant with the relevant legislation with regards to information handling. MI5 has currently classified this as a red risk (meaning that there is a [REDACTED]). This is a relatively long standing risk for MI5 and in response it has created a new [department] that will lead on a whole range of measures including staff training, file reviews and new IT processes in order to improve legislative compliance."[63]

---

61 Minute (MI5 Core Doc 15) **[C2/58/1, 5]**.
62 Minute (MI5 Core Doc 15) **[C2/58/4]**.
63 MI5 Quarterly Performance Report: Q2 of 2016-2017 (HO Core Doc 1) **[C2/62/2]**.

*(e) 2017*

52 By email of 25 January 2017, the Private Secretary to the Home Secretary recorded that the "*Home Secretary noted her concern about two [REDACTED] errors that had been identified in the MI5's management [of a capability].*"[64] The errors that had been reported to the Home Secretary have not been disclosed in OPEN.

53 On 6 February 2017, the 'TE Issues Minute' was published. It stated "*[REDACTED] much of the [TE] is akin to the 'wild west' places [REDACTED]*" and "*RRD was limited in some areas of the TE, although in quite a few areas there is ... automated deletion of data so the picture was described as good in parts. The inadequacy of RRD was viewed as significant compliance risk of uncertain scale.*"[65]

54 A 'TE Risk Acceptance Statement' was published in 2017, which contained a record of residual risks relating to the TE and the decisions made relating to the acceptance (or otherwise) of that risk. The risks, which were rated "*HIGH*", "*MEDIUM-HIGH*" and "*MEDIUM*", have been fully redacted. It stated: "*[A review in 2012-13 identified a number of significant risks in the TE including access]*".[66]

55 On 21 March 2017, the 'Note: [TE] Risks' was shared with the MI5 Director General Strategy. Under the heading "*Compliance / Legal Risks*" it stated:[67]

55.1 "*There is 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.*" (§7);

55.2 "*We [REDACTED] do not have sufficiently comprehensive understanding of what material it holds. Guidance is not sufficiently comprehensive on what material should properly be placed in the [TE]*" (§8);

55.3 "*This impacts on our confidence in our ability to retrieve and disclose material when needed. [REDACTED] Subsequent work [REDACTED] has gone some way to uncover and marshal [REDACTED] This included the design of an MI5*

64 Email RE: Andrew Parker bilateral – readout (HH1 Exhibit HH4) **[C2/63/1]**.
65 TE Issues Minute OPEN **[C2/65A/2]**.
66 TE Risk Acceptance Statement (MI5 Core Doc 20) **[C2/67/2]**.
67 Note: [TE] Risks (MI5 Core Doc 21) **[C2/68/2-3]**.

*[information asset register] and an audit of the [TE]. The legal risks were described in [a senior lawyer's] Legal Compliance Report (January 2016)*" (§9);

55.4 "*Incomplete understanding of the material held on the shell*[68] *also prevents us from implementing an appropriate deletion policy including for categories of data for which there are strict legal requirements such as intercepted material. ...*" (§10); and

55.5 "*There is also a compliance risk in that MI5 would currently be unable to give sufficient assurance externally that we are handling information in accordance with current legislation.*" (§11).

56 On 24 March 2017, the 'MI5 Quarterly Performance Report: Q3' was prepared for the Home Secretary.[69] The report noted that:

> "MI5's corporate risk register continues to flag a red ('very high') risk that MI5 is found to be not compliant MI5 with its statutory obligations, particularly relating to information handling, leading to substantial legal/reputational damage. This means that there is [REDACTED]. This is a relatively long standing risk for MI5 and in response it has created a new [REDACTED] that will lead on a range of [department] measures including staff training, file reviews and new IT processes in order to improve legislative compliance. We met [REDACTED] colleagues to discuss their work to [staff in the new department] manage this risk. It seems clear that MI5 takes this risk seriously and is seeking to address it comprehensively; it aims to reduce the risk to the next category (orange – high) by the third quarter of 2017-18."

57 A 'Minute: TE Programme' also stated "*[There is evidence that in the TE there is data in certain areas. There may be issues with access controls and moving and copying of data. This data is also more difficult to discover, disclose or delete as required for legal compliance].*" It noted that "*[t]here is also a risk that any audit of [TE] by the Investigatory Powers Commission could lead to a negative impact on MI5's [Compliance Programme].*"[70] A further document, 'TE Safer Working Recommendations', stated: "*[The TE programmed* [sic] *had identified a number of further priorities, including (i) Cleaning up uncontrolled data storage areas in TE, as this data was hard to discover, disclose or delete as required for legal compliance; (ii) Limiting access to some pots of data.]*"[71]

---

68 A shell is a computing term for a technology environment, and is assumed to be used in this sense.
69 MI5 Quarterly Performance Report: Q3 of 2016-2017 (HO Core Doc 2) **[C2/69/2]**.
70 Minute: TE Programme (MI5 Core Doc 26) **[C2/74/1]**.
71 TE Safer Working Recommendations (MI5 Core Doc 27) **[C2/75/2]**.

58 On 18 October 2017, the MI5 Quarterly Performance Review 2016/17 was summarised in a submission to the Home Secretary. It stated:[72]

> "Lastly, the performance meeting briefly discussed MI5's corporate risk register. There are two red (very high) risks. The first is compliance with statutory obligations. This is a longstanding risk that MI5 is placing significant effort into managing. Nonetheless the timeframe by which MI5 believes it will be able to reduce the risk from red to orange (high) has slipped from [towards the end of 2017] to [mid 2018]. MI5 says this reflects an original underestimation rather than a change."

59 On 27 October 2017, a 'Minute' was prepared with the subject "*Compliance in the [TE]*". The "*most important issues*" included "*Review, retention & Disposal. We don't have agreed RRD policies for all information on the [TE]. [REDACTED] Many systems can't delete [REDACTED] and <u>we continue to build some without it</u>*"[73] (emphasis added). Another issue that was identified was "*Access Control*", but the commentary in relation to that issue is fully redacted.[74] It is significant that MI5 continued not only to operate, but also to <u>build,</u> systems which facilitated non-compliance with statutory safeguards. In the same 'Minute', MI5 also recognised that it had "*made a number of attempts to solve the [TE] problem…We need a new plan*", underlying the already long-running and difficult-to-challenge state of non-compliance in the TE by 2017.

60 In 2017, a 'Committee Paper' was prepared to update the "*[security and information committee]*" on the work of the TE programme. The paper noted:[75]

> "More widely, significant **information and legal compliance** risks concerning [TE] have been identified by [REDACTED]. This results from the absence of compliance with relevant legislation, Codes of Practice and Handling Arrangements. These were summarised in [REDACTED] summary of [TE] risks shared with DGS on 21 March (attached). The key issues are our lack of understanding about the material held on [TE], which coupled with insufficient guidance on what material should be properly placed on [TE], impacts on our ability to retrieve and disclose material [REDACTED] when needed and prevents us from implementing an appropriate deletion policy (including for categories of data for which there are strict legal requirements). There is also a risk that we would be unable to give sufficient assurance externally that we are handling information in accordance with legislation."

61 The MI5's Management Board Performance Report 2017 recorded that Risk 3 "*continues to be RED as forecast and is not forecast to become AMBER until [mid-2018]*" and that

---

72 MI5 Core Doc 31 **[C2/82/3].**
73 [Minute] (MI5 Core Doc 32) **[C2/83/1]**.
74 [Minute] (MI5 Core Doc 32) **[C2/83/2]**.
75 [Committee Paper] (MI5 Core Doc 33) **[C2/84/3]**.

one of the risks associated with Risk 3 is "*[[REDACTED] significant legal compliance risks relating to RRD [in the TE]].*"[76]

62 In 2017, the TE was re-accredited as a "*[restricted system]*". Five risks were noted in granting its re-accreditation, all of which have been redacted. Accreditation was granted on an interim basis for 12 months and on the condition that "*a programme of [improvements] be put in place*." The paper recommending this decision stated: "*significant risk around the absence of compliance with relevant legislation, Codes of Practice and Handling Arrangements … [an incomplete understanding of material held on the [TE] prevents us from implementing an appropriate deletion policy including for categories of data where there are strict legal requirements such as [warranted] material. … [concluding that] there is also a compliance risk in that MI5 would currently be unable to give sufficient assurance externally that we are handling information in accordance with current legislation.*"[77] Whilst this paper has been excerpted and/or gisted in the CIR, it does not appear to have been disclosed to the Claimants (though given the use of gists, this is difficult for the Claimants to confirm).

63 In October 2017, MI5 explained in the Existing BPD/BCD Claim that it had inaccurately run searches for Privacy International's data because of data which had been saved in an area known as 'Workings', which was not searched and which had no existing RRD policy applied to it. That resulted in MI5 amending its position to confirm that it did unlawfully hold data relating to Privacy International in its BCD prior to avowal. See Amended Grounds of Claim §§87-90 **[A1/5/32-33] [Core/4/32-33]**. The issue of 'Workings' is, the Claimants have been told, a different issue from the TE/TE2 issue (see Amended Grounds of Claim §91 **[A1/5/33-34] [Core/4/33-34]**). But even at this stage, the Respondents did not disclose to the Tribunal the TE/TE2 issue.

64 On 20 December 2017, the 'Note to the Home Secretary on MI5 Quarterly Review of Performance: Q2 of 2017/18' was prepared following a meeting between senior MI5 officials and the Director General of the Office for Security and Counter-Terrorism ("**OSCT**"). It stated:[78]

---

76 [Management Board, Performance Report, 2017] (MI5 Core Doc 34) **[C2/85/8]**.

77 CIR §§70-71 **[C4/185/18].**

78 Note to Home Secretary on MI5 Quarterly Review of Performance: Quarter 2 of 2017-18 (HH1 Exhibit HH7) **[C2/88/4]**.

> "There is one red [REDACTED] risk in MI5's Q2 report, which concerns compliance with statutory obligations. The red rating reflects the long-term challenge of how to ensure that MI5 systems facilitate the organisation's compliance with its legal and other obligations. As you know, this was also red in Q1 and is a longstanding risk that MI5 is placing significant effort into managing. To ensure compliance [REDACTED] MI5 have [taken a number of steps]. ... The quarter by which MI5 hopes to achieve an Amber rating on compliance has slipped again (by a further quarter), to Q2 next financial year."

*(f) 2018*

65 On 11 January 2018 (four months before the commencement of the Judicial Commissioner provisions of the IPA), the 'MI5 Management Board Paper' was prepared to provide the Management Board with "*a fuller picture of MI5's legal compliance risk (Risk 3) and the work underway under the [Compliance Programme] to address it*." It noted:[79]

> "Anticipating risk and getting ahead: while we have made good progress against the Legal Compliance Review recommendations, new areas of risk continue to emerge [REDACTED]; further examples of systems without the necessary RRD regimes [REDACTED] and recent instances breaches of policy [REDACTED]"

66 The paper also stated: "*[w]e do not have comprehensive, effective and implemented RRD policy [in one of the systems]*"; "*[e]ffective RRD has not been implemented across all data stores in [the TE], potentially including warranted material, and therefore there is a risk that elements of it are non-compliant*"; and "*[t]here is a risk that we are unable to guarantee that we can identify and destroy LPP and other CI material consistently across all systems where it may be present.*"[80]

67 At the Management Board Meeting on 11 January 2018, the "*[Director for policy, security, compliance, information]*" introduced a paper on 'Compliance Risk', which "*captured the work already in progress to strengthen compliance and highlighted further areas for development (including [the corporate record and TE] and Retention / Deletion / Destruction policies)*."[81]

68 By email of 5 March 2018, in response to certain questions from OSCT, MI5 noted that the "*RED*" rating on compliance was "*driven primarily by the shortfall in effective procedures for the review, retention and deletion (RRD) in a number of [REDACTED]*

---

79 [Management Board Paper] (MI5 Core Doc 37) **[C2/90/2-3]**.
80 [Management Board Paper] (MI5 Core Doc 37) **[C2/90/6]**.
81 Management Board Meeting (MI5 Core Doc 38) **[C2/91/2]**.

*and risks in relation to the [systems] [handling of confidential material (particularly material subject to Legal Professional Privilege)].*"[82] As well as RRD, MI5 had concerns about the adequacy of safeguards relating to Legal Professional Privilege ("**LPP**") material.

69 In around April 2018, the interim accreditation of the TE was extended for a further 12 months. On 23 March 2018, the paper that recommended this decision noted that "*there is significant risk around the absence of compliance with relevant legislation, Codes of Practice and Handling Arrangements [We do not have a good understanding of what material is in the TE] and there is insufficient guidance on what material should properly be placed in it. This impacts on our confidence in our ability to retrieve and disclose material when needed. It also prevents us from implementing an appropriate deletion policy.*"[83]

70 On 27 April 2018, the '[TE] Improvement Programme: Programme Mandate' was published. The following concerns were noted:[84]

70.1 "*[We are currently holding too much [risk] and are unable to [REDACT]. Existing ways of working are [REDACT] and no single team is coordinating improvement work]*";

70.2 "*[Risk associated with access]*";

70.3 "*[There is [an incomplete] understanding of the [information] within TE. We don't understand what [REDACTED]. We are unable to confidently report on compliance with legal obligations]*";

70.4 "*Automatic or manual deletion of data held within [areas] is not happening in many cases meaning we are holding onto data for longer than we legally should.*"; and

70.5 "*[There is [a risk] that record material is not being transferred from TE [Redacted] which risks the outcome of judicial proceedings]*".

---

82 Email: "RE: Response to questions" **[C2/93/3]**.
83 [TE]: Security Accreditation Update (A2 Exhibit A19) **[C2/94/3]**.
84 [TE]: Security Accreditation Update (A2 Exhibit A19) **[C2/96/1]**.

71 Despite this, by letter dated 17 May 2018, the MI5 Director for Information, Policy, Security and Compliance told Graeme Biggar, Director of National Security in the Home Office, that MI5 would be ready on 31 May 2018 to commence the IPA provisions concerning interception and equipment interference and targeted examination of bulk data and the use of Judicial Commissioners in the associated warranting powers.[85] Whilst the letter noted that "*our 'go' decision does not mean that commencement will be without risk*", there was no reference to the "*RED*" rating on Risk 3, or the compliance issues related to the TE, TE2 Areas 1 or 2.

72 On 7 June 2018, the Minutes of the MI5 Quarterly Review noted as part of the "*Summary of Actions*": "*MI5 to brief the Investigatory Powers Commissioner about progress against the red risk on its [risk register]*."[86] This briefing never happened for reasons that have never been explained in the Respondents' witness evidence.

73 By letter dated 9 July 2018, the MI5 Director for Information, Policy, Security and Compliance told Graeme Biggar that MI5 would be ready on 25 July 2018 to commence the IPA provisions relating to (amongst others) BPD/BCD, also subject to Judicial Commissioner oversight.[87] Again there was no reference to the "*RED*" rating on Risk 3, or the compliance risks associated with the TE, TE2 Area 1 or 2.

74 On 13 July 2018, Graeme Biggar wrote to the Security Minister and Home Secretary to seek agreement to commence the BPD/BCD provisions of the IPA on 25 July 2018.[88] The submission also did not refer to the "*RED*" rating on Risk 3, or the compliance risks associated with the TE, TE2 Area 1 or TE2 Area 2; rather it noted "[a]*ll are in agreement that there are no major outstanding risks and those risks that remain are at an acceptable level…*" (§6).[89] No attempt has been made in the Respondents' evidence to explain this statement or how it came to be made.

75 On 13 August 2018 (after the commencement of all the major warranting powers in the IPA), the 'MI5 Quarterly Performance Report: Q4 of 2017/18' prepared by "[*a member*

---

85 Letter from MI5 (MI5 Core Doc 42**) [C2/98/1]**; CIR §106 **[C4/185/25].**
86 Minutes-MI5 Quarterly Review (Q4 2017/18) (MI5 Core Doc 44) **[C2/102/1]**.
87 Letter from MI5 (MI5 Core Doc 45) **[C2/105/1]**; CIR §114 **[C4/185/27]**.
88 Submission to SSHD & Security Minister (MI5 Core Doc 46) **[C2/106/2]**; CIR §115 **[C4/185/27]**.
89 Submission to SSHD & Security Minister (MI5 Core Doc 46) **[C2/106/2]**.

*of the oversight team*" of NSU, noted that MI5 had "*one red (very high) risk concerning its compliance with statutory obligations in Q4.*" It stated:[90]

> "**There remained one red (very high) corporate risk for MI5 in Q4.** This relates to compliance with statutory obligations. The red rating reflects the long-term challenge of how to ensure that MI5 systems facilitate the organisation's compliance with its legal and other obligations. This was red in Q3 2017/18 and is a longstanding risk that MI5 is placing significant effort into managing. In the Q4 Quarterly Review meeting, MI5 stated that it was implementing the recommendations from the Compliance Board and was on track for this risk to reach amber (high risk) in Q2 2018/19. **OSCT will continue to monitor MI5's progress on compliance.**"

76 In October 2018, the '[Security and information committee] Update on [TE] Remediation Activities' noted that "*[Particular areas in the TE represent] unqualified risk*" (emphasis added, i.e. involving a clear breach of legal requirements) because (amongst other things) there was (i) "*No central corporate understanding of data held here [REDACTED]*"; (ii) "*no training*"; (iii) "*no governance/policy*"; (iv) "*[Related to access controls]*"; (v) "*no mandated review, retention or deletion mechanisms*"; and (vi) "*[There may be] data which we should not be retaining*."[91] It also noted that there was a "*[Risk of material not being appropriately transferred]*."[92]

77 On 4 October 2018, the 'Committee Paper' stated that "*[The TE poses serious and significant risk relating to legal and information compliance]*" and that "*[A team has led good work to understand the legal and compliance risk, particularly information stored in particular areas. It is assessed that there are legal compliance risks that are RED which could lead to successful IPT challenges, loss of confidence of ministers/JCs and consequently restrictions in warrants or reputational damage]*."[93]

78 In October 2018, the MI5 Executive Board had a "*teach-in*" on the TE and TE2. The presentation noted that "*[An appropriate framework and ways of working were never established in the TE – our position is unacceptable.]*". It also stated that (i) "*There is a lack of understanding of what data is currently held [in the TE]*"; (ii) "*Systems are not handling data in accordance with our legal obligations – there is a lack of RRD and clear processes to manage the lifecycle of data held in the [TE]*"; (iii) "*[Users may not*

---

90 MI5 Quarterly Performance Report: Q4 of 2017/2018 (HO Core Doc 4) **[C3/111/4]**.

91 [Security and information committee] Update on [TE] Remediation Activities (MI5 Core Doc 49) **[C3/114/5]**.

92 [Security and information committee] Update on [TE] Remediation Activities (MI5 Core Doc 49) **[C3/114/4]**.

93 Committee Paper (MI5 Core Doc 50) **[C3/115/1]**.

*act compliantly, either through a lack of awareness or effective controls]*"; and (iv) "*[There is a risk of material not being appropriately transferred or stored]*."[94] The key findings (most of which have been redacted) noted that "*[Data continues to be held for longer than is necessary and proportionate and in places cannot be accounted for [REDACTED]]*" and "*[We do not have the [REDACTED] governance to oversee the TE to ensure we realise full operational benefit]*."[95] The presentation set out a strategy for compliance ending on 8 April 2019, which did not include briefing the IPCr or the Home Secretary or disclosure to the IPT. The document did not address or even raise disclosure to Judicial Commissioners in the warrantry context.

79 On 18 October 2018, the 'Minutes' of the MI5 Quarterly Review: Q1 2018/19 recorded the following "*Summary of Actions*": "*MI5 to update on whether it needs to brief the Investigatory Powers Commissioner on [REDACTED]*" and "*MI5 to arrange a context setting meeting with the Home Secretary, with topics of discussion to be [REDACTED]*." It also stated that "*MI5 had not briefed the Investigatory Powers Commissioner about the red risk on compliance in its corporate risk register. However, this red risk had moved to amber in Q1 2018/19 – one quarter earlier than anticipated – and MI5 assessed that it was no longer necessary to brief the Investigatory Powers Commissioner on this risk.*"[96] According to the CIR, the minutes also record that "*[MI5 would need to think about whether to brief the IPC on the new RED risk]*."[97] Again, the document did not address or even raise disclosure to Judicial Commissioners in the warrantry context, again framing the issue as in effect one confined to oversight. It is also astonishing that an "*AMBER*" risk of illegality (i.e. high) is considered by MI5 to be below the threshold for notifying IPCO, especially when the risk is one that is so long-standing and previously "*RED*" (i.e. very high) and nothing material appeared to have changed in the interim (as is shown by the subsequent difficulties in resolving the non-compliance).

80 On 30 October 2018, in the first disclosed paper drawing the (obvious) consequences for warrantry, the MI5 Executive Board Paper set out the "*key legal, compliance risks [REDACTED] of the TE]*" which included:[98]

---

94 [TE] Programme – [TE] Strategy EB Education Session (MI5 Core Doc 50) **[C3/116/7]**.
95 [TE] Programme – [TE] Strategy EB Education Session (MI5 Core Doc 50) **[C3/116/8]**.
96 Minutes-MI5 Quarterly Review (Q1 2018/19) (MI5 Core Doc 52) **[C3/117/1]**; CIR §121 **[C4/185/29]**.
97 CIR §121 **[C4/185/29]**.
98 Executive Board Paper (MI5 Core Doc 53) **[C3/118/2]**; CIR §123 **[C4/185/29-30]**.

80.1 "*The lack of consistent [REDACTED] means that MI5 is unable to provide robust assurances to its oversight bodies that data held in the [TE] cannot be accessed unlawfully. The risk is that the IPC may be unwilling to authorise further warrants until this is rectified, especially for [REDACTED] data*" (§11);

80.2 "*Effective review, retention and deletion (RRD) has not been implemented across all [areas] in the [TE] potentially including warranted material, and therefore there is a risk that elements of it are non-compliant. There is a risk that lack of effective RRD policy could lead to successful IPT challenges, loss of confidence of ministers/JCs and consequently restrictions in warrants or reputational damage.*" (§12); and

80.3 "*In order to mitigate these risks, we anticipate that MI5 will want to pre-emptively brief oversight bodies on these challenges and our plans to address them. [REDACTED]*" (§13).

81 The MI5 Management Board met to discuss the MI5 Executive Board Paper, noting that "*[The Board recognised that the [TE] is important to MI5's mission but acknowledged it had suffered from issues including compliance]*."[99]

82 On 15 November 2018, the MI5 Management Board Minutes recorded that "*The Board noted that [a risk] had changed to [RED] status following the introduction of additional [indicators]. It was recognised that remediation work on the [TE] was in progress to [reduce] this risk.*"[100]

83 On 26 November 2018, the draft agenda for the MI5 Quarterly Review: Q2 2018/19 noted that the recommendation was not to brief the IPCr: "*Discussion ongoing as to whether this is necessary – but MI5 are reviewing their risk management approach, you will receive an update on the new approach at the next quarter meeting. As the risk is likely to change it would make sense to hold off briefing the IPC until that is complete (e.g. [REDACTED] may provide mitigation in this area).*"[101]

---

99 Executive Board Meeting (MI5 Core Doc 54) **[C3/119/1]**.

100 Management Board meeting minutes (MI5 Core Doc 56) **[C3/121/2]**.

101 Attachment to email: Draft Annotated Agenda for DG OSCT – DGS [REDACTED] 18/19 Quarterly Review **[C3/122/6]**.

84 On 28 November 2018, the 'Minutes' for the MI5 Quarterly Review Meeting recorded as follows:[102]

84.1 "*The question of whether to brief the Investigatory Powers Commissioner on [the RED risk] was still under discussion.*" (§2.2);

84.2 Under the heading "*Legacy IT*": "*This is a complex and multi-faceted problem [REDACTED] MI5 acknowledged the need to understand both risks and costs before [acting]. However, the Management Board conversation at Q2 centred around whether there may be options for accepting more risk in this area*" (§4.1) (emphasis added); and "*DG OSCT asked whether there is anything in this space which keeps DDG/DGS 'up at night' [REDACTED]. DDG indicated that there is not – while there are some significant risks, these are all being managed appropriately. MI5 are confident there is no requirement to brief the Home Secretary at this stage.*" (§4.5). Having noted that there were "*some significant risks*", the reasoning or basis for accepting an even greater risk of non-compliance, without briefing the Home Secretary of any such risk, is not understood. The reasoning appears to have been that having identified significant "RED" risk, MI5 was entitled to work out the full extent of the risks and the costs of solving them before reporting them to the Secretary of State/IPCr, an approach demonstrably incapable of justification; and

84.3 Under the heading "*Update on 'hard choices'*": "*In terms of off-balance costs, litigation had become a standing issue, rather than a risk, and remained a serious expense*" (§5.3).

85 On 10 December 2018 (five to seven months after the IPA came into material force), the "*[information policy deputy director]*" prepared a note, 'Legal Issues and IPCO Engagement', for the "*[director of the information, security, compliance and strategic policy department, and the technology and innovation department]*". It recommended briefing the Home Office and the IPCr on a range of issues that MI5 faced in relation to the TE as soon as possible.[103] Under the heading "*Key points*", it recorded as follows:[104]

---

102 Minutes: MI5 Quarterly Review (Q2 2018/19) (MI5 Core Doc 57) **[C3/123/2-5]**; CIR §125 **[C4/185/30]**. The Claimants note that "*[the RED risk]*" in §2.2 is redacted in C3/123, but included in CIR §125.

103 CIR §126 **[C4/185/30-31]**.

104 Legal Issues and IPCO Engagement (MI5 Core Doc 58) **[C3/126/1]**.

85.1 "*[A volume of data obtained from warrants and authorisations is currently being held on the TE, an environment with issues related to auditing]*";

85.2 "*The data is subject to legal requirements, in particular the Investigatory Powers Act Codes of Practice and Handling Arrangements; many of those requirements (particularly RRD) are not being followed. Significant legal and compliance issues arise from this non-compliance*"; and

85.3 "*We are required to report failures to comply with Codes of Practice requirements to IPCO (see para 16 for more detail). Our knowledge regarding compliance risks is not complete, however we know enough to be able to articulate the issues discovered. Failure to report in a timely fashion, would, if discovered by IPCO or by the Investigatory Powers Tribunal, be considered a significant breach of trust and is likely to lead to public censure, damage to reputation and calls to curb our powers. We therefore recommend reporting to IPCO ASAP in the manner recommended in this paper.*"

86 Under the heading "*Are we compliant with legal requirements?*" it is stated:[105]

86.1 "*The general risks relating to access controls [REDACTED] in the [TE] are [legal compliance risks] in that the Codes of Practice contain [specific] requirements to ensure that that data is kept safe. [REDACTED]*";

86.2 "*[Certain users are able to access information in TE without having a clear n&p [necessity and proportionality] case for doing so]*"; and

86.3 "*There is no clear policy, guidance and governance to ensure consistent compliance across the [TE].*"

87 Under the hearing "*What is our legal obligation to report the issues identified and under whose remit do they fall?*" it noted: [106]

87.1 "*It is worth noting that the data within the [TE] could cut across the remit of both IPCO and the Information Commissioner but we need to ascertain precisely what data is held in the [TE] before we can advise further.*" (§14); and

---

105 Legal Issues and IPCO Engagement (MI5 Core Doc 58) **[C3/126/2-3]**.
106 Legal Issues and IPCO Engagement (MI5 Core Doc 58) **[C3/126/5]**.

87.2 "*We could choose not to report the compliance obligations identified, but obviously were the issues to be discovered by IPCO and/or the ICO e.g. through a whistleblower, a data loss, forced disclosure in an IPT hearing etc, the failure to report would significantly undermine the trust we have built up with IPCO and would be likely to lead to public criticism and censure. If we report voluntarily, rather than appear to have the information forced from us, IPCO may be less likely to take a hard-line response.*" (§15)

88 Under the heading "*How might IPCO view the compliance problems if reported?*" it noted: [107]

88.1 "*IPCO are likely to want to know when we first became aware of the legal compliance problems identified above and we will need to be prepared to explain this to them. It is only in recent months that the full extent of the issues have become clear and we have been able to better scope the legal compliance issues sufficiently to be able to report them.*" (§16)

88.2 "*Once we have brought IPCO up to a sufficient level of understanding, they are likely to regard aspects of data management within the [TE] as not complying with legal requirements. They are likely to be sympathetic to our problems, but they will want to be seen to be doing what is required of them as an oversight body*" (§17); and

88.3 "*IPCO may consider that the legal compliance issues should be taken into account by the Secretary of State and IPCO when they consider our warrants. At first blush, it is possible (though we think unlikely) that they could, as their Canadian oversight counterparts have done in similar cases, view the matters identified as so serious as to opine that warrants [REDACTED] should not be authorised [REDACTED]*" (§17(c)). As to the reference to the "Canadian oversight counterparts", see paragraph 168 below.

89 Notwithstanding the recommendation, the IPCr and Home Secretary were not briefed about the issues concerning TE until months later.

---

107 Legal Issues and IPCO Engagement (MI5 Core Doc 58) **[C3/126/5-6]**.

90 On 17 December 2018, the "*[security and information deputy directors] group*" met to discuss progress with TE remediation work.[108] The 'Minutes' recorded that:[109]

*90.1* "*[TE] remediation continues ... the [TE programme] [REDACTION] showing several successful activities to-date. There remains a concern with [REDACTION], but [resolving them] would likely [impact] the business. All [deputy directors] are asked to provide their views [REDACTION].*" (§11); and

90.2 "*The [TE] RRD proposal was presented, highlighting the need to address legal and compliance risks, and to show a credible forward plan. [REDACTION] [Deputy directors] agreed the request to set up a [TE governance group giving data senior manager] the authority to decide when old data could be deleted, or escalate [upwards] as required. It was proposed that old data would be 'quarantined' pending deletion, however the group was not confident that quarantined data met the legal definition of 'putting the data out of use' – as files could still be recovered as needed. Further work remains to confirm the mechanics of [REDACTION] and how best to resource this task*" (§12).

*(g) 2019*

91 On 18 January 2019, the '[TE] [Programme]: Access Controlling TE's File Shares' provided "*background and risk assessment on the [TE]*".[110] It stated "*[Access Controls] present [risk]. Our knowledge of what data is held in [areas] is currently limited (but improving), due to [a reason] and the lack of an appropriate capability [REDACTED]*" (§3) and "*[[Areas] have been identified as a key source of legal compliance risk, most recently in [a note]. The subject is likely to be briefed to the IP Commissioner [REDACTED]. In addition to (another issue], [these areas] are not subject to the application of appropriate RRD rules – an areas of remediation being led by [a department] which has been subject to [REDACTED] consultation. The data contained in [these areas] must be managed in accordance with the relevant Codes of Practice and statutory and internal Handling Arrangements [REDACTED]*" (§4).[111] The note

108 CIR §§128-129 **[C4/185/31]**.
109 Deputy Director Meeting (MI5 Core Doc 60) **[C3/129/2-3]**.
110 Document: [TE] [Programme]: Access Controlling TE's File Shares (MI5 Core Doc 64) **[C3/131/1]**.
111 Document: [TE] [Programme]: Access Controlling TE's File Shares (MI5 Core Doc 64) **[C3/131/1]**.

recorded that MI5 "*intend to brief the IP on this as soon as possible as we are likely to be criticised for the delay in informing him*" (§18).[112]

92 On 24 January 2019, there was a committee meeting of the "*[security and information committee]*". The Minutes recorded that (i) the "*[TE area] issue*" was one of the "*Key points*"; (ii) the issue was "*potentially MI5's largest current compliance risk*"; and (iii) "*[the committee] decided it was right to take the current [position] to IPC and Home Office*".[113]

93 In January 2019, the MI5 Director General authorised briefing the IPCr on issues relating to the TE. In parallel, MI5 was considering internally whether there were implications for warrantry applications of the planned briefing on the TE for the IPCr.[114]

94 On 31 January 2019, "*[the deputy director general]*" wrote to the IPCr and the Director General OSCT summarising a recent MI5 review of the impact of MI5's work of the transition of warrantry arrangements to the IPA. The letter reported benefits including an "*improved… ability to robustly defend its actions in court and a strengthened compliance culture owing to the [compliance programme]*". It did not refer to the ongoing compliance risks or concerns relating to TE or TE2.[115]

95 The Deputy Director then covering the NSU was then given an "*oral outline brief of the issues MI5 faced in relation to [TE]*."[116] The Chief Executive of IPCO was given a "*fuller oral briefing of the compliance and other issues MI5 faced with the [TE]*."[117]

96 By letter dated 21 February 2019, the MI5 Director of Information, Security, Compliance and Strategic Policy wrote to Graeme Biggar to inform him that MI5 intended to brief the IPCr on challenges in maintaining assurance in terms of legal compliance with regard to the TE.[118] The concerns listed included (i) "*[understanding exactly what data is held in the TE]*; and (ii) "*Inconsistent application of Review Retention and Disposal (RRD) policies to systems in the [TE]. [REDACTED] [Some areas have] effective RRD in place;*

112 Document: [TE] [Programme]: Access Controlling TE's File Shares (MI5 Core Doc 64) **[C3/131/5]**.
113 Committee Meeting (MI5 Core Doc 65) **[C3/132/2-3]**.
114 CIR §§134-135 **[C4/185/32]**.
115 Letter from MI5 DDG to DG OSCT **[C3/133/1]**; CIR §137 **[C4/185/32-33]**.
116 CIR §138 **[C4/185/33]**.
117 CIR §139 **[C4/185/33]**.
118 Letter to Home Office from MI5 Director (MI5 Core Doc 66) **[C3/135/1]**; CIR §140 **[C4/185/33]**.

*however, [there is] an inconsistency in approach*."[119] Other concerns have been redacted. It also noted that the "*issues are also of interest to you and your Secretary of State as you consider and approve our warrantry and handling arrangements*."[120] The Tribunal will have to consider whether this was a fair and full account.

97 On 26 February 2019, the Head of Oversight of the NSU informed the Home Secretary and Security Minister of MI5's intention to brief the IPCr on issues related to the TE on 27 February 2019. The note summarised the "*key challenges faced by the TE*" and recorded that "*[g]iven the presence of warranted product on [REDACTED] it is important that Sir Adrian is satisfied with the actions being taken to mitigate any risks MI5 in terms of maintaining legal compliance [REDACTED] on the system*."[121]

98 A '*Note on* [TE] *discussions in Quarterly Review meeting* [sic] *since January 2018*' set out the communications on the TE issue between MI5 and the Home Office and stated that: "[t]*he issues with [TE] were not raised proactively by MI5 in any of the QR meetings*"; "[t]*he issues were raised in low-levels of detail…*"; and "*[NB – the discussion about the risk was in very general terms…*".[122]

**(2) Briefing of the IPCr on compliance relating to the TE**

*(a) Notification to the IPCr and Home Secretary*

99 On 27 February 2019, MI5 briefed the IPCr on compliance and other challenges relating to the TE (but notably not TE2). At the IPCr's request, the content of this briefing was then set out in writing in a letter from the MI5 Director of Policy, Compliance, Security and Information to the IPCr on 11 March 2019.[123] The letter stated that an MI5 compliance team identified in January 2016 that "*data might be being held in ungoverned spaces in contravention of our policies*" (§10).[124] It also stated that the risk had been reported to the MI5 Management Board and regularly reported on from early 2018, and that 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*

119 Document: [TE] [Programme]: Access Controlling TE's File Shares (MI5 Core Doc 64) **[C3/131/2]**.
120 Document: [TE] [Programme]: Access Controlling TE's File Shares (MI5 Core Doc 64) **[C3/131/1]**.
121 Information Note to SSHD & Security Minister (HO Core Doc 5) **[C3/137/1-2]**.
122 Note on TE discussions in Quarterly Review (HO Core Doc 17) **[C3/159/1]**.
123 Letter to Sir Adrian Fulford (MI5 Core Doc 69) **[C3/142/1]**; CIR §142 **[C4/185/33-34]**.
124 Letter to Sir Adrian Fulford (MI5 Core Doc 69) **[C3/142/2]**.

*be compliant with the Investigatory Powers Act*" (§10). No disclosure was made of the (above-canvassed) concerns about RRD and TE and TE2 Areas 1 and 2 that pre-dated 2016 back to at least 2012, in particular minutes from meetings of the MI5 Management Board in May 2013 (referred to in the CIR Summary, but not disclosed) and November 2014 (paragraph 34 above); or indeed any concerns about TE2. No explanation has been given by the Respondents as to why disclosure to the IPCr was so restricted.

100 On 11 March 2019, an internal IPCO document, 'The [TE]: adequacy of IPA Safeguards (as of 11 March 2019)', was published. It assessed whether the TE complied with the IPA safeguards relating to (amongst others) "*access controls*", "*copies: file shares*", "*retention and deletion*" and "*LPP material*".[125] The remaining safeguards have been redacted in OPEN. The commentary in relation to "*copies: files*" is entirely redacted.[126] 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 copies are provided. In relation to the other safeguards identified in OPEN, it stated:

100.1 As to access controls, "*[REDACTED] Arguably the status quo does not represent non-compliance, but underlies the need for [a mitigation]*";[127]

100.2 As to RRD, "*MI5 has submitted an error report on the lack of a retention policy in [an area of TE]. Between 6 October 2016 and 1 March 2019 [the area] did not have any retention and deletion policy [REDACTED]. As a result, no [a type of data] has been deleted for a period [REDACTED], including [REDACTED] LPP material which was retained solely for the purpose of deletion. MI5 have informed IPCO that they plan to have a process in place [REDACTED] to delete material in line with their retention policy on [frequency specified]*";[128] and

100.3 As to LPP material, "*In light of the [error described above] it is unclear what level of assurance MI5 has that LPP material [REDACTED] has in fact been deleted*

---

125 Internal IPCO document entitled "The [TE]: adequacy of IPA Safeguards (as of 11 March 2019)" (IPCO Doc 1) **[C3/141A/1-4]**.

126 Internal IPCO document entitled "The [TE]: adequacy of IPA Safeguards (as of 11 March 2019)" (IPCO Doc 1) **[C3/141A/2]**.

127 Internal IPCO document entitled "The [TE]: adequacy of IPA Safeguards (as of 11 March 2019)" (IPCO Doc 1) **[C3/141A/1]**.

128 Internal IPCO document entitled "The [TE]: adequacy of IPA Safeguards (as of 11 March 2019)" (IPCO Doc 1) **[C3/141A/3]**.

*from [the TE], either when directed by a JC or when marked for deletion by [a staff member].*"[129]

101 Between 18 and 22 March 2019, IPCO conducted an inspection of the TE.[130] See paragraphs 106 to 111 below for more on the results of this inspection.

102 By letter dated 26 March 2019, Tom Hurd, Director General OSCT, informed the Home Secretary ahead of the meeting with the MI5 Director General, that the TE "*poses difficult questions around MI5's compliance with both the Investigatory Powers Act and their own policies in their handling of warranted data*" and that "*a failure of governance has led to this situation*" (§7).[131]

103 On 27 March 2019, Jonathan Emmett, then covering the role of the Home Office's Deputy Director for National Security, provided the Home Secretary and Security Minister with an update on the TE, enclosing IPCO's First Inspection Report. This recommended that, notwithstanding the errors identified and pending the receipt of legal advice, the Home Secretary should continue to consider MI5 warrant applications.[132] Another recommendation that the Home Secretary approve warrant applications was issued on 3 April 2019.[133]

104 By letter dated 4 April 2019, the MI5 Director General wrote to the Home Secretary to provide an update on the compliance challenges relating to the TE. The letter noted: [134]

104.1 "*The compliance risks identified are largely associated with our ability to effectively record* [REDACTED] *access to,* [REDACTED]*, retention and deletion of warranted data*" (§5);

104.2 "*I know that you have received advice from your officials about the impact of the* [TE] *issues on your approval of warrants, which includes legal advice from Sir James Eadie QC, and that you are content to continue to consider MI5 warrants.*" (§8);

---

129 Internal IPCO document entitled "The [TE]: adequacy of IPA Safeguards (as of 11 March 2019)" (IPCO Doc 1) **[C3/141A/4]**.
130 CIR §144 **[C4/185/34]**.
131 Letter to Home Secretary from DG OSCT (HO Core Doc 8) **[C3/147/2]**.
132 TE Update to SSHD and Security Minister (HO Core Doc 10) **[C3/150/1]**.
133 Submission to SSHD and Security Minister (HO Core Doc 15) **[C3/157/1]**.
134 Letter from DG MI5 to SSHD (MI5 Core Doc 76) **[C3/164/1-3]**.

104.3 "*MI5 has been aware of the potential [REDACTED] risks relating to the [TE] for a number of years, and has been working to address those risks. However, it was only late last year that the true nature and scale of the risks we were facing – and in particular the compliance risks – crystallised at Board level.*" (§13). No mention was made of any of the pre-2016 materials canvassed above, or the concerns they raised, in particular minutes from meetings of the MI5 Management Board in May 2013 (referred to in the CIR Summary, but not disclosed) and November 2014 (paragraph 34 above); and

104.4 "*[T]here should be no sense that we treat compliance with anything less than the greatest priority and it is a matter of profound regret that these issues were not identified and fully addressed sooner*" (§14).

105 By letter dated 24 April 2019, Sir Andrew Parker (MI5 Director General) admitted to the then Home Secretary that MI5 had failed to recognise the seriousness of its legal non-compliance (at §§3 and 5):[135]

> "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."

*(b) IPCO Inspection Reports and Annex H*

106 On 29 March 2019, IPCO issued its First Inspection Report (v.2). Six key findings were reported, including (i) "*[REDACTED] MI5 will soon be applying an automated RRD process to operational data [within a suite of systems, which hold a [REDACTED] proportion of the TE's operational data*"; (ii) "*MI5 had a manual process in place for deleting material subject to legal professional privilege (LPP material) from its systems, but was [REDACTED]*"; and (iii) "*by January 2018 if not earlier, MI5 had a clear view of some of the compliance risks around the [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*

135 Letter from DG MI5 to SSHD (MI5 Core Doc 80) **[C3/169/1-2]**.

*to the Investigatory Powers Commissioner.*"[136] The other findings have not been disclosed in the OPEN version.

107 In the First Inspection Report, a RAG rating is included in respect of "[Data Type 1]", as follows:[137]

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*] |

108 It is therefore apparent that there is a "*RED*" rating against an "*IPA safeguard*" (which may be "*LPP*", "*copying of data*" or "*access controls*" – the Claimants and the public served by MI5 are apparently not permitted to know which of the requirements of the IPA have been breached, in addition to the "*RED*" RRD rating. There are also "*AMBER*" ratings for another two areas. It further explained that a "*RED*" rating indicates "*serious compliance gaps*" and amber indicates "*some compliance gaps*" (§4.1.6).[138] Thus the First Inspection Report identified that, in relation to one data type, MI5 is not complying with four out of five IPA safeguards.

109 The First Inspection Report contains five further such tables,[139] apparently relating to different "*[Data Types]*" (or means of obtaining or holding data). The Claimants infer 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

136 IPCO Inspection Report-MI5 (Audit of the [Technology Environment]) Version 2 (MI5 Core Doc 73) **[C3/151/3]**.

137 IPCO Inspection Report-MI5 (Audit of the [Technology Environment]) Version 2 (MI5 Core Doc 73) **[C3/151/5]**.

138 IPCO Inspection Report-MI5 (Audit of the [Technology Environment]) Version 2 (MI5 Core Doc 73) **[C3/151/4].**

139 IPCO Inspection Report-MI5 (Audit of the [Technology Environment]) Version 2 (MI5 Core Doc 73) **[C3/151/7-10]**.

"*RED*" ratings and four "*AMBER*" ratings. The basis for the non-provision/gisting of the data-type is unclear but the Claimants infer it must be that the legal risks (whether in criminal or civil proceedings) that may flow from illegally obtained, retained or shared data being identified, either for the Respondents or for their intelligence partners (in the case of sharing), are such that it is said to be contrary to national security to reveal failings of this type and gravity.

110 On 1 April 2019, MI5 issued Annex H (an attachment to the Handbook for Judicial Commissioners), which set out the "*mitigations*" MI5 had implemented and explained on what basis MI5 considered that warrants could lawfully be issued to it.[140] Annex H stated that the First Inspection Report had rated compliance with LPP safeguards as an "*AMBER*" risk in relation to some data (§§49-53).[141] It recorded that:

110.1 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*" (§50); and

110.2 There were two further "*compliance risk[s]*" that related to requirements to mark LPP material (once it has been identified as privileged): some systems within the "*TE*" did not allow LPP 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*" (§§52-53).

111 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. In these circumstances, it is impossible to see how any warrant where there was any risk of obtaining LPP material could lawfully have been issued.

---

140 Annex H-Section II: further information about [the TE] and the mitigations being progressed (MI5 Core Doc 74) **[C3/154/1]**.

141 Annex H-Section II: further information about [the TE] and the mitigations being progressed (MI5 Core Doc 74) **[C3/154/5]**.

112 On 26 April 2019, IPCO's Second Inspection Report was published, further to a follow-up inspection of MI5 by IPCO on 15-16 April 2019, stating that there were two "*RED*" recommendations and a further three "*AMBER*" recommendations (§3.1.1), the majority of which remain entirely secret.[142]

*(c) Generic Warrants Decision*

113 On 5 April 2019, Fulford LJ (the IPCr) issued the 'Generic Warrants Decision'.[143] He summarised MI5's failure as follows: "*MI5 has inadequate control over where data is stored; [REDACTED]; and the deletion processes which applied to it.*" (§10)[144] Specific errors Fulford LJ identified include the absence of proper mechanisms for RRD of retained data and an absence of effective safeguards relating to LPP material (§§12, 19).[145]

114 Fulford LJ referred to "*the undoubted unlawful manner in which data has been held and handled*", and gave "*file shares*" and "*data stores*" as examples of this (§10).[146] Other errors include "*Copying of Data*" and "*Access Controls*" (§12).[147]

115 Fulford LJ, on the basis of the material then before him, made clear that these serious and systemic failings: (i) had existed unremedied after MI5 first identified them in 2016 (it is unclear whether he had sight of the pre-2016 material, including in particular any minutes from meetings of the MI5 Management Board in May 2013 and November 2014); and (ii) still persisted in relation to data obtained prior to the Generic Warrants Decision on 5 April 2019.

116 Fulford LJ noted that, when the significant issues in the TE were (eventually) disclosed to him, they were underplayed by MI5 (§9).[148] Fulford LJ held that warrants had been

---

142 IPCO Inspection Report: [Technology Environment] follow up inspection 15-16 April 2019 (MI5 Core Doc 82) **[C3/171/3-4]**.

143 Applications for approval of warrants by the Home Office: Decision: the TE and Compliance (MI5 Core Doc 77) **[C3/165]**.

144 Applications for approval of warrants by the Home Office: Decision: the TE and Compliance (MI5 Core Doc 77) **[C3/165/3]**.

145 Applications for approval of warrants by the Home Office: Decision: the TE and Compliance (MI5 Core Doc 77) **[C3/165/3, 5]**.

146 Applications for approval of warrants by the Home Office: Decision: the TE and Compliance (MI5 Core Doc 77) **[C3/165/3]**.

147 Applications for approval of warrants by the Home Office: Decision: the TE and Compliance (MI5 Core Doc 77) **[C3/165/3]**.

148 Applications for approval of warrants by the Home Office: Decision: the TE and Compliance (MI5 Core Doc 77) **[C3/165/3]**.

issued to MI5 on a basis that MI5 knew to be incorrect and, under the IPA, Judicial Commissioners were given false information. He said at §3:[149]

> "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." (emphasis added)

117 Similarly, at §6, Fulford LJ said:[150]

> "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. 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." (emphasis added)

118 At §44, Fulford LJ said:[151]

> "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 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."

---

149 Applications for approval of warrants by the Home Office: Decision: the TE and Compliance (MI5 Core Doc 77) **[C3/165/1]**.

150 Applications for approval of warrants by the Home Office: Decision: the TE and Compliance (MI5 Core Doc 77) **[C3/165/2]**.

151 Applications for approval of warrants by the Home Office: Decision: the TE and Compliance (MI5 Core Doc 77) **[C3/165/8]**.

119 Fulford LJ stated 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*" (§4), namely, that:[152]

> "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."

120 Fulford LJ observed 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*" (§46).[153] It seems that inspections and audits had previously been conducted without such access, but this had somehow been treated as sufficient.

121 At §49, Fulford LJ concluded:[154]

> "This is a serious and inherently fragile situation. …. 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'. 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)

**(3) Belated notification of compliance issues relating to TE2**

122 On 3 May 2019, the Oversight and Errors Team of MI5 set out to IPCO the preliminary error reports by MI5. It stated:[155]

122.1 MI5 was "*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.*" As far as the Claimants can tell on the

---

152 Applications for approval of warrants by the Home Office: Decision: the TE and Compliance (MI5 Core Doc 77) **[C3/165/1]**.

153 Applications for approval of warrants by the Home Office: Decision: the TE and Compliance (MI5 Core Doc 77) **[C3/165/8]**.

154 Applications for approval of warrants by the Home Office: Decision: the TE and Compliance (MI5 Core Doc 77) **[C3/165/9]**.

155 Letter to IPCO from MI5 (MI5 Core Doc 83) **[C3/173/2-3]**.

basis of the OPEN materials, nothing of the issues relating to "*[other areas]*" has been disclosed;

122.2 MI5 would "*have particular regard to the [REDACTED] results of selection for examination*", a statutory process applying only to bulk powers. This confirms that the defects extend to bulk data; and

122.3 MI5 continued (as at May 2019) to investigate "*potential issues related to [two areas of another technology environment: TE2]*" (§4). The letter suggested MI5 continued to have little idea of what data it holds and, even today, cannot properly audit it. Thus on page 3 it states 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 remained unable to document the current and historic state of its bulk data holdings and how those holdings have been or will be processed (despite concerns about compliance in the TE2 being known since at least 2010). In such circumstances, there had 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.

123 On 8 May 2019, Fulford LJ raised concerns 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."[156]

Again, this account suggests that Fulford LJ was not made aware of the materials (set out above) suggesting problems in TE2 as far back as 2010 (in respect of TE2 Area 1) and 2012 (in respect of TE2 Area 2), if not earlier.

124 On 9 May 2019, Andrew Parker replied in the following terms:[157]

> "2. In our letter we provided a synopsis of current investigations, none of which is yet confirmed as a reportable error. In your response you raise a concern that two of these investigations, relating to two discrete systems in the [TE2 (TE2 Areas 1 & 2)] seem to indicate 'underlying problems' in [TE2] akin to those in the [TE]. I would like to assure you that we do not assess this is the case; our investigation has identified only these two discrete [REDACTED] areas as of concern. There is nothing to suggest any wider concerns in connection with [TE2] as a whole.
>
> 3. We have historically followed the agreed protocol with IPCO of notifying you only once we have confirmed that a reportable error has occurred (even if the full extent and detail is not known at that point). We have not previously provided notification of ongoing investigations where, as in this case, we have not established that an error has actually occurred. However, given the ongoing [TE] concerns, we had considered that it was better to provide early sight of our investigations. I know you are also considering whether ways of working should change in future and I would be grateful therefore if my senior team could work with yours to consider how to handle such matters in future."

125 By letter dated 15 May 2019, MI5 responded to Fulford LJ's letter of 8 May 2019. It disclosed 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:[158]

> "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, even after like concerns were raised as far back as 2010 (in respect of TE2 Area 1) and 2012 (in respect of TE2 Area 2), there cannot have been proper oversight or an effective system of control.

---

156 Letter from IPCO to DG MI5 (MI5 Core Doc 84) **[C3/174/1]**.
157 DG MI5 reply to IPC letter of 8 May 19 (IPCO Doc 14) **[C3/174A/1]**.
158 Letter from Oversight and Errors team MI5 to Sir Adrian Fulford (MI5 Core Doc 85) [**C3/178/1]**.

### (4) The Compliance Improvement Review

126 In 2017, Liberty brought a claim for judicial review concerning the compatibility of the IPA with both EU and ECHR law (the "**IPA Claim**"). After the conclusion of the second substantive hearing in the IPA Claim on 21 June 2019, the Defendants in that claim disclosed on 15 July 2019 and published online the CIR Summary, which is a summary of the independent review into MI5's serious, systemic and longstanding failure to observe statutory safeguards on access control, copying, RRD and LPP for information obtained under warrants. A redacted version of the CIR was subsequently disclosed. The Summary demonstrates that:

126.1 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);[159]

126.2 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). MI5 had a "*lack of urgency in reducing the legal risks*" and systems lacking essential safeguards were expanding (§11).[160] There was "*a sustained organisational failure to appreciate the extent of the compliance problem and its consequences*" (p.3);[161] and

126.3 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). 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), although it is difficult to understand how this generous conclusion can be justified given the disclosure now provided to the

159 Compliance Improvement Review – Summary of Key Findings (MI5 Core Doc 86) **[C4/184/1]**.
160 Compliance Improvement Review – Summary of Key Findings (MI5 Core Doc 86) **[C4/184/2]**.
161 Compliance Improvement Review – Summary of Key Findings (MI5 Core Doc 86) **[C4/184/4]**.

Claimants. But he qualifies this, stating that "*the information shared was insufficient to highlight the increasingly urgent problems caused by continuing compliance difficulties*" (§12).[162]

126.4 There was no prospect of MI5's compliance in the near future. A striking recommendation is that "*MI5 must ensure that all its data can be shown to be held in accordance with legal compliance requirements by June 2020*."[163] The reviewer considered that the issues (it is inferred with TE or TE2) had not been resolved.[164] 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.

126.5 Fundamental change was required to comply. Recommendations 1-14 seek the creation of a "*compliance culture*" in MI5.[165] This required a fundamental "*step change*" to comply with the IPA.[166]

127 The Respondents have now also belatedly disclosed redacted versions of the interviews by the reviewer, Sir Martin Donnelly (the contents of which are not addressed in their evidence for these proceedings). A striking picture of institutional non-compliance in the Home Office and MI5 is evident from those interviews. A meeting note for Peter Fish, GLD Deputy General, dated 20 May 2019 stated as follows:[167]

> "[Sir Martin Donnelly ("**SMD**")] and [Peter Fish ("**PF**")] discussed who decides on legality. Sir Adrian Fulford (SAF) had felt MI5 were sailing close to the wind and he could have called it either way. MI5 consider their legal view as the only. [REDACTED]
>
> PF shared his personal view that he felt that there was a cultural issue in MI5. There was a distinct lack of movement in the lawyers. He mentioned a recruitment campaign where the MI5 'lifer' was seen as a better candidate than an external lawyer. The general GLD culture of 'phone a friend' approach to any legal issue for discussion/consideration was not something that was replicated with MI5 lawyers. Any issues continued to be internalised. MI5 lawyers see their position is to defend MI5's position. There is regular contact with the MI5 lawyers, but this issue was not shared.

---

162 Compliance Improvement Review – Summary of Key Findings (MI5 Core Doc 86) **[C4/184/2]**.
163 Compliance Improvement Review – Summary of Key Findings (MI5 Core Doc 86) **[C4/184/9]**.
164 Compliance Improvement Review – Summary of Key Findings (MI5 Core Doc 86) **[C4/184/3]**.
165 Compliance Improvement Review – Summary of Key Findings (MI5 Core Doc 86) **[C4/184/5-8]**.
166 Compliance Improvement Review – Summary of Key Findings (MI5 Core Doc 86) **[C4/184/9]**.
167 Meeting note for Peter Fish (CIR Interview Doc 4) **[C3/178F/1]**.

> PF explained GLD and HOLA are not resourced to 'oversee' MI5 working and believe their lawyers should do so. PF mentioned that correspondence often went to IPCO before it came to light at the Home Office [with the inference that ideally it should be the other way around].
>
> What needed strengthening? Both legal and policy oversight from the Home Office. PF noted that the HO pulled back from the more rigorous oversight in the 70s/80s."

128 A note of a meeting between MI5's "*[Information, Security, Compliance and Strategic Policy Director]*" and Sir Martin Donnelly contains several damning observations about MI5's 'non-compliance' culture.[168] An observation is also noted in a meeting between "*[a member of the information specialists team*] and Sir Martin Donnelly, that "*at the SMG level we need to see a cultural change*".[169] The interviews also contain information about the knowledge of Mr Graeme Biggar at the Home Office – for example that "[w]*hen the IPA was implemented Graeme had no concerns and was satisfied with MI5's rating*" [170] – and about failures in Home Office oversight of MI5, such as the (near invariable) cancellation of meetings between DG MI5 and the Home Secretary.[171]

### (5) Subsequent developments

129 Between 3 and 5 June 2019, IPCO conducted its third inspection of the TE at MI5. On 22 July 2019, the Third Inspection Report was published.[172] As part of the "*Key findings*", it was recorded that "*MI5 must urgently complete work to understand the extent to which warranted data is held [in the TE] and initiate a process to delete any non-compliant data. ...*". This was described as a "*Core recommendation: improvement must be made*."[173] On 9 August 2019, MI5 indicated that its "*scanning and analysis ... across [an area] on the [TE] is now [a high %] complete]*" and *"[the redacted text explains why the analysis may not be conclusive and why MI5 does not consider further analysis is practical to complete]*";[174] MI5 therefore appears to be resigned to not understanding the extent of authorised data handled in error in areas of the TE.

---

168 CIR Interview Doc 5 **[C3/178G/1]**. For example: "*The challenge can be that the mission is prioritised over everything else. Compliance can often be in conflict at times*" (page 2); "[t]*he broader accountability was not something that struck [Information, Security, Compliance and Strategic Policy Director] as being understood within MI5*" (page 2); "[t]*here wasn't a joining up of the dots…compliance…therefore a warrantry problem. MI5 could have twigged earlier that the warrantry would be affected – this was very late in the day…Unfortunately it was assumed it was "always like this" and so overlooked*" (page 2).

169 CIR Interview Doc 13 **[C4/183D/2]**.

170 CIR Interview Doc 12 **[C4/183C/1]**.

171 CIR Interview Doc 16, §7 **[C4/183G/3]**.

172 [TE] Inspection Report (MI5 Core Doc 89) **[C4/190/1]**.

173 [TE] Inspection Report (MI5 Core Doc 89) **[C4/190/2]**.

174 MI5 notification of errors in [an area of the TE] (IPCO Doc 24) **[C4/192A/1]**.

130 A fourth inspection of the TE was conducted on 23 and 24 September 2019. The Fourth Inspection Report was published on 22 October 2019.[175] It stated that "*MI5 is at an early stage of its work to delete [REDACTED] warranted data from [TE] but has a viable plan in place delete data* [sic] *held on [particular areas] in [TE] which has gone past its agreed retention period*." (§3.2.1)[176] This noted that, as of 18 September 2019, "*MI5 had reported ten relevant errors associated with [TE]*" and "*[a] further twelve potential errors were under active investigation by the MI5 errors team*" (§5.6.1); and *"[s]everal of the errors summarised above are very significant in scale: one error, for example, related to the retention of [material] October 2016, none of which was deleted from [an area]*" (§5.6.2).[177] The report also noted that in IPCO's Second Inspection Report, IPCO had "*identified two risks associated with the use of [a particular area] in the [TE]*, and that as for the two recommendations that IPCO had made in respect of those risks "*neither… had been discharged*" (§5.2.1).[178]

131 Further detail was provided in IPCO's 'Annual Report: Confidential Annex 2019'.[179] Examples of the relevant errors associated with the TE were provided, such that a category of warranted data "*obtained by MI5 since 2016 was retained and was not subject to any deletion policy*".[180] And in relation to "*[an area] within [TE2]*", there were further "*significant errors*" including that MI5 made copies of data but "*failed properly to apply the relevant retention and deletion policies to data within these copies"* and the data *"was being held in breach of MI5's handling arrangements and the IPA's safeguards*". And, as a result of not activating an auto-delete function upon commencement of the relevant IPA provisions on 29 June 2018, *"MI5 had been holding the content of [some data] in error since June 2018"*.[181]

132 In February 2020, IPCO conducted an investigation of MI5's safeguards. A report, 'Inspection Report: Security Service Safeguards Inspection',[182] required MI5 to review the adequacy of safeguards and/or provide further information in relation to LLP material (§§3.1.1, 4.1.4-4.1.9) and RRD processes (§§3.1.1, 4.2.3).

---

175 IPCO Inspection Report [TE] September 2019 (MI5 Core Doc 93) **[C4/199/1]**.
176 IPCO Inspection Report [TE] September 2019 (MI5 Core Doc 93) **[C4/199/3]**.
177 IPCO Inspection Report [TE] September 2019 (MI5 Core Doc 93) **[C4/199/9-10]**.
178 IPCO Inspection Report [TE] September 2019 (MI5 Core Doc 93) **[C4/199/7]**.
179 IPCO Annual Report 2019: Confidential Annex **[C4/215/3, 4]**.
180 IPCO Annual Report 2019: Confidential Annex §9.3 **[C4/215/3]**.
181 IPCO Annual Report 2019: Confidential Annex §9.5 **[C4/215/4]**.
182 IPCO Inspection Security Service Safeguards Inspection (Calam/6) **[C4/221/1]**.

133 In December 2020, the report by Mary Calam (the "**Calam Report**") was published to consider progress on the three areas identified by the CIR.[183] The summary of the report noted that "*Not all Sir Martin's recommendations have yet been fully implemented …*".[184] It also made clear that MI5's data holdings remain non-compliant:[185]

> "ARE MI5'S DATA HOLDINGS NOW LEGALLY COMPLIANT?
>
> MI5 has reviewed its data holdings to identify relevant systems and infrastructure storage assets, assess the legal compliance risk for each and develop mitigations for identified risks. Implementation of those mitigations continue. While there is more still to be done, the broader changes that MI5 has made to strengthen its legal compliance risk management processes, instil a culture of individual accountability for legal compliance risk and ensure that compliance is built in to new products should give Ministers greater confidence that new risks will be identified early and addressed promptly."

134 The Calam Report stated as follows:[186]

134.1 "*MI5 assess (in January 2021) that [a percentage] of [areas] and [a percentage] of [areas] are currently fully compliant with the legal compliance standards that were introduced in February 2020 (see Recommendation 3 below), with some potential compliance risk in the remainder MI5 have a high degree of confidence that by July 2021, [a percentage] of [areas] and [a percentage] of [areas] will have been confirmed to be legally compliant (subject to covid restrictions [REDACTED])*";[187]

134.2 Of the systems identified as posing a compliance risk: "*Mitigations have been identified for [most of the] systems (of which [a percentage] are manual interventions, such as policy or process changes and [some] are technology solutions). As yet, [only a small proportion] of mitigations have been implemented, but MIS anticipate that the majority will be in place by mid 2021. MI5 has a high degree of confidence that [a high percentage] of the higher risk systems will be fully compliant by July 2021. However, a small residual number which require [more] resource are unlikely to be completed until [later]*";[188]

---

183 Mary Calam Report – Compliance Improvement Review: Independent Verification **[C4/219]**.
184 Summary of Mary Calam Report **[C4/220/2]**.
185 Summary of Mary Calam Report **[C4/220/3]**.
186 Mary Calam Report – Compliance Improvement Review: Independent Verification **[C4/219]**.
187 Mary Calam Report – Compliance Improvement Review: Independent Verification **[C4/219/9]**.
188 Mary Calam Report – Compliance Improvement Review: Independent Verification **[C4/219/32]**.

134.3 "*So far the review has focused on higher priority [infrastructure] including the [areas] for the [TE2 Area 1], the new file share [areas] created during the [TE] remediation, [TE areas] [REDACTED]. This has identified one issue which requires further investigation to establish whether it needs to be reported to IPCO as a relevant error under the IPA and a range of other changes needed, including more consistent assurance processes across MI5 [REDACTED]. MI5 assesses that in January 2021 [over half] of higher risk [infrastructure] are now legally compliant and that this will have risen [significantly] by July 2021*";[189] and

134.4 "*Mitigations for any relevant errors under the IPA will be prioritized. The Summary Action mitigation roadmap anticipates that mitigation work will not be completed until at least 2022.*"[190]

135 There is no recent update since the Calam Report.

136 In May 2021, IPCO conducted a further investigation into the safeguards in place within MI5 to protect material obtained under investigatory powers. From the report, 'Inspection Report: MI5 Safeguards Inspection',[191] it is apparent that MI5 is unable to give assurance that all data on all areas of the TE is held compliantly with statutory safeguards. It noted that "*MI5 have confidence that [a high percentage of data] in [particular areas of the TE] is assured*" (§5.7.3) and that "*MI5 assess [over half] of higher risk systems as compliant*" (§5.7.15). The obvious implication is that there is a percentage (perhaps low) where data is not assured, and that less than half of the higher risk systems are still not compliant.

137 In recent weeks (9 June 2022), MI5 has reported a further "[f]*ailure to adhere to safeguards*" to IPCO. According to MI5's report, which was disclosed to the Claimants on 30 June 2022, "*[Authorised material] [was] found to have been retained after there were no longer any relevant grounds to retain the information*". The report noted: "*We therefore assess that this case may be symptomatic of a more systemic issue, that there is likely to be further warranted or authorised [material] that has been stored in [the TE] for longer than is necessary and proportionate, and that the failure to enforce the necessary safeguards is likely to have resulted in the occurrence of further breaches*"

189 Mary Calam Report – Compliance Improvement Review: Independent Verification **[C4/219/34]**.
190 Mary Calam Report – Compliance Improvement Review: Independent Verification **[C4/219/37]**.
191 IPCO Inspection Report: MI5 Safeguards Inspection **[C4/223G/1]**.

(emphasis added). It stated that a formal investigation has been opened into the issue.[192] As such, even now it is apparent that there are and remain "*systemic*" failures to comply with statutory safeguards in the TE.

## C THE EXISTING BPD/BCD CLAIM

138 Various references have been made above to the Existing BPD/BCD Claim. The Amended Grounds of Claim, at §§62-105 **[A1/5/26-38] [Core/4/26-38]**, and the chronology at Appendix 1 **[A1/5/61-67] [Core/4/61-67]**, set out the circumstances of the Existing BPD/BCD Claim, and the position that was being adopted by the Respondents in that claim to this Tribunal, in parallel to their understanding of the unlawfulness of the underlying position.

139 Further to the Order of the Tribunal dated 14 February 2020, paragraphs 2 and 19 **[A2/31/2, 4]**, there is an application to re-open the Existing BPD/BCD Claim which is stayed pending determination of the present issues. However, the Tribunal at this hearing is considering the key factual issue in the area of overlap, namely the extent to which there was a breach of the duty of candour by the Respondents to the Tribunal in those proceedings.

140 The Claimants' position is that the fact that there was systemic unlawful holding of BPD and BCD (or their product) by MI5, and that this had gone unreported to and unobserved by the mechanisms for oversight for many years, was obviously a material factor to bring to the attention of the Tribunal. The Respondents in the Existing BPD/BCD Claim could not have, and should not have, assured the Tribunal as to the ECHR-compliant nature of the manner in which BPD and BCD (or their product) would be held. Had the crucial facts unearthed in this claim been disclosed, the Tribunal's decision in the Existing BPD/BCD Claim could not have been as it was. The Tribunal was seriously misled.

141 The Respondents have two responses, at Amended OPEN Response §§98-99 **[A1/6/27] [Core/5/27]**.

---

192 Letter from MI5 to IPCO **[C4/223P/1-2]**.

141.1 First, as regards BPD, the Respondents contend that the BPD/BCD claim concerned only the pre-IPA legal regime for BPDs, and the pre-IPA regime did not require BPDs to be retained or examined subject to warrants or directions.

141.2 Second, as regard BCD, the Respondents contend that "*BCD obtained pursuant to [directions under s.94 TA84] was and is not held in the TE or TE2 Area 1 or Area 2*".

It was presumably on that basis that the Respondents wrote to the Tribunal on 7 June 2019 asserting that the issues with the TE were not considered to be *"relevant to any issue which remains for consideration by the Tribunal"* in the Existing BPD/BCD Claim (see Amended Grounds of Claim §102 **[A1/5/37] [Core/4/37]**). Each of the Respondents' justifications is wrong.

**(1) BPD**

142 First, the Respondents in the Existing BPD/BCD Claim argued that the regime for handling BPD/BCD was lawful under the ECHR because there were procedures and Handling Arrangements in place which imposed equivalent safeguards to those in legislation. If those safeguards in policies were not in fact being complied with, that was plainly a matter that had to be disclosed to the Tribunal. It was not so disclosed. The Respondents were therefore required to engage with the Claimants' allegations of breach of candour in respect of BPDs, rather than dismiss them as irrelevant (cf. MI5 A2 §220 **[B/2/36] [Core/9/36]**).

143 Secondly, the Respondents are wrong to contend that the Existing BPD/BCD Claim concerned only the position prior to the IPA being made. The claim is not and was not so limited; in any event, the pre-IPA regime, due to delayed commencement and complex transitional provisions, extended far beyond November 2016 to 22 February 2019.[193] Further, the IPA does not create *new* powers in respect of BPDs but rather provides an authorisation procedure for the acquisition and use of BPDs; and nor is the acquisition of BPDs limited to Part 7 IPA (see '*Intelligence services' retention and use of bulk personal datasets: Code of Practice*', March 2018, para 2.11). At the very first hearing of the

[193] The Investigatory Powers Act 2016 (Commencement No. 7 and Transitional and Saving Provisions) Regulations 2018, Regulation 8.

Existing BPD/BCD Claim, the IPA had not yet been made, and the Tribunal was instead addressed on the Bill that became the IPA. However, the Existing BPD/BCD Claim proceedings remain extant. The relevant legal position has continued to be considered by the Tribunal.

144 The Respondents' suggestion that the proceedings as to BPDs are "closed" is especially untenable in circumstances where, in the Tribunal's third judgment (23 July 2018), the Tribunal re-opened its first judgment (17 October 2016) as to the lawfulness of s.94 directions after November 2015, in light of further disclosure that had been given in the proceedings. Various issues remain for resolution in the Existing BPD/BCD Claim, including issues that have been stayed behind these proceedings. The duty of candour is not 'once and for all', but is an ongoing duty. MI5 should have thought whether what it had been telling the Tribunal was true, and should have made disclosure in the Existing BPD/BCD Claim proceedings once it was apparent that it was not.

145 In any event, the fact that the pre-IPA regime for BPD retention and examination was not subject to warrants/authorisations is not an answer to the issues raised in this claim. The defects identified in relation to RRD, LPP and beyond are just as much an (apparent) breach of the MI5 BPD Handling Arrangements that applied before the IPA to **ensure** Article 8 compatibility: see, e.g. Amended Grounds of Claim §§67, 69, 76 **[A1/5/27, 28, 30] [Core/4/27, 28, 30]**; and the Tribunal's knowledge of such systematic and systemic breaches, including the bypassing of the IOCCO, would have informed its view of the compliance of the system in the round or of the value of Handling Arrangements. It is notable in the materials cited above how frequently they refer to compliance risks in relation to Handling Arrangements. In that connection, it is important to note that it is systematic or systemic breaches that are germane: see the recent judicial review of an aspect of the Tribunal's third judgment (sharing BPD with international partners) in *R* (*Privacy International) v Investigatory Powers Tribunal* [2022] EWHC 770 (QB) at [73] and [93], referring on those facts to the "*critical finding of the majority that the "episodic" problems it identifies do not demonstrate that there was "systemic failure"*".

**(2) BCD**

146 The Respondents have refused to explain in OPEN the extent to which there is a relationship between communications data obtained in bulk under s.94 TA and the

TE/TE2. The Respondents have confirmed that the datasets in bulk have not been held in those areas. But their position as to whether the product of s.94 directions has been so held has been entirely redacted (see e.g. Amended OPEN Response to RFI §124(d)-(f) **[A1/10/33] [Core/6/33]**). The Claimants have proceeded on the assumption that such product is so held. It is material to the legality of s.94 directions to know that the product of the direction would be held unlawfully; the fact that it relates to an extract from the dataset rather than the dataset itself is therefore (contrary to the position that appears to be adopted by the Respondents) no answer to unlawfulness of its holding.

147 While the question of re-opening the judgment in the Existing BPD/BCD Claim is not being determined now, the Tribunal's first judgment of the Existing BPD/BCD Claim was materially based on assurances as to compliance with Handling Arrangements post-avowal, and the evidence set out above is irreconcilable with the Tribunal's conclusions in relation to MI5 in that first judgment: see Amended Grounds of Claim §150 **[A1/5/56-57] [Core/4/56-57]**. The breach of the duty of candour has been both flagrant and material.

148 The Respondents have subsequently recognised their ongoing duty of candour, and in July 2021 indicated that further documents fell to be disclosed. Pursuant to paragraph 24 of the Order of the Tribunal dated 4 January 2022 **[A2/53C/5]**, the Respondents were to disclose by 21 January 2022 any agreed OPEN gist of the documents, but no such gist was provided. The Claimants have been told that the documents consist of notifications or updates to IPCO sent in the period 2019 to 2021, detailing instances of MI5's retention of data beyond the relevant RRD periods (presumably those in the Handling Arrangements accompanying the s.94 directions, as well as s.8(4) warranted data) or when no longer necessary. It is not clear why these documents, which are obviously relevant to the systemic failures in RRD, have not been disclosed.

## D SCOPE OF THESE PROCEEDINGS

149 An issue has arisen between the parties, and which was ventilated before the Tribunal at the directions hearing in April 2022, as to the proper scope of these proceedings. The Claimants' position is that their claim, as pleaded, extends to all systemic defects in MI5's holding of data. The Respondents' position is that they are entitled unilaterally to narrow the scope of the claim to the particular systemic issues that MI5 decided to report

to the IPCr in 2019. However, the Claimants already have an indication that such other systemic issues existed or exist at the material time, albeit they cannot be identified meaningfully in OPEN: see, for example, paragraph 122.1 above, and the issue of 'Workings' at paragraph 63 above; at least potentially, the issue falling for disclosure in the Existing BPD/BCD Claim (see paragraph 148 above); and MI5 A2 §86(d)(ii) referring to *"wider compliance risks of which [MI5] was aware"* **[B/2/16] [Core/9/16]**.

150 The relevant correspondence is at **[D2/199] [Core/23]** (Claimants' letter dated 8 February 2022); **[D2/205] [Core/25]** (Respondents' letter in response dated 28 February 2022); **[D2/211] [Core/27]** (Claimants' letter in response dated 25 March 2022); and **[D2/214] [Core/28]** (Respondents' letter in response dated 1 April 2022). The Claimants' proposed approach, given the limited time that remained before this substantive hearing, was that this hearing would consider the failings in respect of the TE and TE2 Areas 1 and 2 that were notified to the IPCr in 2019. However, the Claimants maintain their position that other "similar fact" failings – failings which may be characterised as systemic, rather than one-off errors – across MI5's data holding systems remain relevant. The existence of such other systemic flaws is obviously material to the conclusions that the Claimants are inviting the Tribunal to draw. The Tribunal is therefore invited in its judgment to confirm the relevance of such other matters, and to direct that the Respondents make disclosure to the Claimants in respect of them. Upon such disclosure, the parties can return to the Tribunal with proposed directions, including as to whether it is necessary to have a further hearing, or whether matters arising out of the further disclosure can be determined in light of written submissions.

## E SUBMISSIONS

151 The Claimants' submissions are structured as follows:

151.1 First, brief submissions on the factual position;

151.2 Second, the question of the Claimants' standing;

151.3 Third, the challenge to legality of the warrants obtained (and data under them) and bulk data;

151.4 Fourth, the systemic challenge to the compatibility of the legal regimes; and

151.5 Fifth, relief.

## (1) Factual Position

### *(a) MI5*

152 By way of summary of the underlying disclosure (the understanding of which may alter following oral evidence and subsequent gisting):

152.1 MI5 knew about a series of serious failings with the basic requirements for compliance with Articles 8 and 10 ECHR, and with fundamental statutory requirements (augmented by Codes of Practice, such as §§6.3 to 6.10 of the Code of Practice for Equipment Interference issued in 2016) imposed on it by Parliament for the issue of warrants (under RIPA, ss.5, 7 of the Intelligence Services Act 1994 (equipment interference) and IPA) as far back as 2010. MI5's own case is that it knew that the TE represented legal and compliance risks "*since at least 2015*" **[C3/178M/1]**;

152.2 MI5 did not fix these issues;

152.3 Notwithstanding knowledge at the highest levels of MI5,[194] which extends back as far as May 2013 at Board level, and to 2012 below that, MI5 did not itself report the issues to the Secretary of State, the Tribunal or its regulators for several years. That was notwithstanding being directly asked about such issues by the Commissioner in 2013 (see paragraph 26 above). When it did finally report these matters to the IPCr in February 2019, MI5 was not frank and made at best a partial and incomplete report;

152.4 These problems were not separately identified by the IPCr (or predecessors under RIPA) in IPCO's audit role;

152.5 More fundamentally, at no stage during any warranting or authorisation process before May 2019 was the extent of the RRD problems even arguably properly

[194] Note also the terms of MI5's concession made at an earlier directions hearing and recorded at **[A1/14/1]**: "*any matter set out in any of the documents MI5 has so far disclosed, evidencing knowledge within MI5 of the compliance issues arising in the present proceedings, is accepted as being within the knowledge of MI5 itself*".

disclosed. That is true whether the warrant/authorisation was granted by the Secretary of State (on the application of MI5); or with the "double lock" or Judicial Commissioner review or its equivalent. Both modes of warrant grant called for full and frank disclosure to Secretary of State and (where applicable) the judge; and

152.6 Nor were such defects disclosed in the litigation designed to explore the legality of BPD/BCD authorisations and handling practices. Even in the litigation concerning the IPA (the IPA Claim), (incomplete and partial) disclosure was only provided only after the substantive hearing even though that material was available before.

153 In these proceedings, the Respondents seek to belittle the seriousness of the failings in three ways.

153.1 First, the Respondents contend that it is "*important to distinguish for the purposes of this case between matters identified as "compliance risks", and actual failures to comply*" (Amended OPEN Response §4 **[A1/6/2-3] [Core/5/2-3]**, §61(c) **[A1/6/16] [Core/5/16]**). For the reasons explained further below, it is not accepted that this is a legally relevant distinction. In any event, it is unclear how MI5 consistently distinguishes between "actual failures" and "risks" of not complying, e.g. in circumstances where it was impossible to flag LPP material and MI5 did not know what material it held in the TE. What, it may be asked rhetorically, is the respectable legal argument that would suggest any of these practices complied with the law? It is notable the Secretary of State cannot find one, even now. Certainly Fulford LJ thought the matter a black and white one of clear breach. He was right to do so where MI5 did not even know what material it held in the TE. Further, the Claimants submit that it is not open to the Respondents to rely in this way on any distinction between "*compliance risks*" and "*actual failures to comply*" in circumstances in which MI5 admits it itself wrongly interpreted extant non-compliance as "risk".[195]

153.2 Second, and relatedly, the Respondents seek to focus on material having been held in excess of the appropriate retention period as the *only* real issue with the TE (see e.g. Amended OPEN Response §5(c)(iv) (**[A1/6/4] [Core/5/4]**). That attempt at a

[195] See, for example, Amended OPEN Response to RFI §§ 87, 94, 105, 112; see also Parties' OPEN Scott Schedule pp.16-18.

self-serving "framing" of the issues is not capable of being sensibly maintained in light of the contemporaneous documents. Even from the OPEN materials it is evident the problems were far more extensive, and amounted to all the problems that flowed naturally from not having controlled information or its copying, such that MI5 neither knew what they (or others) had, or had had, whether they still had it, and if so (to any of the above) where. Much of the detail has been redacted but see, for example:

(a) the RAG tables, summarised at paragraphs 106-109 above;

(b) MI5's treatment of LPP material (§110.2 above): see MI5 A2 §168 *"Some parts of the TE did not enable LPP material to be flagged"* **[B/2/31] [Core/9/31]**; Amended OPEN Response to the RFI §31 "*not all systems within the [TE] enabled material to be flagged as LPP*" **[A1/10/8] [Core/6/8]**; email from March 2018 indicating that the RED risks included risks "*in relation to the [systems handling of confidential material (particularly material subject to Legal Professional Privilege)]*" **[C2/93/3]**;

(c) that users are able to access information in TE without having a clear necessity and proportionality case for doing so: see paragraph 86.2 above; MI5 A2 §119: "*it has become apparent that appropriate access control was not always put in place*" **[B/2/24] [Core/9/24]**; "*risk associated with access*" **[C2/96/3]**; and "*risks identified are largely associated with … access to … warranted data*" **[C3/164/1]**; and

(d) the repeated references (particularly germane in view of the litigation in the IPT and beyond) to MI5's inability to provide compliant disclosure when required, a direct function of being unable to say what their data holdings were and are; see paragraphs 34, 45, 50, 55.3, 60, 69 and 70.5 above.

153.3 Third, MI5 contends that its failure to disclose matters to the IPCr or Judicial Commissioners "*was a matter of insufficient understanding of the factual position and of its obligations in light of that position, rather than deliberate default*" **[A1/6/18] [Core/5/18]**. That is of course no answer, even if true. And it does not appear to be true. The contemporaneous documents above show that there was adequate understanding for MI5 to act upon and find out about its systemic

breaches, right back to 2010, if it had made the legality of operations a matter of concern and had investigated the matter. Certainly the position from 2012/2013 onwards was inexcusable, when the defects in TE and TE2 Areas 1 and 2 were known and yet not disclosed in response to a direct request for this very sort of information, from the regulator whose function it was make such requests and investigate such matters (even if the defects were not fully scoped by MI5).

*(b) Home Office*

154 The long-standing risk arising from MI5's defective handling of data was brought to the attention of the Home Secretary from at least December 2016: paragraph 51 above. As at March 2017, it was highlighted to the Home Secretary that there was a very high risk that MI5 would be found not to be compliant with its statutory obligations, in particular in relation to information handling: paragraph 56 above. The timescale for MI5 allegedly fixing this problem slipped repeatedly (e.g. October 2017: paragraph 58 above; December 2017: paragraph 64 above; August 2018: paragraph 75 above).

155 Although the risk was brought to the attention of the Home Secretary in the manner described above, MI5 was not candid with the Home Secretary as to its full knowledge of the issue: see, for example, paragraphs 71 and 73 above, and the evidence of Mr Jonathan Emmett at §28 **[B/8/7] [Core/18/7]**. MI5 said it intended to brief the IPCr in June 2018 (paragraph 72 above), and the decision to brief the Home Office and IPCr was taken in December 2018 (paragraph 85 above), but then the briefings did not occur until some months later. MI5 recognised it ought to have been candid with the Home Secretary much earlier: see paragraph 105 above. But, equally troubling, having been told of the nature of the problems (if not their full scope), the Secretary of State did nothing proactive to explore the problems: there was no inquiry, no detailed requests for further information or explanation. And, most surprisingly of all, no concern expressed that such defects as described bore directly upon the warrants/authorisations the Secretary of State continued to be asked to approve in MI5's favour.

**(2) Standing**

156 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 and their staff (workers or volunteers). It is noted that the IPT has already found that the Security and Intelligence Agencies unlawfully collected, retained and processed bulk data relating to Privacy International. The Claimants have standing to complain about the breaches of domestic law pleaded as a result of their belief that they have been the subject of unlawful conduct by MI5.

157 The Respondents concede that the Claimants have standing and are victims for claims in relation to bulk material (see Amended OPEN Response, §14 **[A/6/6] [Core/5/6]**).

158 However, the Respondents have contended (see Parties' OPEN Scott Schedule **[A1/11/20-21] [Core/7/20-21]**) that the Claimants could have standing in respect of non-bulk material only if it is their case "*that they pose a threat to national security*". This is not the test in *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) ("*potentially at risk of being subjected to such measures*") and nor does it reflect the test applied by the Tribunal (as per *Human Rights Watch v Secretary of State for the Foreign and Commonwealth Office* [2016] UKIPTrib15_165-CH). The Claimants are plainly at such risk. Privacy International's data has been processed and held unlawfully. Liberty represents substantial numbers of people likely to be of intelligence interest and its data is therefore likely on any view to be caught up in targeted operations. The Respondents' position has been to neither confirm nor deny whether any individual working for one of the Claimant organisations has been potentially at risk of being subjected to targeted surveillance (Amended OPEN Response §68 **[A1/6/19] [Core/5/19]**). But that is irrelevant. The warrant need not be directed against the Claimants or their staff for it to affect their data. The detailed basis for the Claimants' position on standing, set out in Amended Grounds of Claim §107 **[A1/5/38-40] [Core/4/38-40]**, has therefore not been engaged with at all by the Respondents, including the basis for the Claimants' belief that their communications are likely to have been collected and processed. In the circumstances, there is no basis on which the Claimants' standing falls to be questioned. The Claimants have standing applying the principles in *Zakharov* and *Klass v Germany* (1979) 2 EHRR 214 (and on the basis of the assurances given by the UK as to the position to be adopted in relation to standing by the IPT in *Kennedy v UK* (2011) 52 EHRR 4).

### (3) Unlawfulness of warrants, authorisations and directions, and authorised and unauthorised data holdings

159 The core of the statutory protection for privacy over warranted data once obtained is now provided by the 'retention safeguards' sections in the IPA, namely, ss.53 (targeted and thematic interception), 129 (targeted and thematic equipment interference), 150(2), (4)–(5) (bulk interception), 171 (bulk communications data) and 191(2), (4)–(5) (bulk equipment interference). Equivalent provisions were formerly in s.15 of RIPA and, before that, s.6 of the Interception of Communications Act 1985 and, in weaker form, s.8 RIPA and ss.5 and 7 Intelligence Services Act 1994. These provisions are referred to as the "**Statutory Safeguards**".

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

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

161 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 ..."

By s.150(2), (4) and (5) (emphasis added):

> "(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, which 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))."

162 Thus, the effect of these provisions, and the equivalent provisions for bulk powers under Part 6 of the IPA (but without equivalent provision in Part 7), 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:

162.1 the number of persons to whom material is disclosed, extent of any disclosure, extent of any copying of material and number of copies made are kept to the minimum necessary;

162.2 the material must be stored in a secure manner; and

162.3 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 any of the material made: see, e.g., s.150(9)).

163 Similarly, under IPA Part 7, ss.204 and 205[196] 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*

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

*personal dataset and for protecting it from unauthorised disclosure are satisfactory*" (s.205(6)(d)). There is, however, no analogue to s.150.

164 In respect of obtaining BCD, prior to the IPA, this was obtained by a direction under s.94 TA. It required the Secretary of State to conclude that the conduct required by the direction *"is proportionate to what is sought to be achieved by that conduct"* and *"necessary"* in the interests of national security or relations with the government of a country or territory outside the United Kingdom.

*(a) Were warrants issued to or in favour of MI5 under RIPA Provisions and/or the IPA Provisions in breach of the Statutory Safeguards on their proper construction, and/or in the absence of a precedent fact, and/or based on a mistake as to an established and relevant fact or in ignorance thereof, in relation to TE and/or TE2 so as to make them invalid?*

165 In light of the foregoing, it is apparent the Secretary of State was exercising his or her discretion in issuing warrants and/or granting directions on the basis of a mistake as to an established and relevant fact: see Amended Grounds of Claim §§135-136 **[A1/5/50-51] [Core/4/50-51]**. The conditions required to establish this domestic ground of review were set out in *E v Secretary of State for the Home Department* [2004] EWCA Civ 49, [2004] QB 1044. A decision is unlawful and void where a decision is 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.

166 The fact that there was such a mistake has been conceded, at least in relation to the TE. Amended OPEN Response §67(c) **[A1/6/18] [Core/5/18]** admits that the Secretary of State granted warrants in ignorance of relevant facts, and the Respondents clarified in submissions at the November 2020 directions hearing that they accepted that this meant that the warrants were granted unlawfully (see also the Parties' OPEN Scott Schedule at **[A1/11/24] [Core/7/24]**). That concession is perhaps unsurprising in light of Fulford LJ's Generic Warrants Decision at §44 **[C3/165/8]**:

> "… 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 …"

167 At Amended OPEN Response §67(d) **[A1/6/18-19] [Core/5/18-19]**, the Respondents contend that the Tribunal should reach a different conclusion, however, in relation to TE2, on the basis that in relation to TE2 the compliance risks were not "*a relevant matter that the Secretary of State and Judicial Commissioner were required to be aware of*". That is simply not understood in circumstances where, for example, MI5 reported to IPCO that "*we have not been able to definitively confirm our original assessment that there are no complete datasets residing in the TE2 Area 1 nor that all relevant, historic BPD data has been successfully deleted*" **[C4/196/1]**. The Respondents' argument is purely formalistic and without merit – it is the existence or not of the facts that gave rise to the compliance risks or breaches that was material; such facts existed; that means that the Secretary of State could not thereafter lawfully conclude that the satisfactory arrangements were in force for securing compliance.

168 It is also an argument that has been rejected by the Canadian Federal Court (*In the matter of an application by [REDACTED] for warrants pursuant to sections 12 and 21 of the Canadian Security Intelligence Service Act, RSC 1985, C C-23 and in the matter of Islamist Terrorism* [2020] FC 616). Gleeson J held at [129]-[131] that the attempt to frame breaches of statutory safeguards as merely being matters of "risk" was wrong in principle and no excuse:

"[129] The framework characterizes all issues in terms of risk. This approach at least suggests that the risk can either be accepted or mitigated. Thus, an activity that plainly breaches the CSIS Act is characterized as a "high legal risk": one that, when viewed from an operational perspective may be balanced against the benefits of the operation and accepted where the benefits are viewed as being significant. This is exactly what occurred. However, an activity that breaches the CSIS Act is not like any other risk. It is activity that on its face is illegal and if undertaken would also be contrary to the Service's foundational commitment to collect intelligence within the bounds of the law.

[130] If the proposed Service activity is not authorized by the CSIS Act, there is no room to balance interests: the activity is illegal and cannot proceed, at least not within the bounds of the law. Characterizing unlawful activity in terms of risk does not change the fact that it is illegal.

[131] The legal risk assessment framework mischaracterized Service activity that was on its face illegal as posing a "high legal risk." In doing so, it allowed decision-makers to authorize illegal activity on the basis that it could be weighed against expected benefits. This circumstance not only resulted in the Service engaging in illegal operational activity: it may have also contributed to the failure of those involved in the warrant approval process to

> identify the information collected as a result of this activity as having been unlawfully collected. Lack of awareness of illegality has been advanced as one explanation for the breach of candour."

169 A further or alternative legal basis for impugning the warrants (other than under Part 7) is that, in circumstances where there was no adequate assessment by the Secretary of State as to whether there were satisfactory arrangements in force (under s.150 and its analogues), and there were in fact no proper arrangements in force for securing the safeguards, then the exercise of the discretion under IPA (and RIPA before it) is unlawful. For the statutory words to mean anything (i.e. that the Secretary of State must consider that "*satisfactory*" arrangements are in force, having first "*ensure[d] ... that arrangements are in force for securing*" the safeguards), then there must be some assessment of the effectiveness of the arrangements in place, and an objective and reasonable basis for a conclusion that they are (or will be) satisfactory.

170 Where a decision-maker fails to comply with provisions in legislation that are "mandatory", their decision is unlawful and (at least in general) void *ab initio*. As to whether a requirement in legislation is a "mandatory" provision, see *De Smith's Judicial Review* (8th ed.) at para 5-062:

> "In order to decide whether a presumption that a provision is "mandatory" is in fact rebutted, the whole scope and purpose of the enactment must be considered, and one must assess "the importance of the provision that has been disregarded, and the relation of that provision to the general object intended to be secured by the Act". In [a]ssessing the importance of the provision, particular regard should be given to its significance as a protection of individual rights; the relative value that is normally attached to the rights that may be adversely affected by the decision, and the importance of the procedural requirement in the overall administrative scheme established by the statute. Breach of procedural or formal rules is likely to be treated as a mere irregularity if the departure from the terms of the Act is of a trivial nature, or if no substantial prejudice has been suffered by those for whose benefit the requirements were introduced. But the requirement will be treated as "fundamental" and "of central importance" if members of the public might suffer from its breach. Another factor influencing the categorisation is whether there may be another opportunity to rectify the situation; of putting right the failure to observe the requirement."

The Statutory Safeguards clearly satisfy the tests identified in this passage as making them mandatory requirements – they are fundamental to the lawful operation of the Act and have primary significance for the protection of individual rights.

171 Similarly, where a set of facts must exist for the exercise of the jurisdiction of the decision-maker, the courts are entitled to inquire into the existence of those facts: "*The*

*statute in such a case imposes a condition as precedent to the exercise of the public authority's power and it is the duty of the court to ensure that the condition has been met.*" (*De Smith's Judicial Review* (8th ed) para 4-056).

172 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:

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

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

173 That accords with Fulford LJ's characterisation in the Generic Warrants Decision **[C3/165/4-5]**, in his summary of the legislative position at §§14-17:

> "Section 53 deals with "Safeguards relating to retention and disclosure of [intercepted] material." Subsection 1 stipulates that the Home Office has to ensure that there are arrangements in force to secure compliance with the requirements of subsections 2 and 5 (subject to subsection 9). The obligation on MI5 is to act in accordance with those arrangements. By subsection 2, the promulgation of product must be limited to the least necessary for the purpose authorised. That covers the number of people to which it is disclosed or made available and the extent to which copies are made. Subsection 4 requires that similar protections apply to each copy. Subsections 5 and 6 require destruction of the material as soon as it is no longer needed. These are mandatory requirements. …
>
> If a warrant is lawfully to be approved, the Secretary of State must be satisfied that the product will be appropriately safeguarded; otherwise the application for the warrant cannot be granted."

174 On the present facts, the Secretary of State was unaware (and did not seek to be made aware) for the material period of the defective nature of the arrangements, or that the arrangements in force would not in fact secure the relevant safeguards. That was therefore a precedent fact (ensured compliance under s.150 IPA or, previously, s.15 RIPA), i.e. a matter which had to be in place for the Secretary of State to be in a position to authorise the making of the warrant, which was absent.

175 The Respondents say that a proper construction of IPA and RIPA focuses instead on the fact that arrangements "*for*" securing the relevant matters must be in force (which they

contend were in force at all times, even if they were entirely ineffective or ignored in practice): see Amended OPEN Response §58 **[A1/6/16] [Core/5/16]**. However, the statutory requirement cannot simply be a requirement that *something* was in force, entirely divorced from its effectiveness in practice. The Respondents' argument is a formalistic parsing of the statutory words that has no role in the construction of a set of statutory safeguards intended to give meaningful protection to fundamental rights of privacy (and more), and to ensure, and which must be construed so as to ensure, compliance with ECHR Articles 8 and 10 through "*adequate and effective guarantees against abuse*" (*Zakharov* at [232]). Further, and unsurprisingly, the Respondents do not even appear to go that far on their own approach. As they summarise it in the Parties' OPEN Scott Schedule **[A1/11/23] [Core/7/23]**, *"the Respondents have accepted that when granting warrants, it was a relevant matter for the Secretary of State to understand the compliance risks concerning the TE. Such compliance risks were relevant to the question whether "satisfactory" arrangements were in force".*

176 It follows that the warrants granted in these circumstances were invalid applying ordinary public law principles.

*(b) Did MI5 (a) owe and (b) breach a duty of full and frank disclosure in applying for warrants and/or directions in all the circumstances?*

177 It is common ground (see **[A1/11/25] [Core/7/25]**) that MI5 had a duty of full and frank disclosure in relation to each request made to the Secretary of State to exercise his or her discretion to issue a relevant warrant, authorisation and/or direction. And that position was confirmed, in relation to warrant applications, by IPCr Notice 1/2018: *"It is important that the Secretary of State has all relevant matters drawn to his or her attention when considering applications. In accordance with the Codes of Practice, all reasonable efforts will be made to take account of the information which militates against the grant of the application, which includes material which weakens the case for the warrant, authorisation or notice"* (paragraph 31).[197] As held in *R (Haralambous) v Crown Court at St Albans* [2018] UKSC 1, [2018] AC 236, the duty of candour in such applications means that "*information on which he or she relies must constitute a fair and balanced presentation of the circumstances on the basis of which a warrant is sought*". Such duty

[197] IPCr Advisory Notice 1/2018: Approval of Warrants, Authorisations and Notices by Judicial Commissioners **[C2/93A/6]**.

of full and frank disclosure applied to MI5 at both stages of the "double locked" IPA procedures (i.e. full and frank disclosure to both the Secretary of State and Judicial Commissioners) and, before that, when applying to the Secretary of State under the predecessor powers.

178 As part of the duty of full and frank disclosure resting on any application for a warrant, the applicant (MI5 in this case) also has a duty of inquiry – as summarised in paragraph 34 of the IPCr Notice 1/2018, that is a duty to make "*all reasonable efforts to take account of information which may weaken the case for the warrant*".[198]

179 The Respondents deny that MI5's duty of full and frank disclosure was breached. But the suggestion that MI5 at all times complied with such a duty is untenable, and the Respondents notably do not try to explain the point. The factual summary above demonstrates that MI5 held relevant knowledge about the defects in its systems from 2010, or at the very least 2013. Despite this, something plausibly characterisable as full and frank disclosure in respect of the TE was only first achieved in February/March 2019, and the immediate result was to put MI5 in "*special measures*". There had not been full and frank disclosure before then.

180 The professed basis upon which MI5 contends that it did not breach the duty of full and frank disclosure is that (i) it lacked a proper knowledge of the factual position as it was then understood at all relevant times **[A1/11/25] [Core/7/25]**; and (ii) MI5 relies upon the fact that it provided the Home Office with its Quarterly Performance Reviews (Amended OPEN Response §4(j) **[A1/6/3] [Core/5/3]**) that first raised the issue from December 2016 onwards. However:

180.1 MI5 did not begin to provide a full and frank account of the knowledge it held about its non-compliant holding of data, whether by the Quarterly Performance Reviews or otherwise. The disclosure in these proceedings has shown that there was a far greater degree of knowledge within MI5 than it let on. As Mr Henry Hirsch states in Hirsch 1 §56 "*I now believe I was being partially … informed about the compliance issue and constraints of the [TE] – however, I was not aware of the scale of the issue at this time and it was not until after I left my role and the full*

198 IPCr Advisory Notice 1/2018: Approval of Warrants, Authorisations and Notices by Judicial Commissioners **[C2/93A/7]**.

*nature of the issue emerged that I was able to consider this link further"* **[B/6/13] [Core/16/13]**. Although Mr Hirsch attributes that "*to MI5's incomplete understanding at this stage*", in fact MI5 had a much greater understanding of the problems. MI5 did not wish to live with the consequences of disclosure (potential loss of warrantry) in circumstances where it had not begun to fix the problems.

180.2 The Respondents' position is all the more untenable once MI5's own duty of inquiry, as part of its duty of full and frank disclosure, is understood. MI5 had to ask itself whether it understood enough about the level of compliance of its own data holdings to be making a candid account of anything that may weaken the case for the warrant. Even the most basic inquiries would have revealed the likelihood of serious failings that subsequently came to light (even assuming the implications were not clear from an early stage, which is implausible). It was not necessary to know the full extent of the breaches or their ramifications. Once it became clear, as It did as early as 2010 or at least May 2013, that MI5 could not say with any degree of certainty what data it had in TE or TE2 Areas 1 and 2, and so whether it could comply with its RRD duties, its disclosure duties, and its duties in respect of LPP material, that was a matter it was obliged to disclose *even if* the matters remained under investigation. It is no answer that its knowledge at that stage was not complete. That is the approach any regulator (be it the Financial Conduct Authority, Ofcom/Ofgem/Ofwat, the General Medical Council, Information Commissioner's Office, etc.) would expect those it regulates to take to any equivalent breach of duty. Yet MI5 did not do so, and it thereby breached its duty of full and frank disclosure. Indeed, it appears MI5 knew that it was (at the lowest) very likely that it was not complying with the law but relied upon the secrecy of its operations to keep this matter to itself. (It is a matter of some note that AMBER (high) and even RED (very high) risks of illegality are not automatically reported to either the Secretary of State or the IPCr).

181 The requests for warrants, directions and authorisations were therefore obtained in circumstances where there was a breach of MI5's duty of full and frank disclosure, and that was a breach that was material (as is shown by the IPCr's response to the disclosure). Where a warrant is obtained by virtue of a breach of a duty of full and frank disclosure, the usual consequence is that the warrant should be quashed: see *R (Rawlinson & Hunter*

*Trustees & ors) v Central Criminal Court & ors* [2013] 1 WLR 1634 (Div Ct) at [171]-[177].

*(c) Were warrants issued to or in favour of MI5 under the RIPA Provisions and/or the IPA Provisions, or were directions issued under TA s.94, unlawfully due to the Secretary of State's failure to comply with his or her duty of sufficient enquiry?*

182 It is common ground that the Secretary of State owed a *Tameside* duty of sufficient enquiry **[A1/11/25] [Core/7/25]**. As Lord Diplock held in *Secretary of State for Education and Science v Tameside MBC* [1977] AC 1014 at 1065B: "*The question for the court is, did the Secretary of State ask himself the right question and take reasonable steps to acquaint himself with the relevant information to enable him to answer it correctly?*" The obligation upon the decision-maker is only to take such steps to inform himself as are reasonable; a decision will be unlawful if no reasonable Secretary of State possessed of that material could suppose that the enquiries were sufficient: *R (Plantagenet Alliance Ltd) v Secretary of State for Justice* [2014] EWHC 1662 (QB) at [100].

183 As the factual summary above makes clear, the Secretary of State had been made aware of a serious compliance risk within MI5 by at least 2016. The Claimants cite six examples of the Secretary of State being addressed on the matter at Amended Grounds of Claim §147A **[A1/5/54-55] [Core/4/54-55]**. These documents have been specifically responded to in Hirsch 2 §§46-52 **[B/7/12-14] [Core/17/12-14]**.

183.1 On 15 December 2016, a Note from the Head of Oversight, NSU to the Home Secretary on the MI5 Quarterly Performance Report: Quarter 2 of 2016/17, noted that MI5's corporate risk register "*flags that it is currently carrying a risk that MI5 is not compliant with the relevant legislation with regards to information handling*", which is a "*red risk*" and "*relatively long standing*" (§8).[199] Mr Hirsch explains that, following a briefing in February 2017, he was satisfied that MI5 "*had the matter in hand*" (Hirsch 2 §47 **[B/7/12] [Core/17/12]**). It appears that no sufficient enquiries were made actually to understand the nature of the compliance issue or its implications; a mere belief that MI5 was resolving the matter was insufficient and the Secretary of State should have kept the topic under review,

[199] MI5 Quarterly Performance Report: Q2 of 2016-2017 (HO Core Doc 1) **[C2/62/2]**.

amongst other things by asking follow up questions and demanding information, until the matter was in fact resolved (including deciding whether warrantry/authorisations could continue to be granted). The fact that the matter was "*in hand*" is no answer if the breach, or facts underlying a possible breach, were still extant.

183.2 By email on 25 January 2017, further to a bilateral meeting between the Home Secretary and Sir Andrew Parker (MI5 Director General) on 23 January 2017, it was recorded that "*the Home Secretary noted her concern about [REDACTED] errors that had been identified in MI5's management [REDACTED]. AP apologised for the errors and confirmed that corrective measures had been put in place. He had also established a [REDACTED], headed by a Director, to strengthen MI5's processes in this area and prepare for the implementation of the Investigatory Powers Act*".[200] Mr Hirsch states that these issues "*were unrelated to the general compliance risk at consideration here*" (i.e. what was subsequently reported to the IPCr) (Hirsch 1 §30 **[B/6/7] [Core/16/7]**). It is not accepted that these issues are irrelevant to the compliance risk within MI5's data holdings; they should, in any event, have been contributing to a picture that there were unresolved compliance issues within MI5 affecting warrantry/authorisations.

183.3 On 24 March 2017, a Note from the Deputy Head NSU, to the Home Secretary noted that "*MI5's corporate risk register continues to flag a red ('very high') risk that MI5 is found to be not compliant with its statutory obligations, particularly relating to information handling, leading to substantial legal/reputational damage*" (§8).[201] The risk was noted to be "*relatively long standing*". The Home Secretary was therefore aware of the seriousness of the risk and its long-standing nature. But again, she continued to ask no questions; nor query how this bore upon warrants/authorisations that she must have continued to grant under IPA predecessor legislation.

183.4 On 27 September 2017, the Home Office minutes of the Quarterly Performance Report meeting noted that the Management Board "*had also flagged the compliance risk as a continued concern and would discuss this in more detail again*

200 Email RE: Andrew Parker bilateral – readout (HH1 Exhibit HH4) **[C2/63/1]**.
201 MI5 Quarterly Performance Report: Q3 of 2016-2017 (HO Core Doc 2) **[C2/69/2]**.

*in future*".[202] There was recognised to be a "*delay*" in "*achieving an amber rating in compliance*".[203] The response from Mr Hirsch was that he met colleagues and considered that MI5 "*is seeking to address it comprehensively*" (Hirsch 2 §49 **[B/7/13] [Core/17/13]**). However, that does not indicate whether the Secretary of State knew the extent of the compliance issue, or what steps MI5 was taking to address it (and whether those steps would be sufficient to address it). It appears that the enquiries did not go to either of these (obviously material) points or indeed materially further than the verbal assurances previously received.

183.5 A Home Office document dated 18 October 2017 records that MI5's corporate risk register contains "*two red (very high) risks. The first is compliance with statutory obligations. This is a longstanding risk that MI5 is placing significant effort into managing. Nonetheless the timeframe by which MI5 believes it will be able to reduce the risk from red to orange (high) has slipped from [towards the end of 2017] to [mid 2018]*" (§12).[204] Mr Hirsch explains (Hirsch 2 §51 **[B/7/13] [Core/17/13]**) that his team passed on to the Home Secretary "*MI5's reasonable explanation to our inquiries to reassure the Home Secretary that we had an understanding of the compliance risk at that time*", namely that MI5 had underestimated "*the scale of challenge*". However, that does not demonstrate that the Secretary of State had an understanding of the compliance risk at the time or of its obvious implications for warrantry/authorisations (even pre-IPA); quite the contrary – it shows that the Secretary of State was relying on a description of the issue that had not reflected the scale of the problem.

183.6 The Home Office MI5 Quarterly Review (Q2 2017/18) on 20 November 2017 discussed the compliance risk: "*MI5 explained that the red rating reflects the long-term challenge of how to ensure current systems are in a compliant state, and ensuring that where systems are not compliant, there is resource to acquire new systems which are compliant. The Investigatory Powers Act has helped get legacy systems more up to scratch, but the risk is still high because the process has yet to be finalised*".[205] A note to the Home Secretary dated 20 December 2017 noted

---

202 Minutes (HH1 Exhibit HH5) **[C2/81/2]**.
203 Minutes (HH1 Exhibit HH5) **[C2/81/5]**.
204 MI5 Core Doc 31 **[C2/82/3]**.
205 Minutes of MI5 Quarterly Review (Q2 2017/18) (MI5 Core Doc 36) **[C2/87/4-5]**.

*"There is one red … risk in MI5's Q2 report, which concerns compliance with statutory obligations. The red rating reflects the long-term challenge of how to ensure that MI5 … compliance with its legal and other obligations. As you know, this was also red in Q1 and is a longstanding risk that MI5 is placing significant effort into managing*" (§15).[206] Mr Hirsch explains (Hirsch 2 §52 **[B/7/13] [Core/17/13]**) that "*since the February 2017 meeting we saw an intrinsic link between the compliance risk and the commencement of the IPA and therefore as the timeline for the project was slipping it was unsurprising that the same was true of the former"*. This explanation confirms that the (obvious) link with legality of warrantry had finally been drawn; it should have led the Secretary of State to consider whether or not there was no proper basis to justify the continued granting of warrants; but it was hardly a justification as to why it was acceptable to carry on without further inquiries.

184 In short, the material shows twin failings. The Secretary of State was not being provided with full and proper explanations by MI5. However, the Secretary of State was him/herself put on sufficient notice of the compliance problems by (at least) reference to the matters above. The Secretary of State did not react appropriately by exercising independent scrutiny and inquiry to discover the nature and implications of the non-compliances identified. Instead, the Secretary of State remained reliant on vague assurances being fed back from MI5 (even when they were not delivered), and continued to issue warrants and/or directions and/or otherwise exercise statutory discretion on the basis of the assertion that the compliance arrangements within MI5 were or would be satisfactory. She did so despite the fact that she was being told in terms that safeguards in the legislation were not being complied with.

185 This is the acme of the sort of irrationality that *Tameside* captures. When put on notice of a "red"/ "very high" risk of non-compliance, no reasonable Secretary of State posed with the question of whether there were "satisfactory" arrangements in force and to ensure that "arrangements are in force for securing" the safeguards could suppose that the enquiries made were sufficient to be able to exercise that discretion on an informed basis. That is all the more apparent in circumstances of the heightened importance of the

---

206 Note to Home Secretary on MI5 Quarterly Review of Performance: Quarter 2 of 2017-18 (HH1 Exhibit HH7) **[C2/88/4]**.

*Tameside* duty of enquiry in this context, given the highly intrusive nature of the powers and the obvious human rights implications of the Secretary of State's decisions. The Secretary of State's relevant exercises of discretion, from the time that the Secretary of State was first put on notice of the serious compliance risk, were therefore unlawful.

186 The Respondents contend that there is no breach of the *Tameside* duty in circumstances where the "*relationship between the Home Office and MI5 is necessarily and appropriately based upon trust. The Home Office does not and cannot be expected to review every element of MI5's business, and relies upon MI5 to identify matters relating to compliance of which the Secretary of State needs to be aware*" (Amended OPEN Response §4(j)(i) **[A1/6/3] [Core/5/3]**; and see Hirsch 2 §§7-8 **[B/7/2-3] [Core/17/2-3]**). This is both to tilt at a straw man and to neuter *Tameside*.

186.1 As for the straw man, there is no suggestion that the Secretary of State needs to review every element of MI5's business. It is, however, necessary, in circumstances where the statute provides the Secretary of State with an express independent role (and one which is relied on by HM Government as a major safeguard) to exercise judgement and to exercise that role diligently and with a proper understanding of the matters that the Secretary of State is required to ensure, and to react to evidence that a problem has arisen, such as a report saying, in effect, 'there is a red (very high) risk that we are not complying with our statutory obligations relating to information handling, leading to substantial legal/reputational damage'. Such reports are surely exceptional.

186.2 As for the fact that the relationship is one of trust, so much is true about so much of the fabric of Government, for instance the relationship between a Minister and civil servants, central government and executive agencies etc. But it cannot displace the requirements of the law and for rational action, particularly when "red flags" suggest such trust is misplaced (for whatever reason). That is particularly so when the role of the Secretary of State in approving warrants is relied upon as a "safeguard" (both pre- and post-IPA). But a "safeguard" when the party whose conduct is under scrutiny/challenge is taken on trust is no safeguard at all.

187 It is further said to excuse the Secretary of State that MI5 presented to it "*risks to be mitigated, rather than issues to be fixed*" (Amended OPEN Response §4(j)(iii) **[A1/6/4] [Core/5/4]**). This is a desperate but meritless distinction for the reasons given above.

*(d) ECHR claim*

188 By obtaining warrants/authorisations in the circumstances set out above, and thereafter by obtaining or retaining any data obtained under them, MI5 has acted in a manner that was "not in accordance with the law" and not "provided by law" under Article 6 (relevant to legal privilege) and Article 8 ECHR. In obtaining the warrants, it has failed to comply with domestic law because the statutory safeguards were not met.

189 Further, in relation to directions for the acquisition of BCD pursuant to s.94 TA granted to MI5, even after the dates of the s.94 directions quashed by the IPT, there was no Convention-compliant basis for the direction to be issued and/or for data to be retained. Each such s.94 direction and/or retaining was therefore unlawful.

190 The intention of the Statutory Safeguards, and of compliance with the domestic law in relation to them, was an attempt to achieve a position that was compliant with Article 8 ECHR. The breaches of the Statutory Safeguards themselves constitute breaches of the Claimants' ECHR rights.

*(e) EU law*

191 EU law is engaged because, and to the extent, of the compulsory acquisition of bulk communications data from public communications networks and the handling of the product so acquired. This further ground of unlawfulness therefore arises in circumstances where BCD, or the product of BCD, or indeed any form of communications data (bulk or otherwise) compelled from a commercial provider, was held in the TE or TE2; that is addressed at paragraph 146 above.

192 As per C-623/17 *Privacy International*, such acquisition of data is within the scope of EU law. Under EU law, that action is subject to the following requirements:

192.1 Article 15(1) of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (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*".

192.2 Articles 7, 8 and 11 Charter of Fundamental Rights ("**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. 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) CFR 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*".

193 The proceedings were commenced before 31 December 2020 and therefore s.5(4) of the European Union (Withdrawal) Act 2018 (the "**2018 Act**") (the "Charter of Fundamental Rights is not part of domestic law on or after IP completion day") does not apply to these proceedings by virtue of Part 4, para 39(3) of Sch 8 to the 2018 Act. 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.

194 The Respondents' conduct described above, in granting and obtaining warrants and directions, and retaining data purportedly pursuant to them, was also in breach of EU law:

194.1 The actions did not occur in accordance with domestic law, namely the statutory powers that provide for them, with the 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 rights under Article 8 CFR, "*laid down by law*"), nor is their basis "*legislative measures*" under Article 15 of the ePrivacy Directive.

194.2 Further or alternatively, those actions occurred pursuant to a system that did not meet the requirements of Article 8 ECHR that an interference be "*in accordance with the law*" and thus *a fortiori* one that did 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.

**(4) Has either of the Claimants' data been unlawfully held and/or used?**

195 The Claimants have set out their position in the Parties' OPEN Scott Schedule at **[A1/11/26] [Core/7/26]**. If and to the extent that (i) any warrant or authorisation is unlawful (it being conceded that at least some warrants were unlawfully issued) and data has been obtained, retained or used purportedly pursuant to it or (ii) there has been a breach of any of the Statutory Safeguards or arrangements made under them in relation to any data obtained or held by MI5, 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. The same analysis applies insofar as there was non-compliance with any requirement the warrant/authorisation itself imposes. The Claimants request the Respondents address (at least in CLOSED) whether the Claimants' own data was unlawfully held. The Tribunal made a preservation order **[A2/31]** (as varied upon MI5's application **[A2/32]**) in order to facilitate such a report being provided.

**(5) Systemic challenge to the ECHR-compatibility of the legal regimes**

196 This episode demonstrates that the safeguards in the legislative system – as it existed under RIPA (and s.94 TA / ss.5, 7 Intelligence Services Act 1994), and also under IPA – did not result in safeguards that were effective in practice. This was not a one-off error, or a mere oversight, but a protracted systemic and systematic failure on three levels:

196.1 First, in the handling of data by MI5, and the processes designed to ensure such conduct was lawful, failures were not only allowed to persist for years, but indeed were actively facilitated to permit more and more personal data to be ingested into deficient systems;

196.2 Secondly, in the operation of the prescribed internal and external oversight systems which for at least seven years were unable to uncover root and branch failures. The safeguards that were in place proved inadequate in practice to prevent and/or rectify these breaches. The system was overwhelmingly reliant on MI5's own assessment of its systems, and the importance (or lack of it) that MI5 decided to accord to the

legality of its data handling. Neither internal lawyers/processes nor the Secretary of State provided any meaningful independent oversight over the process, in circumstances where the Secretary of State was content to trust the limited information being shared with him or her by MI5, and MI5 lawyers seem to have been incapable of objective advice or "challenge", instead wrongly viewing their role as being to "*defend MI5's position*" (paragraph 127 above). As a result, MI5 was able to conceal systemic deficiencies from the Commissioners and (thereafter) the IPCr and the IPT (revealing the limitations of the system of oversight); and

196.3 Thirdly, in the outputs required of MI5, whether in terms of candour in warrantry (to the Secretary of State and the Judicial Commissioners), candour in legal proceedings (in this Tribunal and beyond) and in the disclosure MI5 is periodically required to give.

197 The question for the Tribunal is whether together this amounts to the sorts of systemic failure in the statutory scheme and oversight process that leads to global Article 8 and 10 incompatibility, or whether this was nothing more than an 'error' which is apt to be properly resolved by the very mechanisms established by the scheme and oversight process. It is noted that this aspect of the claim is one where the existence of other systemic flaws in the system, which have not been brought to light yet even in these proceedings, is likely to be highly relevant; to the extent that the Tribunal is minded (as per paragraphs 149-150 above) to direct that there be disclosure of such other systemic failings, then it respectfully should stay its determination of this aspect of the claim pending such disclosure. Out of an abundance of caution, this aspect of the claim is addressed on the material available to the Claimants as of now.

198 As to the relevant legal framework:

198.1 In *R (P) v Secretary of State for Justice* [2019] UKSC 3, [2019] 2 WLR 509, Lord Sumption held at [24]:

> "the Strasbourg court has treated the need for safeguards as part of the requirement of foreseeability. It has applied it as part of the principle of legality in cases where a discretionary power would otherwise be unconstrained and lack certainty of application. This may be illustrated by reference to the subsequent decisions in *Liberty v United Kingdom* (2009) 48 EHRR 1 and *Gillan v United Kingdom* (2010) 50 EHRR

45. Liberty concerned the bulk interception of telephone communications passing through submarine cables terminating in the United Kingdom. There was statutory authority for the interception, but as the court pointed out at para 69, the legal framework did not have the quality of law. This was because "the court does not consider that the domestic law at the relevant time indicated with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the state to intercept and examine external communications. In particular, it did not, as required by the court's case law, set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material."

198.2 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]. 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].

198.3 The ECtHR Grand Chamber's judgment in *BBW* considered*, inter alia,* the compliance with the ECHR of the legal framework for bulk interception in RIPA – and, in particular, the power in s.8(4) RIPA for the Secretary of State to issue warrants for the interception of external communications. The Grand Chamber held at [349], [350], and [356] (emphasis added):

"349. In its case-law on targeted interception, the Court has had regard to the arrangements for supervising and reviewing the interception regime (see Roman Zakharov, cited above, §§ 233-234). In the context of bulk interception the importance of supervision and review will be amplified, because of the inherent risk of abuse and because the legitimate need for secrecy will inevitably mean that, for reasons of national security, States will often not be at liberty to disclose information concerning the operation of the impugned regime.

350. Therefore, in order to minimise the risk of the bulk interception power being abused, the Court considers that the process must be subject to "end-to-end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent ex post facto review. In the Court's view, these

are fundamental safeguards which will be the cornerstone of any Article 8 compliant bulk interception regime (see also the report of the Venice Commission, at paragraph 197 above, which similarly found that two of the most significant safeguards in a bulk interception regime were the authorisation and oversight of the process).

356. Each stage of the bulk interception process – including the initial authorisation and any subsequent renewals, the selection of bearers, the choice and application of selectors and query terms, and the use, storage, onward transmission and deletion of the intercept material – should also be subject to supervision by an independent authority and that supervision should be sufficiently robust to keep the "interference" to what is "necessary in a democratic society" (see Roman Zakharov, cited above, § 232; see also Klass and Other, cited above, §§ 49, 50 and 59; Weber and Saravia, cited above, § 106 and Kennedy, cited above, §§ 153 and 154). In particular, the supervising body should be in a position to assess the necessity and proportionality of the action being taken, having due regard to the corresponding level of intrusion into the Convention rights of the persons likely to be affected. In order to facilitate this supervision, detailed records should be kept by the intelligence services at each stage of the process."

198.4 As noted in Amended Grounds of Claim §113 **[A1/5/44] [Core/4/44]**, of course not every breach or error will be such as to show this requirement is not met. Some errors, and their prompt identification and correction, might show a system of regulation oversight that is working properly. If the IPCr identifies swiftly through audit a problem, investigates it, and resolves it, this may be said to show that the system of oversight works – i.e. demonstrating that the system of guarantees is effective. In contrast, if a systemic failing can persist for years unreported to and unidentified by the oversight mechanisms, then the opposite conclusion is proper.

199 The present systemic failings demonstrate a legal regime that is not in accordance with the law or prescribed by law because it relies upon safeguards that are not effective in practice.

200 This point was explored with the Secretary of State upon the longstanding failure coming to light. As detailed in the submission to the Home Secretary and the Security Minister (9 April 2019) §25:[207]

"Should IPCO or in slower time the courts conclude the MI5 safeguards are inadequate there are a number of options which can be progressed depending on the exact nature of the concern.

a. Support MI5 to add further safeguards as necessary in order to address the concerns.

[207] Note to SSHD and Security Minister TE: Investigatory Powers Compliance-handling update (HO Core Doc 18) **[C3/167/5-6]**.

b. If having put in place all possible safeguards then further, … mitigations could include MI5 stopping certain warrantry or … [using] data differently, potentially through the imposition of conditions on warrants.

c. If the operational changes would not address the concerns or the consequences of those changes are … then changes to guidance or legislation are potential other options …".

201 The various safeguards under RIPA and IPA that were supposed to exist and to operate failed in practice. The IPCr and Judicial Commissioners did not know about the problems at all, and they were not identified through their audit activities. The regulators have proven to be far too reliant on voluntary disclosure by MI5, which was not forthcoming. The Secretary of State was not addressed on the defects in a sufficiently clear way to exercise any robust independent control over the fact that data would be held non-compliantly and now asserts she can and did work simply on trust (which provides no assurance of protection in the future). No disclosure was made by an employee or officer of MI5 to IPCO pursuant to the whistle-blowing provision in IPA s.235(6). MI5 committed a serious breach of the Code of Practice and s.231(9) IPA by failing to report the matter to the IPCr promptly (within 10 working days, according to the current Interception of Communications Code of Practice). There was, and was allowed to persist, an ingrained institutional culture of accepting and permitting unlawful conduct in MI5 as to the handling of data.

202 The Respondents rely (Amended OPEN Response §§87-89**[A1/6/25] [Core/5/25]**) on the assertion that the legislative regimes are *capable* of being operated in a manner which is compatible with ECHR rights, and contend that the matter has been conclusively resolved in the judgment of the Divisional Court in *R (National Council for Civil Liberties) v Secretary of State for the Home Department* [2019] EWHC 2057 (Admin); [2020] 1 WLR 243. That is not right.

202.1 The Divisional Court summarised the evidence relied upon by Liberty, and acknowledged the seriousness and concerning nature of MI5's systemic failings (at [361]-[372]), but 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]). However, the Divisional Court proceeded without any CLOSED material and in the absence of the vast bulk of the OPEN material now before the IPT. At [387], the Divisional Court adverted to

possible proceedings before the IPT, in which the lawfulness of instances of conduct relating to the failings could be considered afresh; the Divisional Court emphasised that "*[n]othing we say in this judgment should be taken to anticipate in any way what might be said in any such future litigation*". The decision of the Divisional Court does not therefore limit the Tribunal's decision on the evidence now before it.

202.2 In any event, permission to appeal to the Court of Appeal has been sought on this point.

203 In light of the foregoing, the domestic legislative regime has proven insufficient. The safeguards do not do enough and have not worked in practice. Something more is required – it cannot be allowed that such widespread systemic illegality can persist unnoticed and unabated, and (subject to the determination of relief) potentially without consequence. This Tribunal is asked to declare as much. It is, of course, not for this Tribunal to identify the solution – that is for Parliament. But it is for this Tribunal to declare when it has found that the supposed world-class interlocking scheme of safeguards has failed to be practical and effective in a systemic, long-standing and material way.

## F RELIEF

204 The relief sought by the Claimants, in addition to the declaration of ineffective safeguards for the purposes of ECHR-compliance set out above, is set out at the Amended Grounds of Claim §156 **[A1/5/59-60] [Core/4/59-60]**. The Claimants seek (i) quashing of warrants, authorisations and/or directions that were unlawfully issued; (ii) declaratory relief as to the unlawful obtaining, use, retention and failure to destroy material; (iii) the destruction of data that remains unlawfully retained; and (iv) subject to the determination of the issue at paragraph 195 above, further or other relief including damages.

205 The Respondents' position is that *"Subject to the issue of the application of s.31(2A) Senior Courts Act 1981, no relief other than limited declaratory relief should be granted"* **[A1/11/31] [Core/7/31]**. However, (i) s.31(2A) Senior Courts Act 1981 ("**SCA81**") does not apply in this Tribunal; and (ii) relief ought not to be limited as the Respondents contend.

**(1) Section 31(2A) Senior Courts Act 1981**

206 The Respondents seek to rely on s.31(2A) SCA81 to contend that relief ought to be refused, which provides that *"The High Court (a) must refuse to grant relief on an application for judicial review … if it appears to the court to be highly likely that the outcome for the applicant would not have been substantially different if the conduct complained of had not occurred*".

207 Such submission is wrong in principle and fanciful on the facts.

208 As for the first point, the critical fact is that s.31(2A) SCA81 applies only to the High Court of England and Wales. It does not apply to this Tribunal. RIPA s.67(2) provides that in determining *legality* the Tribunal *"shall apply the same principles for making their determination in those proceedings as would be applied by a court on an application for judicial review"* – that is not apt to include s.31(2A) SCA81, which regulates the question of *relief* in the High Court of England and Wales. Relief in the Tribunal is regulated by s.67(7) RIPA which contains no equivalent provision.

209 The conclusion that s.31(2A) does not apply to the powers of relief of a statutory tribunal required to apply judicial review principles has already been reached in other such statutory tribunals.

209.1 In the OPEN judgment in *Arumugam & ors* (PC/04/2019, 21 October 2020) in the Proscribed Organisations Appeal Commission ("**POAC**") (Elisabeth Laing J (as she then was), Richard Whittam QC, Philip Nelson CMG), the Commission held at [100] that, considering the relevant statutory provision for relief in the Commission pursuant to s.5(4) of the Terrorism Act 2000, s.31(2A) SCA81 "*does not apply to this Commission*".

209.2 POAC relied upon the decision of SIAC in *LA & ors v SSHD* [2018] UKSIAC 1 SN 63 2015, in which SIAC held that, as a matter of statutory construction, s.31(2A) does not apply "*substantially for the (obiter) reasons given by the Commission (chaired by Singh J (as he then was)) in* MWH v Secretary of State for the Home Department *(SI NO/57/2015)*" (at [108]).

209.3 In *MWH* (supra), it was held *obiter* at [60]-[64]:

> "We do not accept that section 31(2A) applies to this Commission. On its face it applies only to the High Court. If Parliament had wished to apply it, or something like it, to the Commission it could have done so expressly. … In our view, the reference in section 2D(3) of the 1997 Act to principles of judicial review is a reference to the substantive law and not to the principles which apply when considering whether to grant a remedy.
>
> Further, we take the view that a strict approach to the construction of section 31(2A) is appropriate, since it is an unusual provision in that it tends to restrict what would otherwise be a discretion vested in an independent court or tribunal …".

209.4 Recently, in *Meta Platforms Inc v CMA* [2022] CAT 26 (14 June 2022) (Marcus Smith J, Professor John Cubbin and Simon Jones), the Competition Appeal Tribunal considered the same point at [167]-[171]. In that context, s.120(4) of the Enterprise Act 2022 provides that, in determining applications such as the case before it, "*the Competition Appeal Tribunal shall apply the same principles as would be applied by a court on an application for judicial review"*. The Competition Appeal Tribunal concluded that s.31(2A) does not apply; it noted that the legislative scheme drew a distinction between principles applied on an application for judicial review and remedies where a claim for judicial review has succeeded (at [170(3)(i)]), and also remarked that *"the Tribunal is a Tribunal of the United Kingdom … and it would be odd (to say no more than that) if remedies were to differ according to whether proceedings are treated as being in one jurisdiction rather than another. The Senior Courts Act 1981 has no application in Scotland, and we regard it as undesirable for rule 18 to become a forensic battleground between applicant and respondent because judicial review remedies are different in one jurisdiction rather than another"*. The same reasoning applies to the present case: RIPA deals separately with principles and remedies, and the IPT is UK-wide in its jurisdiction and constitution.

210 In the alternative, even if s.31(2A) were to apply (which is denied), it would have no application to the present case in any event:

210.1 In order to conclude for the purposes of s.31(2A) that the outcome of any warrant application would "*highly likely*" have been the same, the Tribunal must "*undertake its own objective assessment of the decision-making process, and what its result would have been*" absent the illegality (*R (Goring-on-Thames Parish*

*Council) v South Oxfordshire District Council (Practice Note)* [2018] EWCA Civ 860 at [55]). It is inconceivable that the Tribunal could reach such a conclusion in respect of any, never mind all, of the decisions to grant warrants over the relevant period in the face of such stark illegality amounting to non-compliance with mandatory statutory safeguards. As Fulford LJ explained at §17 of the Generic Warrants Decision **[C3/165/5]**: *"If a warrant is lawfully to be approved, the Secretary of State must be satisfied that the product will be appropriately safeguarded; otherwise the application for the warrant cannot be granted"*; and at §49 *"IPCO will need to be reassured on a continuing basis that new warranted material is being handled lawfully. In the absence of this reassurance, it is likely that future warrant applications for data held in [TE] will not be approved"* **[C3/165/9]**.

210.2 Indeed, such a position would prove the systemic breach of the ECHR – for it would demonstrate that the statutory safeguards were in practice entirely illusory, and their actual or potential breach could be ignored by the decision makers due to the national security context.

210.3 The Respondents do not even appear to put their case so high. At Amended OPEN Response §104(c) **[A1/6/28] [Core/5/28]**, they contend that, had the Judicial Commissioners known about the inability to comply with statutory handling safeguards, any such warrants would instead *"have been issued and/or approved, with further conditions attached as to the manner in which information collected under such warrants should be handled"*. But that is to argue not in defence of the acts/measures under scrutiny but for the potential existence of different warrants, and to confuse the issue of legality (e.g. of a decision as to which there may have been a more protracted consultation but with the same end result) with the "*Lumba counterfactual*"[208] that might be relevant in a damages claim. Even if that were the approach that would have been adopted (which is not admitted, and is on its face inconsistent with the Generic Warrants Decision), such conditions would have been important boundaries of the legality of the warrant, and those conditions

---

[208] Cf *R (Lumba) v Secretary of State for the Home Department* [2011] UKSC 12, [2012] 1 AC 245: unlawful policy applied when exercising power of detention, but Claimants entitled to nominal damages only where would have been detained if the published policy had been applied.

would then no doubt have been either breached by the then-prevailing situation, or would have avoided the systematic and persistent unlawful retention of data.

211 In any event, if s.31(2A) were to apply (which is denied), and the Tribunal were able to determine it was highly likely that the outcome would have been the same (which is denied), then it would be appropriate to disregard the requirement in s.31(2A) for reasons of exceptional public interest. These proceedings concern the widespread, and partially admitted, infringement of rights over an extended period.

**(2) Appropriate relief**

212 As set out above, a conclusion that no relief is warranted would be to demonstrate a lack of any effective *ex post* oversight role in relation to all warrants. The illegality by MI5 in relation to bulk and other warrants would be ignored simply (in effect) because it had occurred in the past and in the national security context. The ECtHR (in *Kennedy* and *BBW* at [413]-[415]) has relied upon the effectiveness of the Tribunal as a safeguard, which would be severely undermined if the Tribunal in practice were unable to, or did not, provide any *ex post* remedy for unlawful activity of this magnitude, including in respect of bulk warrants.

213 First, there should be declaratory relief as to the extent of the unlawfulness (including that requested at paragraph 203 above).

214 Second, there should be a quashing of all warrants, authorisations and/or directions that were unlawfully issued.

215 Third, there should be an order for destruction of data that has been unlawfully retained. The Respondents have not explained in OPEN why they object to such an order, which is the normal consequence of a finding that data has been unlawfully retained – the matters have been almost entirely redacted from the Claimants (see e.g. MI5 A2 §§186-216 **[B/2/33-35] [Core/9/33-35]**). To the extent that the Respondents' submissions are simply that this is the national security context, such unlawfully-retained information is useful and/or otherwise difficult to disentangle, that is no good answer. If it were a good answer, then again the Tribunal can offer no effective remedy and the safeguards are in reality illusory.

216 Fourth, subject to the determination of the issue at paragraph 195 above, further or other relief including damages. Such a matter could be reserved to be dealt with at a remedies hearing following judgment.

## G CONCLUSION

217 Over a period of multiple years, MI5's approach to its handling of data was gravely deficient. The statutory safeguards were ignored. The regime for protecting Article 8 (and other) rights became illusory in practice – and yet the matter was not identified, reported, or even properly understood. This Tribunal was seriously misled. It has taken protracted and persistent litigation to extract something approximating to the full position from the Respondents in a situation where very real question marks remain about the accuracy and candour of the evidence of their witnesses, a matter for further submission after cross-examination in CLOSED and gisting. The Tribunal is asked to grant relief in accordance with the submissions above.

**TOM DE LA MARE QC**
**BEN JAFFEY QC**
**DANIEL CASHMAN**
**DAVID HEATON**
**GAYATRI SARATHY**
**4 July 2022**