IPT/20/01/CH

Neutral Citation Number: [2023] UKIPTrib 1

IN THE INVESTIGATORY POWERS TRIBUNAL

30TH JANUARY 2023

Before:

LORD JUSTICE EDIS
MRS JUSTICE LIEVEN
MR CHARLES FLINT KC

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

TOM DE LA MARE KC, BEN JAFFEY KC, DANIEL CASHMAN, DAVID HEATON and GAYATRI SARATHY (instructed by Megan Goulding, Solicitor, Liberty and Bhatt Murphy) for the Claimants

SIR JAMES EADIE KC, JULIAN MILFORD KC, RICHARD O'BRIEN, ANDREW BYASS, NATASHA BARNES and JOHN BETHELL (instructed by Government Legal Department) appeared on behalf of the Respondents.

MR J. GLASSON KC and MISS S. HANNETT KC appeared as Counsel to the Tribunal

Hearing Dates 25-29 July 2022

OPEN JUDGMENT

1. This is the judgment of the Tribunal to which all members have contributed.

2. This case concerns the failure by the Security Service ("MI5") over a considerable period of time to comply with the statutory safeguards required by the Regulation of Investigatory Powers Act 2000 ("RIPA") and the Investigatory Powers Act 2016 ("IPA") concerning the acquisition and holding of personal data. The relevant safeguards were the retention, review and disposal ("RRD") of personal data within MI5's technology environments. The relevant parts of those technology environments are described in this judgment, for security reasons, as "TE" and "TE2 Areas 1 and 2". Relevant datasets referred to fall into two categories, bulk personal datasets ("BPD"), and bulk communications data ("BCD").

3. The Claimants are non-governmental organisations concerned with the protection of privacy rights. They, both individually and together, have brought a number of challenges to the handling of data by MI5, both in the Investigatory Powers Tribunal ("IPT" or "the Tribunal"). In *R (Liberty) v Secretary of State for the Home Department* [2020] *"Liberty JR"* 1 WLR 243 the Divisional Court considered a challenge *inter alia* to the scheme under the IPA for the handling of BPD and BCD.

4. The Claimants allege that there has been systemic and systematic non-compliance with the relevant statutory safeguards and related non-statutory arrangements, over a prolonged period, despite considerable knowledge within MI5 of the compliance issues. The relevant time period straddles the statutory regimes under RIPA from 2010 and IPA from 2018.

5. The Respondents have accepted that MI5 was aware, as the contemporaneous documentation makes clear, of a very high risk that it was in breach of its statutory obligations from May 2016 onwards, and aware of the possibility from late 2015 of compliance failures in the TE in relation to RRD. The Respondents also accept that the state of MI5's knowledge of its failure to comply with the safeguards was such that there was from 2016 a requirement to notify the Investigatory Powers Commissioner ("IPC") of these issues. The IPC was not given any notice of the serious and extensive compliance problems in the TE until 21 February 2019.

The Issues

6. The issues that remain outstanding before the IPT concern disputes both as to the facts and the law.

7. MI5 has admitted that between 2016 and 2019 it failed to comply with the RRD requirements in respect of Authorised Data and it ought to have reported that failure to the IPC in 2016. The remaining factual issues between the parties are:

   a. Whether MI5's failure in respect of RRD commenced before 2016;
   b. Whether the failures extended beyond RRD and included the requirements of RIPA and IPA as to safeguards in respect of access controls, data copying, protection of Legal Professional Privilege ("LPP") and other requirements;
   c. The scope of MI5 reporting to the Home Office between 2013 and 2016 and whether the Home Office was put on notice of the non-compliance, which should have triggered proper enquiries.

8. The Claimants submit that the proper scope of the claim is not limited to the issues of RRD but covers all systemic failings in the handling of data. Further, that it is not limited to TE and Areas 1 and 2 of TE2 but extends to other areas where similar issues have occurred. The Claimants seek a direction that there should be disclosure of "similar fact" evidence which would enable them to seek a further hearing or a determination based on written submissions.

9. Those issues are relevant to the application to be made by the Claimants to re-open decisions made by the Tribunal in *Privacy International v Secretary of State for Commonwealth Affairs and others* ("the BPD/BCD Claim"). That case was commenced in June 2015 and the first judgment was handed down on 17 October 2016. The application to re-open the BPD/BCD Claim has been stayed pending the determinations in this hearing. The Claimants seek a determination that MI5 was in breach of its duty of candour in the conduct of the BPD/BCD Claim in failing to notify the Tribunal that MI5's handling arrangements did not comply with the law.

10. The legal issues which remain in dispute are:

    a. Whether the warrants and authorisations were issued unlawfully by the Secretary of State ("SoS")? This is put on three alternatives bases: mistake; failure to assess the material properly; and failure to undertake proper investigation, pursuant to *Tameside v Secretary of State for Education* [1977] AC 1014;
    b. Whether MI5 breached its duty of full and frank disclosure when applying to the SoS for warrants and directions?
    c. Whether in obtaining warrants / authorisations and retaining data, MI5 has breached Articles 6 and 8 of the European Convention on Human Rights ("ECHR")?
    d. Whether there is a systemic failure in the statutory scheme and oversight process under both RIPA and IPA, leading to a systemic breach of Articles 8 and 10?
    e. Whether there is a breach of retained EU law?

11. The following issues arise in relation to the relief the Court should grant:

    a. Whether section 31(2A) of the Senior Courts Act 1981 applies?
    b. If section 31(2A) does apply, whether any order should still be made?
    c. The form of any declaration;
    d. Whether the warrants / authorisations should be quashed, and whether the IPT should order data be destroyed?

The Statutes and Guidance

12. The facts in this case straddle the statutory provisions in RIPA and IPA.

Regulation of Investigatory Powers Act 2000

13. By section 1 of RIPA it is an offence to intentionally intercept a telecommunications system without lawful authority. Section 5 provides for the SoS to issue warrants to permit the interception of such communications.

14. Section 15 sets out the duty upon the SoS to ensure that certain safeguards are in place:

(1) "Subject to subsection (6), it shall be the duty of the Secretary of State to ensure, in relation to all interception warrants, that such arrangements are in force as he considers necessary for securing-

(a) that the requirements of subsections (2) and (3) are satisfied in relation to the intercepted material and any related communications data; and

(b) in the case of warrants in relation to which there are section 8(4) certificates, that the requirements of section 16 are also satisfied.

(2) The requirements of this subsection are satisfied in relation to the intercepted material and any related communications data if each of the following-

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

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

(c) the extent to which any of the material or data is copied, and

(d) the number of copies made

is limited to the minimum that is necessary for the authorised purposes.

(3) The requirements of this subsection are satisfied in relation to the intercepted material and any related communications data if each copy made of any material or data (if not destroyed earlier) is destroyed as soon as there are no longer any grounds for retaining it as necessary for the authorised purposes.

(4) For the purposes of this section something is necessary for the authorised purposes if, and only if-

(a) it continues to be, or is likely to become, necessary as mentioned in section 5(3);

(b) it is necessary for facilitating the carrying out of any of the functions under this Chapter of the Secretary of State;

(c) it is necessary for facilitating the carrying out of any functions in relation to this Part of the Interception of Communications Commissioner or of the Tribunal;

(d) it is necessary to ensure that a person conducting a criminal prosecution has the information he needs to determine what is required of him by his duty to secure the fairness of the prosecution; or

(e) it is necessary for the performance of any duty imposed on any person by the Public Records Act 1958 or the Public Records Act (Northern Ireland) 1923.

...

(8) In this section "copy", in relation to intercepted material or related communications data, means any of the following (whether or not in documentary form
(a) any copy, extract or summary of the material or data which identifies itself as the product of an interception, and

(b) any record referring to an interception which is a record of the identities of the persons to or by whom the intercepted material was sent, or to whom the communications data relates,

and "copied" shall be construed accordingly."

15. Section 71 places a duty on the SoS to issue one or more Codes of Practice, inter alia, on the performance of powers and duties under Parts 1 and 3 of the Act.

16. The first relevant Code of Practice issued under RIPA is "Interception of Communications" dated January 2007, where Chapter 6 deals with Safeguards. This deals with the destruction of material obtained at para 6.8:

"Intercepted material, and all copies, extracts, and summaries which can be identified as the product of an interception, must be securely destroyed as soon as it is no longer needed for any of the authorised purposes. If such material is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid under section 15(3) of the Act."

17. A revised Code was issued in January 2016. In relation to deletion, paras 7.8 and 7.9 are relevant:

"7.8. Intercepted material, and all copies, extracts and summaries which can be identified as the product of an interception, must be marked for deletion and securely destroyed as soon as possible once it is no longer needed for any of the authorised purposes. If such intercepted material is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid under section 15(3) of RIPA.

7.9. Where an intercepting agency undertakes interception under a section 8(4) warrant and receives unanalysed intercepted material and related communications data from interception under that warrant, the agency must specify (or must determine on a system by system basis) maximum retention periods for different categories of the data which reflect its nature and intrusiveness. The specified periods should normally be no longer than two years, and should be agreed with the Interception of Communications Commissioner. Data may only be retained for longer than the applicable maximum retention periods if prior authorisation is obtained from a senior official within the particular intercepting agency on the basis that continued retention of the data has been assessed to be necessary and proportionate. If continued retention of any such data is thereafter assessed to no longer meet the tests of necessity and proportionality, it must be deleted. So far as possible,

all retention periods should be implemented by a process of automated deletion, which is triggered once the maximum retention period has been reached for the data at issue."

18. Chapter 10 deals with duties in respect of Oversight. Para 10.3 states:

"Any person who exercises the powers in RIPA Part 1 Chapter 1 must report to the Commissioner any action that is believed to be contrary to the provisions of RIPA or any inadequate discharge of section 15 safeguards. He or she must also comply with any request made by the Commissioner to provide any such information as the Commissioner requires for the purpose of enabling him or her to discharge his or her functions."

Investigatory Powers Act 2016

19. The IPA Bill received Royal Assent on 29 November 2016. The relevant provisions as to interception of communications, equipment interference, bulk interception, bulk communications data, and bulk equipment interference came into effect on and after 31 May 2018.

20. Section 2 sets out the general duties as to privacy:

"2. General duties in relation to privacy

(1) Subsection (2) applies where a public authority is deciding whether-
(a) to issue, renew or cancel a warrant under Part 2, 5, 6 or 7 [the duty on the SoS]

...

(c) to approve a decision to issue, renew or modify such a warrant [the duty on the Commissioners]

...

(k) to apply for or otherwise seek to issue, grant, giving, modification, variation or renewal of a kind falling within paragraph (a), (b), (d), (e), (f) or (i) [the duty on MI5]

...

(2) The public authority must have regard to-
(a) whether what is sought to be achieved by the warrant, authorisation or notice could reasonably be achieved by other less intrusive means,
(b) whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant, authorisation or notice is higher because of the particular sensitivity of that information,
(c) the public interest in the integrity and security of telecommunication systems and postal services, and
(d) any other aspects of the public interest in the protection of privacy.

(3) The duties under subsection (2)-
(a) apply so far as they are relevant in the particular context, and
(b) are subject to the need to have regard to other considerations that are also relevant in that context.

(4) The other considerations may, in particular, include-
(a) the interests of national security or of the economic well-being of the United Kingdom,
(b) the public interest in preventing or detecting serious crime,
(c) other considerations which are relevant to-
(i) whether the conduct authorised or required by the warrant, authorisation or notice is proportionate, or
(ii) whether it is necessary to act for a purpose provided for by this Act,
(d) the requirements of the Human Rights Act 1988, and
(e) other requirements of public law.

(5) For the purposes of subsection 2(b), examples of sensitive information include-
(a) items subject to legal privilege,

..."

21. The duty in section 2(1)(a) falls on the SoS in issuing the warrant. The duty in section 2(1)(c) falls on the Judicial Commissioners acting under section 23 who approve the decision. The duty in section 2(1)(k) falls on MI5 in applying for a warrant.

22. Section 19(1) gives the SoS power to issue warrants, subject to certain conditions; section 23 provides for the approval of warrants by Judicial Commissioners.

23. Section 53(1) and (5) provide:

"53 Safeguards relating to retention and disclosure of material

(1) The issuing authority must ensure, in relation to every targeted interception warrant or mutual assistance warrant issued by that authority, that arrangements are in force for securing that the requirements of subsections (2) and (5) are met in relation to the material obtained under the warrant. This is subject to subsection (9).
(2) ...
(3) ...
(4) ...
(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))."

24. Section 55 gives safeguards in respect of items subject to legal privilege:

"55 Additional safeguards for items subject to legal privilege

(1) This section applies where an item subject to legal privilege which has been intercepted in accordance with a targeted interception warrant or mutual assistance warrant is retained, following its examination, for purposes other than the destruction of the item."

25. The same structure of safeguards in respect of warrants for targeted equipment interference, bulk interception, bulk acquisition of communications data termed in this litigation bulk communications data (BCD), and bulk equipment interference are set out in sections 129, 150, 171 and 191. For BPD the statutory safeguards in sections 221-223 are different, but the same requirements in respect of mandatory deletion are applied through the relevant Codes of Practice.

26. The IPA created the position of the Investigatory Powers Commissioner ("IPC"). By section 231 the IPC has a duty to report relevant errors in relation to a person to that person, and section 231(9) defines a relevant error as:

"(9) In this section "relevant error" means an error-
(a) by a public authority in complying with any requirements which are imposed on it by virtue of this Act or any other enactment and which are subject to review by a Judicial Commissioner, and
(b) of a description identified for this purpose in a code of practice under Schedule 7,
and the Investigatory Powers Commissioner must keep under review the definition of "relevant error".

27. In March 2018 a Code of Practice on "Interception of Communications" was issued pursuant to Schedule 7 of IPA. Chapter 9 deals with Safeguards, and at para 9.1 states:

"All material intercepted under the authority of an interception warrant and any secondary data must be handled in accordance with safeguards which the Secretary of State has approved in line with the duty imposed on him or her by the Act. These safeguards are made available to the Investigatory Powers Commissioner, and they must meet the requirements of section 53 for Part 2 warrants and section 150 for bulk interception warrants. Breaches of these safeguards must be reported to the Investigatory Powers Commissioner in a fashion agreed with him or her. The intercepting authorities must keep their internal safeguards under periodic review to ensure that they remain up-to-date and effective. During the course of such periodic reviews, the intercepting authorities must consider whether more of their internal arrangements might safely and usefully be put into the public domain."

28. Paragraphs 9.23 and 9.24 deal with Destruction of material obtained:

"9.23. Material obtained under a warrant, and all copies, extracts and summaries which can be identified as the product of an interception, must be scheduled for destruction as soon as possible once it is no longer needed for any of the authorised purposes. Section 263(1) of the Act defines destroy for the

purposes of the Act as deleting the data in such a way as to make access to the data impossible. If material obtained under a warrant is obtained other than for the purposes of destruction, it should be reviewed at appropriate intervals to confirm that the justification for its retention, is still valid under section 53(3) or, in the case of a bulk warrant, section 150(3) of the Act.

9.24. Where an intercepting authority undertakes interception under a bulk warrant the agency must specify (or must determine on a system by system basis) maximum retention periods for different categories of the data which reflect its nature and intrusiveness. The specified periods should normally be no longer than two years, and should be agreed with the Investigatory Powers Commissioner. Where communications are stored on a system, they will not be stored for the purpose of Investigatory Powers Commissioner oversight beyond the retention period already set for that system. Data may only be retained for longer than the applicable maximum retention periods if prior authorisation is obtained from a senior official within the particular intercepting authority on the basis that continued retention of the data has been assess to be necessary and proportionate. If continued retention of any such data is thereafter assessed to no longer meet the tests of necessity and proportionality, it must be deleted. So far as possible, all retention periods should be implemented by a process of automated deletion, which is triggered once the applicable maximum retention period has been reached for the data at issue."

29. Chapter 10 deals with error reports and relevant errors:

"10.14. A relevant error may only occur in one or more of the following circumstances:

- *there has been a failure to adhere to the additional safeguards set out at sections 26 to 29 of the Act*
- *there has been a failure to adhere to the restrictions on use or disclosure of material imposed by sections 53 to 55 and sections 150 to 154 of the Act.*

10.15. The following provides a non-exhaustive list of possible relevant errors by a public authority in complying with the requirements imposed on it that would fall within the description of a relevant error at paragraph 10.14:

...

- *retention of material obtained under a warrant when it is no longer necessary for the authorised purposes;*

...

10.17. When a relevant error has occurred, the public authority that made the error must notify the Investigatory Powers Commissioner as soon as reasonably practicable, and no later than ten working days after it has been established by appropriate internal governance processes that a relevant error has occurred. Such internal governance processes are subject to review by the Investigatory

Powers Commissioner. Where the full facts of the error cannot be ascertained within that time, an initial notification must be sent within an estimated timescale for the error being reported in full and an explanation of the steps being undertaken to establish the full facts of the error.

10.18. From the point at which the public authority identifies that a relevant error may have occurred, they must take steps to confirm the fact of an error as quickly as it is reasonably practicable to do so. Where it is subsequently confirmed that an error has occurred and that error is notified to the Commissioner, the intercepting authority must also inform the Commissioner of when it was initially identified that an error may have taken place."

30. The March 2018 Equipment Interference Code of Practice stated as follows:

"5.29. In this chapter, reference to an 'application' for a warrant includes the application form and draft warrant (including the draft instrument and any draft schedules). An application for a targeted interception warrant, a copy of which must be retained by the applicant, should contain the following information:
...
r) an assurance that all the material obtained under the warrant will be kept for no longer than necessary and handled in accordance with the safeguards required by sections 53 and 54 of the Act (see chapter 9).

5.30. When completing a warrant application, the intercepting authority must ensure that the case for the warrant is presented in the application in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which weakens the case for the warrant."

31. The Investigatory Powers Commissioner Office ("IPCO") produced Advisory Note 1/2018 entitled *Approval of Warrants, Authorisations and Notices by Judicial Commissioners* (8 March 2018). This is referred to below in relation to the submissions on the duty of disclosure.

Facts – Breach of statutory obligations by MI5

32. TE is a technology environment used by MI5 to store and analyse warranted and authorised data, that is data obtained under RIPA, IPA and the Intelligence Services Act 1994 ("ISA").

33. The main issue of fact to be determined in this section is the time at which MI5 became aware of the system failings in the TE relating to safeguards in the handling of data which had the effect that the statutory requirements were not being complied with.

34. At paragraph 86 of their second witness statement Witness A stated:

"MI5 was aware, as the contemporaneous documentation makes clear, of a very high risk that it was in breach of its statutory obligations from May 2016 onwards ... MI5 was aware of the possibility of compliance failures in the TE, including in relation to RRD (Retention, Review, Destruction), from late 2015 ...

In the period 2016 – 2018 MI5 took substantial steps to mitigate wider compliance risks of which it was aware."

35. The skeleton argument for the Respondents accepted that MI5:

"could, and should, have been aware that it was failing to comply in respect of RRD over Authorised Data in the relevant areas of its IT estate, triggering a requirement to notify the oversight body in 2016, almost 3 years before it did so."

The Respondents also accept that any knowledge derived from MI5 documents may be treated as within the knowledge of MI5 as a whole.

36. The Claimants in their skeleton argument submit that over an extended period of time MI5 engaged in systemic and systematic non-compliance with the safeguards imposed by statute. That non-compliance and the failure to make disclosure to the oversight bodies is said to have started at the latest by 2012. It is alleged that from 2013 there was a pattern of deliberate non-disclosure of known failings in the RRD procedures.

37. There is a second issue whether the MI5 failings in compliance extended beyond the TE to Areas 1 and 2 of TE2, and beyond RRD to other safeguards required by statute, including access controls, data copying and protection of LPP.

38. Following an investigation commenced by IPCO on 18 March 2019 very serious failings came to light. On 5 April 2019 the IPC made a decision that there had been "a serious failure to handle warranted data in compliance with the IPA for a considerable period of time" and that data had been held and handled "in an undoubted unlawful manner" ("the Generic Warrants decision").

39. On 9 May 2019 the Home Secretary made a statement to Parliament announcing the establishment of an independent review to be conducted by Sir Martin Donnelly, a former Permanent Secretary. On 15 July 2019 the Home Secretary made a further statement on the conclusion of the Compliance Improvement Review ("CIR"), which set out a number of summary recommendations. These were accepted by the SoS and the Director General of MI5. MI5 then established a Compliance Improvement Programme, which was subject to verification by an independent reviewer, Mary Calam. That independent review was published on 1 February 2021. Those two reports provide insight into the circumstances in which the TE was established and developed, and the issues as to compliance which subsequently emerged.

40. The CIR conducted by Sir Martin Donnelly stated at paragraph 35:

"The first major compliance issue with the TE had first been identified in 2014 [REDACTED]. Subsequent internal reviews identified three major causes:

(i) [A failure to create a type of record on another TE;]
(ii) A failure to apply review, retention and disposal policy to the repository of data on the [TE];

(iii) A failure to understand what data was held on the [TE].

The reviews framed (ii) and (iii) as risks relating to [REDACTED], but not in terms of MI5's compliance with its statutory obligations."

2010 - 2013

41. The TE was granted interim accreditation on 15 October 2010 and a TE Security Working Group was established. The role of the Accreditor was to act as an impartial assessor of the risks that an IT service or system might be exposed to through its lifecycle and, inter alia, to escalate medium or high residual risks to the appropriate authority for a decision. The interim accreditation granted on 15 October 2010 was restricted, to holding only restricted information, and the accreditation was subject to a number of residual risks which were rated as high. Those risks included the lack of policies mandating how the TE was to be utilised, managed and supported. A plan to resolve these issues was considered after the accreditation. A compliance group was established at a meeting held on 4 November 2010.

42. The purpose of the Management Board Paper prepared for discussion on 16 April 2010 was to set out the planned programme to deliver the "surge on Information Assurance". The statement of intent at annex A included the establishment or strengthening of mechanisms which would ensure compliance, and the risks noted included the major compliance risk defined as:

"(the) need to ensure that relevant information is available for compliance purposes, so that we can – with a high degree of confidence – recover information relevant to a disclosure exercise (and thus minimise the risk of compliance failure occurring)."

It noted that

"Current 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. Simultaneously we need to increase confidence that information is being appropriately handled and adequately protected...".

43. That paper does not evidence that systemic failings had occurred. It recognises that significant deep-rooted risks existed and proposed means by which those risks could be mitigated.

44. On 13 September 2010 an assistant director issued a paper on 'Recent Compliance Failures' which raised a number of issues. The points made in the paper included:

(1) the scale of recent compliance errors justified a fresh look at how compliance was handled, even if no single systemic cause underlay the recent failures;

(2) the principal vulnerability was a new and serious compliance error and no strategic compliance framework in place to help mitigate the risk;
(3) in some areas there was an imperfect understanding of processes and the scale of risk they entailed; addressing knowledge and culture in a more systematic way was a priority;
(4) some small strategic changes would go a long way to reduce risk, at minimal cost; in outline these involved systematically embedding compliance in management and processes.

45. The paper stated that the implementation of the recommendations made should not be a major exercise and could be done within the existing resources. The compliance failures had been reported to the Interception of Communications Commissioner ("IOCC") and the Intelligence Services Commissioner ("ISC"). MI5 had explained to the Commissioners the steps being taken to prevent recurrence. The CIR analysis of this report was that *"it focuses on issues related to collection and authorisation, rather than how data should be handled once obtained."* In May 2011, a Compliance Audit report was issued. The IOCC had been briefed on the incidents and the proposed compliance error mitigations. The conclusions included the recognition that "the pace of change, growth, complexity, scope & demand of/in [a team] was not matched by compliance knowledge and practice" and that "awareness of compliance issues had drifted". The recommendations included that there should be quarterly compliance reviews.

46. In June 2011, the IOCC issued his annual report for 2010. In relation to MI5 the inspectors were generally satisfied that the Security Service had achieved a good level of compliance with RIPA. The Commissioner stated:

> *"7.35. It is inevitable that some mistakes will be made, especially considering the fact the Security Service is dealing with large volumes of communications data requests in complex investigations and that there is a degree of automation in the process. It is important to make the point that their error rate is still very low in comparison with the number of requests which are processed for communications data. I am satisfied with the measures that the Security Service have put in place to rectify these issues and these should prevent further recurrence of such errors. It is clear to me that the Security Service is committed to achieving the best possible level of compliance with the Act and Code of Practice."*

47. A data retention policy was issued in February 2012 which stated that its purpose was *"to ensure we legally comply with the terms of our data handling arrangements and to make sure we do not unlawfully interfere with privacy by retaining material obtained through interception that our warrant applications say we will not keep."*

48. On 1 May 2013, MI5 published a specific RRD policy for all MI5 staff, the aim of which was *"to explain the rules governing the Security Service's management of its information holdings during, and at the end of the information management life cycle"*. The policy emphasised that *"to satisfy legal requirements, the Service must judge whether legal justification still exists for the continued retention of its information holdings and whether they should be retained, archived, destroyed, or released to the National Archives"*.

49. The Management Board Paper discussed in June 2013 provided an update on the 'Information Management Transformation Programme' ("IMTP") on information risks. The paper was principally directed at improving MI5's overall information management to ensure MI5 could carry out its core functions. A programme of measures was proposed to the Board which aimed *"to improve the integrity of our record, enhance our ability to discover our information and increase confidence in the protection of the sensitive information we hold"*. The paper recognised that a major shift in attitude and behaviour was required. The paper was endorsed by the Management Board. It does not evidence any intention by MI5 that IMTP policy should not be carried into effect.

50. Between 2010 and 2013 there were compliance failures which were discovered by MI5 and reported to the relevant Commissioners. In each case steps were taken to put forward remedies and those remedial steps were accepted by the oversight body. There is no evidence that those errors continued in breach of the statutory safeguards. It is clear from the CIR that Sir Martin Donnelly did not consider that the paper dated 13 September 2010 related to safeguarding arrangements. His conclusion was that the first major compliance issue with the TE arose only in late 2014. Further reasons for this decision are contained in the CLOSED judgment.

2013 Enquiry from the Interception of Communications Commissioner

51. In June 2013 Edward Snowden disclosed to a number of journalists classified information obtained from the United States National Security Agency. By letter dated 14 August 2013 the Interception Commissioner, Sir Anthony May, requested that each of the law enforcement and intelligence agencies which undertook warranted interception of communications under Part 1 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 material ... with particular reference to every generic database in which intercepted material is for a time stored."*

52. On 24 October 2013, the MI5 Deputy Director General (DDG) answered with an overview of the retention, storage and deletion of intercepted material by MI5. In that letter he stated that MI5 had included in the response all voice and content data acquired through RIPA Part 1, Chapter 1.

53. On 6 November 2013 IOCC undertook an inspection, the outcome of which was set out in a letter to MI5 dated 19 December 2013. The letter noted that "certain themes" had emerged from the review of RRD of intercept material and contained the following summary of his concerns:

"To summarise:

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 inspection, MI5 were in the process of mobilising their Information Management Transformation Programme, 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."*

54. In a note dated 16 December 2013 the Home Office Head of the National Security Unit ("NSU") briefed the Home Secretary on the IOCC inspection of MI5 stating:

"MI5 have [compliance problems] where they are retaining material for too long and deletion is not always effected. MI5's IT systems, especially post-7/7 have focused on [reducing the risk of] intelligence failure, and as MI5 recognise, the legal compliance of their IT systems has not fully kept pace. MI5's major IT reform programme, the Information Management Transformation Programme (IMTP) is seeking to rectify this."

55. On 26 November 2014 the Interception Commissioner, then Sir Paul Kennedy, carried out an inspection of MI5. The objectives included a review of the recommendations from the previous inspection, and to ensure that errors were being reported and systems reviewed where any weaknesses or faults were exposed. The subsequent report noted that the Commissioner 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."*

56. The conclusion of the Commissioner was that interception was being undertaken lawfully and MI5 had a good level of compliance with RIPA and its Code of Practice. The work that MI5 was continuing to undertake in relation to the retention, storage and destruction of intercepted material was significant. The Deputy Director General had provided IOCC with further information on 23 December 2014. The letter stated that the longer-term approach and design of RRD capability was part of MI5's programme.

57. It is accepted by MI5 that it did not inform the Interception Commissioner about RRD issues in relation to multiple systems as MI5 was not aware of any specific RRD issues in these areas at that time. MI5 asserts that it did provide a full and candid accounts of the matters of which it was aware and which had been requested by the Commissioner. This point is further discussed in the CLOSED judgment.

58. The report of the IOCC for 2014 was published in March 2015. The report referred to the enquiry made of the interception agencies in August 2013, which led to major reviews of RRD followed by recommendations from the Commissioner, which were accepted by all the agencies. At paragraph 6.65 it was stated that those agencies which had not yet managed to implement the recommendations in full were waiting on technical changes to be made to IT systems.

59. The Tribunal does not accept that there was any failure properly to respond to the enquiries made by IOCC. MI5 had published a RRD policy for all MI5 staff and issued revised handling arrangements for material obtained under RIPA interception warrants. In relation to RRD, MI5 was not aware of serious RRD failings in relation to multiple systems. There was no evident failure in compliance in those specific areas which required to be reported to IOCC. Further reasons for this decision are contained in the CLOSED judgment.

2014 - 2015

60. The evidence of Witness A in their second statement at paragraph 88 stated that MI5 was aware of the possibility of compliance failures in the TE from late 2015. Reports provided to the Management Board of MI5 from about 2015 set out relevant risks in the risk register including:

    (i) Risk 2, the risk that *"MI5 fails to create, use or store information adequately and in a legally compliant manner";*
    (ii) Risk 3, the 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".*

61. In January 2014 (with a second version issued in October 2014), MI5 consolidated the guidance on information management into a single policy known as the Information Management Policy. The aim was to *"set out how MI5 will manage its information in order to give effect to MI5's overarching Information Principles"*, one of which was that *"we will manage our information and only keep it for as long as necessary for our functions".*

62. On 24 March 2014, the TE was re-accredited as a *"[restricted] system"* notwithstanding that *"[A number of risks were noted]"* and the risks were assessed as "HIGH" and "MEDIUM-HIGH". A Performance Report 2014/2015 was prepared for the MI5 Management Board. It reported that progress was being made on compliance with the RRD policy. The paper referred to *"[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"*, and stated that there was no change in Red Amber Green ("RAG") status which remained AMBER. The Management Board was also informed

that risks relating to legal disclosure had become apparent because of the absence of a formal, comprehensive and effective RRD policy.

63. On 18 November 2014 a (gisted) minute stated as follows:

> *"The document identifies a risk of incorrect or partial disclosure in legal proceedings. There are issues with data in 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. The document identifies that a disclosure search may not look into all areas. As such MI5 could not expect the search mechanism to find such data. The document proposes that MI5 explores agreeing a process whereby retained data is held in one place with an agreed format for how the search process examines that single pot".*

There was a subsequent minute dated 13 October 2015 which referred to the information which had been identified in 2014 in relation to legal proceedings. The possibility of information risk in legal proceedings had not been eliminated but reasonable steps had been taken. It was proposed to focus on processes going forward, while the remaining legacy risk was assumed to be diminishing.

64. The Executive Board minutes dated 7 July 2015 recorded that the Board agreed the importance of completing work on the bulk data strategy to prepare for "a more formal statutory footing". The Board agreed that MI5 was at a compliance watershed and a structured programmatic approach would be needed to address the risk to statutory compliance as a priority, together with RRD.

65. The Claimants submit that these documents disclosed fundamental failings in data holdings so that RRD policies were not being properly applied, much of the data was being kept in breach of RRD policies, and there was a risk of incorrect or partial disclosure in legal proceedings. Sir Martin Donnelly in the CIR noted that the *"first major compliance issue with the [TE]"* was identified in 2014, which appears to be a reference to the minute dated 18 November 2014. The evidence of Witness A at paragraph 86 stated that MI5 was aware of the possibility of compliance failures in the TE from late 2015, but the CIR places the awareness of compliance failures in late 2014.

66. The Tribunal finds that from late 2014 there were serious failings in compliance with the RRD policies which required urgent action to be taken by the Management Board of MI5.

2016 - 2019

67. The IPA Bill received Royal Assent on 29 November 2016. The relevant provisions as to interception of communications, equipment interference, bulk interception, bulk communications data, and bulk equipment interference came into effect on and after 31 May 2018 and bulk personal datasets in July 2018. A performance report to the Management Board for 2015/2016 had noted that the IPA Bill created the most challenging area of legal work, and a project board was set up to focus on this work.

68. The Respondents accept in their submissions that MI5 *"could, and should, have been aware that it was failing to comply in respect of RRD over Authorised Data in the relevant areas of its IT estate, triggering a requirement to notify the oversight body in 2016, almost 3 years before it did so"*. This is consistent with the evidence of Witness A that *"MI5 was aware, as the contemporaneous documentation makes clear, of a very high risk that it was in breach of its statutory obligations from May 2016 onwards."*

69. Given these concessions, it is only necessary to consider the most significant documents which reveal serious failings in compliance with MI5's statutory obligations, and its failure to recognise and act upon these failings.

(1) On 27 January 2016 the Bulk Data Review Panel identified a lack of governance across the TE2 Area 1.

(2) A paper on legal risk on compliance in January 2016 identified risk arising from data in *"ungoverned spaces"* on the TE, in relation to the legal obligation to disclose material in court cases.

(3) A minute dated 14 October 2016 noted that the understanding of the TE was not as complete as the Board would wish and the current level of action was not acceptable. The author had been asked to carry out a review of the TE, including a summary of the "key risks/issues generated by the TE, their scale and (for risks) proximity".

(4) An undated paper noted a series of risks in relation to TE and commented that much of the TE was akin to *"wild west"* spaces.

(5) A paper dated 21 March 2017 asked for endorsement of the formal accreditation statement, notwithstanding that there was a series of identified compliance and legal risks, concluding with the statement that MI5 would currently be unable to give sufficient assurance externally that it was handling information in accordance with current legislation.

(6) The TE Improvement Programme dated 27 April 2018 itemised a series of high risks followed by a problem statement that MI5 was holding too much risk and was unable to report confidently on compliance with legal obligations.

(7) In July 2018 MI5 issued three sets of internal handling arrangements for material to be held or obtained under an IPA warrant covering the different safeguards required in respect of interception and equipment interference, communications data, and bulk personal datasets.

(8) In October 2018 an education session with the Executive Board made clear that an appropriate framework had never been established in the TE, and systems were not handling data in accordance with legal obligations, as there was a lack of RRD processes.

(9) On 30 October 2018 the Executive Board noted the fundamental challenges that required urgent and sustained action, that MI5 was unable to provide robust assurances to its oversight bodies that data held in the TE could not be accessed unlawfully, and that RRD had not been implemented across all of the TE, potentially including warranted material, raising a risk that elements were non-compliant. It was suggested that MI5 would want to pre-emptively brief oversight bodies.

(10) A minute of a meeting at the Home Office on 18 October 2018 noted that MI5 had decided not to brief the IPC as the relevant RED risk had moved to AMBER.

(11) On 28 November 2018 MI5 informed the Home Office that the significant risks were being managed appropriately and that MI5 were confident that there was no need to brief the Home Secretary at that stage.

(12) In a paper dated 30 December 2018, submitted by the information policy director, advice was given to the Board in these terms:

> *"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."*

(13) On 24 January 2019 a committee of the Board took the decision to inform the IPC and the Home Office of the current position; that decision was approved by the Director General.

70. In a letter dated 31 January 2019 the DDG wrote to the IPC and the Director General of the Office for Security and Counter-Terrorism ("OSCT") summarising a recent MI5 review of the impact of MI5's work on the transition of warrantry arrangements to the IPA. The letter stated that *"the large and complex implementation task has gone well so far"*, *"the IPA has brought real benefit for MI5"* and *"within MI5, implementing the IPA, under a programme ... has helped strengthen our culture of legal compliance ... The Act's implementation has been challenging ... we have spent [REDACTED] delivering changes to [REDACTED] our technical systems ... The "double lock" has not significantly impacted our operations and we have continued to be able to gain approval for the vast majority of our warrants and operations."*

71. By letter dated 21 February 2019, a Director wrote to Graeme Biggar, Director of National Security at the Home Office, to inform him that MI5 intended to brief the IPC on challenges in maintaining assurance in terms of legal compliance with regard to the TE. 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; however, [there is] an inconsistency in approach." 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."*

72. On 27 February 2019 MI5 made its presentation to the IPC. The response of the Commissioner was to require MI5 to give a full explanation of the situation in writing. A Director sent a letter dated 11 March 2019 setting out the challenges faced by the TE system. The letter stated that a MI5 compliance team had identified in January 2016 that *"data might be being held in ungoverned spaces in contravention of our policies"*. It also stated that the risk had been reported to the 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 be compliant with the Investigatory Powers Act."* The only explanation offered as to why IPC had not been informed earlier was as follows:

> "I apologise if you consider that we should have briefed you on these matters earlier. The truth is that we did not sufficiently understand the issues ourselves under the (Executive Board) discussions in late 2018 and our understanding is still developing. However, we considered the issues were of sufficient importance to brief you at this stage."

IPCO inspections, reports and decisions

73. IPCO conducted an inspection of the TE between 18 and 22 March 2019. On 29 March 2019, IPCO issued its First Inspection Report. 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 TE], to the extent that they should have carefully considered the legality of continuing to store and exploit operational data in [the TE]. The risks were also sufficiently clear that they should have been communicated to the Investigatory Powers Commissioner". The RRD RAG rating was assessed as RED.

74. On 5 April 2019, Sir Adrian Fulford issued his 'Generic Warrant Decisions'. This decision was highly critical of the failure of MI5 to manage data in the TE in accordance with its statutory duty and of the conduct of the agency in failing to report its failures at an earlier stage. The key conclusions of his decision were:

(1) the manner in which data had been held and handled was undoubtedly unlawful;

(2) there had been a serious failure to handle warranted data in compliance with the IPA over a considerable period of time;

(3) warrants had been granted and judicially approved on an incomplete understanding of the true factual position;

(4) by January 2018 the Management Board had a clear view of the serious problems which should have caused MI5 to consider the legality of continuing to store authorised data;

(5) the seriousness of the failings required MI5 to be placed in effect in "special measures" so that if MI5 was unable to give the reassurance that new warranted material would be handled lawfully then it was likely that future warrant applications would not be approved by the Judicial Commissioners.

This decision was focused on the TE. It covered not only the RRD aspects of Handling Arrangements, but also safeguards including access to warranted material, and data subject to LPP.

75. IPCO conducted a further inspection of TE between 10 and 16 April 2019. On 26 April a second inspection report was produced. That report communicated two critical recommendations which, if not addressed, would affect MI5's compliance status.

76. On 3 May 2019 the MI5 Oversight Team wrote to IPCO notifying potential issues relating to two areas of another technology environment, TE2. The letter referred to TE2 Area 1 and TE2 Area 2. Initial scans of Area 1 had identified files which might contain warranted data, but this was stated to be a complex area which was challenging to investigate. It was admitted that knowledge of some compliance risk associated with TE2 Areas 1 and 2 had been held by MI5 in 2016. That letter elicited a swift answer from the IPC sent on 8 May 2019 raising concerns that MI5 appeared to have been aware of the compliance risks in TE2 Areas 1 and 2 since 2016. In reply, the Director General explained that MI5 did not consider that there were underlying issues in TE2; only two issues in TE2 Areas 1 and 2 had been identified as being of concern.

77. Further inspections were carried out by IPCO in June and September 2019. The third inspection report dated 22 July 2019 included the requirement 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 ..."*. The fourth inspection report was dated 22 October 2019. Its key observations noted that MI5 had adequate arrangements in place to ensure that warranted data was compliant with the relevant IPA safeguards, but that work to delete warranted data from TE was at an early stage. MI5's use of the IT system in question was determined to be fit for purpose. IPCO issued a public statement from the Commissioner stating:

"MI5 has devoted substantial resources both to the programme of work to fix the compliance problems identified and to service this intensive inspection regime. I am confident that MI5's remediation work has secured compliance with the standards required. I have been impressed by MI5's reaction to our criticisms, in particular the speed, focus and dedication with which they acted to rectify the situation."

78. The confidential annex to the 2019 IPCO report gave some information on the compliance failings and errors that were discovered following the first inspection conducted in March 2019. It was reported that MI5's remediation work had made very substantial progress in deleting data from the TE, which task was to be completed as soon as possible.

Summary of findings – MI5 failings

79. For the reasons given above, we find that there were serious failings in compliance with the statutory obligations of MI5 from late 2014 onwards, and those failings ought to have been addressed urgently by the Management Board.

80. In a MI5 committee paper dated 4 October 2018 it was reported that there were legal compliance risks marked as RED which could lead to legal challenges. In an education paper presented in October 2018, Board members were informed that the systems were not handling data in accordance with legal obligations and that there was a lack of RRD and clear processes to manage data in TE. Notwithstanding that advice, MI5 informed the Home Office on 18 October 2018 that it was not necessary to brief IPCO as the RED risk had moved to AMBER. MI5 was well aware, as disclosed in the Executive Board Paper dated 30 October 2018, that there was a risk that the IPC might be unwilling to authorise further warrants until the lack of an effective RRD policy was rectified. Yet on 28 November 2018 the DDG informed the Home Office that the significant risks were being managed appropriately and there was no requirement to brief the Home Secretary. The Management Board had considered whether there might be *"options for accepting more risk in this area"*, a proposal which appears extraordinary in light of the advice which the Management Board had received in October. Below we deal with the question whether the use by MI5 and the Home Office of risk factors relating to compliance had the effect of concealing that substantial compliance failings had permitted MI5 to breach its statutory obligations.

81. On 18 December 2018 the Management Board was advised to report to IPCO as soon as possible. It was not until 21 February 2019 that IPCO was given notice that MI5 wished to brief the Commissioner of some of the challenges that had been discovered in the systems. In its written explanation of the position sent to IPCO on 11 March 2019 MI5 took the line, at paragraph 10, that in 2016 a review of legal compliance had led a team to discover that data might be held in ungoverned spaces, the risk had been identified further in 2018, it was not until late 2018 that the Executive Board noted the scale of the challenges involving TE, and *"we did not sufficiently understand the issues ourselves until the (Executive Board) discussions in late 2018"*. The view taken by Sir Adrian Fulford was that the Management Board had a clear view of the serious problems by January 2018 at the latest, MI5 should have considered the legality of continuing to store authorised data in the TE, and had failed to consider the need to inform IPCO and the Home Office at that

stage. The explanatory letter which had been sent on 11 March 2019 was clearly considered by Sir Adrian to be economical with the truth. In a subsequent meeting with the Home Office, Sir Adrian described the failure properly to disclose the seriousness of the issue as inexcusable.

82. Sir Martin Donnelly's conclusion in the CIR, having interviewed a number of officials, was that there was no attempt by MI5 to hide information, but *"the information shared was insufficient to highlight the increasingly urgent problems caused by continuing compliance difficulties"*. The Tribunal has no evidential basis to find that any officers of MI5 did seek to hide any information, but the failure of the Management Board to disclose the compliance failings to IPCO until February 2019, and then only in unilluminating terms, was a serious misjudgement.

Facts – oversight by the Home Office

83. From 2016 MI5 was required to provide Quarterly Performance Reports ("QPR" or "QR") to the National Security Unit ("NSU") at the Home Office for communication to the Home Secretary. The first QPR to make reference to a compliance risk was notified to the Home Secretary on 15 December 2016. The QPR stated:

> *"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 [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".*

84. On 24 March 2017 a QPR was forwarded to the Home Secretary. It contained this note:

> *"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. 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 next category (orange – high) by the third quarter of 2017-2018."*

85. On 18 October 2018 a meeting of MI5 with the NSU discussed the current QPR, in particular whether it was necessary for MI5 to brief the IPC. The response from MI5 was noted as follows:

> *"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."

86. On 28 November 2018 a meeting of MI5 with the NSU discussed the QPR for Q2 2018/2019. The minutes recorded, under the heading of 'Legacy IT':

"This was a complex and multi faceted problem ... 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 ...

DG OSCT asked whether there is anything in this space which keeps DDG/DGS "up at night" ...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."

87. These assurances given to the Home Office were not consistent with the internal papers and advice received by MI5 in October 2018.

(1) MI5 committee paper dated 4 October 2018:

"It is assessed 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."

(2) Education session for the Executive Board October 2018:

"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".

(3) Executive Board Paper 30 October 2018 at paragraphs 11 & 12

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

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 and reputational damage."

88. It was not until 21 February 2019 that MI5 informed the Director National Security that MI5 was about to brief the IPC on "aspects of our IT systems and platforms". On 26 February 2019 the Home Secretary was informed that MI5 was briefing the IPC on the following day. On 27 March 2019 the Home Secretary was advised by the Deputy Director National Security that MI5 had identified significant shortcomings in the information handling regime, and a recent IPCO inspection had confirmed that view. The immediate concern was that some warranted data held by MI5 had not been handled as required by the provisions of IPA, but MI5 had considered that the use of some measures was important to their ongoing operational effectiveness and to national security. The Home Secretary, pending legal advice, agreed, to consider continuing to approve MI5 warrant applications, given the importance for national security.

89. 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 DG stated:

> *"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 ... [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".*

90. On 9 April 2019 the Investigatory Powers Unit provided a further brief to the Home Secretary. Towards the end of that note it referred to a review which was to be commissioned, and stated:

> *"One of the areas that the review will clearly need to focus on is why IPCO were not notified sooner. We are currently conducting a review of our own knowledge on this issue and have checked the minutes of our quarterly review meetings with MI5. These risks were not raised proactively by MI5. In June 2018 OSCT asked MI5 about ...where the risk of MI5 not complying with their statutory obligations was rated "red". This led to a general discussion around MI5's programme of work to ensure it complied with the IP Act. The scale of the issue ... and associated risks were not made apparent during this discussion. It was recorded as an action in the minutes of the meeting that MI5 would brief the IPC on the risks around IP Act compliance. When OSCT asked what progress had been made in briefing the IPC in the next meeting we were informed that the rating of the risk had been downgraded to 'amber' and that MI5 no longer felt that it was necessary to brief the IPC.*
>
> *Prior to the commencement of various provisions in the IPA there was a process by which relevant parties formally wrote to the Home Office to confirm their readiness for commencement. Letters were received from MI5 on 17 May 2018 in relation to interception and equipment interference, including bulk data and 9 July 2018 in relation to the commencement of the bulk communications data and bulk personal data set provisions. Both letters were clear that MI5 would be*

ready to "operate in full compliance with" the relevant provisions of the IPA. Whilst these letters set out a number of assumptions or caveats surrounding that confirmation no mention was made of a risk of non-compliance with the safeguards."

In a separate Annex C, the Home Office listed the QPR meetings since January 2018 and stated that the issues had not been raised proactively by MI5 in any of the QPR meetings; the issue was raised in low levels of detail in the 'risk register' section. The discussion in the Q4 meting in June 2018 was in very general terms and did not capture the extent of the problem faced in relation to compliance.

91. What those notes do not answer is why, following the QR meeting on 24 March 2017 in which the risk was expressed in stark terms, "a red ("very high") risk", no enquiries were made by the Home Office for details of this risk, how the TE operated and how the risk was to be mitigated.

92. By letter dated 24 April 2019 to the Home Secretary the Director General accepted that MI5 had failed to recognise the seriousness of its legal non-compliance (at paragraphs 3 & 5):

"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."

93. Henry Hirsch was the Deputy Director National Security at the Home Office from August 2016 to January 2019, responsible for the oversight of MI5. QPRs were a key aspect of that oversight. Under the protocol between the Home Office and MI5 the Home Secretary required good visibility of the risk carried by MI5. For the period January to May 2019 Jonathan Emmett covered the role of Deputy Director National Security and was responsible for the Home Office oversight of MI5.

94. Mr Hirsch states in his first witness statement that, for the time he was in post, his understanding was that:

"risks on the risk register were related to potential problems rather than current issues, therefore in the context of compliance risk it was a concern that they may not be compliant, not that they were currently non-compliant."

So he stated the *"specific link between the compliance risk and the TE compliance issue was not established"*. Mr Hirsch repeats the point in his second witness statement that the compliance risk was considered to be about *"the prospect of future failure rather than the existence of a failure at that time"*.

Notwithstanding that the red risk was stated to mean there was a very high likelihood of it happening:

> *"MI5 and the Home Office viewed this as a current risk and potential issue if left unaddressed but it was not an issue at that time... this identifies the possibility of failure but it is not presenting it as current (in that moment) issue ... this demonstrates that the risk was not considered to be a materialised issue at this time and therefore our response to it was tempered accordingly."*

The compliance risk was *"a long term challenge that was being tackled by MI5 which the IPA would partially address".*

95. The QPR note dated 15 December 2016 was the first occasion on which a compliance issue had been placed on the risk register. Mr Hirsch states:

> *"The note did not elaborate on what specific element of the relevant legislation MI5 considered it might not be found to be compliant with. We had no additional information beyond this as to which specific element of information handling the risk related to. ... MI5's expected trajectory was for the risk to downgrade from red to amber in ...".*

96. Mr Hirsch states that in February 2017 compliance remained a RED ('very high') risk in the QPR for Q3 2016/2017. It was agreed that there would be a separate specific meeting with MI5 on the compliance risk, but Mr Hirsch was unable to attend. The meeting was not minuted, as was the normal practice for a meeting outside the QPR process. The recollection of the Deputy Head who attended the meeting was very generalised. The meeting in February 2017 with MI5 did not answer the points about which Mr Hirsch was concerned. The upshot was that *"MI5 had already made progress against the red risk, they did not expect it to go green this year (i.e. in 2017) but there was a plan in place to get it to amber. They also felt that they had a credible story to tell to the new Commissioners".*

97. It had been intended to put to Ministers specific advice on this briefing, but the occurrence of the Westminster Bridge attack on 22 March 2017 prevented that happening. On 24 March 2017 a routine QPR note was put to the Home Secretary, but the MI5 advice did not specify which elements of the statutory obligations were being referred to. This was a point reiterated by Mr Hirsch in respect of the QPR report provided to the Home Secretary on 13 August 2018. So on his evidence Mr Hirsch did not know, and did not ask, which were the statutory obligations which MI5 was at risk of breaching.

98. The QPR note in February 2018 did not include the continuing compliance risk rated RED because of other priorities. However, junior officials were asked to raise queries with MI5. The general thrust of the email in response was that MI5 was on track with IPA implementation, it had had a series of positive sessions with the IPC, and remained on track to reduce the risk to AMBER by [REDACTED] 2018/2019.

99. In October 2018 the compliance risk had been reduced to AMBER, although risk 3 remained RED. Prior to the meeting one of Mr Hirsch's team asked MI5 what the TE was. The explanation was provided to DG OSCT, but apparently not to Mr Hirsch. His view was *"While there were*

concerns about compliance risks generally it was not necessary to understand exactly what systems they related to".

100. This is not consistent with Mr Hirsch's first witness statement at paragraph 55 which states:

> *"I asked the Deputy Director responsible for compliance to provide greater insight into their IT infrastructure. I wanted to ensure the Home Office had oversight of the impact of the issue. I was particularly concerned with trying to understand which data sets were impacted by ... and therefore sought to understand which data was stored on which environment. We subsequently provided an information note to the Home Secretary and Security Minister on this issue ..."*

At paragraph 56 he says that he did not fully understand the underlying data architecture, but MI5 had agreed to conduct a more in-depth discussion of the TE programme to help him understand it. However, that discussion did not take place. He did not identify the compliance issue as relating to TE but as an issue with the legacy IT systems generally.

101. It is not apparent from this evidence that at any stage the Home Secretary received advice on the seriousness of the longstanding compliance risk. The only element of advice on the QPR from Home Office officials to which Mr Hirsch refers is:

> *"We met [department colleagues] to discuss their work to manage this risk. It seems clear that MI5 takes this risk seriously and is seeking to address is comprehensively."*

In Mr Hirsch's opinion *"When the totality of the content of the document (i.e. paragraph 8 of the QPR dated 24 March 2017) is considered, and bearing in mind also the detailed meeting with MI5 in February 2017, it is clear that we had made sufficient inquiries on behalf of the Home Secretary and were confident that MI5 were managing the risk appropriately."*

102. After the seriousness of the compliance issues became apparent to the Home Office in February 2019 it was Jonathan Emmett who was responsible for the oversight of MI5. In the note put to the Home Secretary on 9 April 2019 the view expressed was that it was MI5 which had failed properly to disclose the compliance risks:

> *"We are currently conducting a review of our own knowledge on this issue and have checked the minutes of our quarterly review meetings with MI5. These risks were not raised proactively by MI5. In June 2018 OSCT asked MI5 about ... where the risk of MI5 not complying with their statutory obligations was rated "red". This led to a general discussion around MI5's programme of work to ensure it complied with the IP Act. The scale of the issue with [TE]... and associated risks were not made apparent during this discussion."*

103. In his first witness statement at paragraph 28 Jonathan Emmett referred to the QR meetings which had taken place since January 2018, when he took over as Deputy Director National Security, which were summarised in a note, and stated:

> *"... the issue was not raised proactively by MI5 at any of the meetings and only low levels of detail were provided in the risk register for Q4, it was queried and then followed up on the next two meetings when MI5 said they were still considering whether and how to raise this with the IPC."*

104. On consideration of the evidence of Mr Hirsch it is clear that MI5 had not been forthcoming on the nature, scale and seriousness of the compliance risks referred to in the QR meetings after January 2018. However, it is also clear that the Home Office did not press MI5 for any detail nor challenge the very generalised assurances which had been offered. The statement in the Respondents' skeleton argument at paragraph 144 that Mr Hirsch had made sure there was a specific briefing from MI5 on the compliance risk covered in the risk register is not sustainable.

105. In his witness statements Mr Hirsch stated that risks on the risk register *"were related to potential problems rather than current issues ... it was a concern that they may not be compliant not that they were currently non-compliant"* and the QPRs identified the *"possibility of failure but it is not presenting it as current (in that moment) issue"*. The meaning of the statement that MI5 was not considered to be currently "in that moment" non-compliant with its statutory obligations is not at all clear. The logic appears to be that, notwithstanding that the risk was from March 2017 at the latest described as being a long-standing RED "very high" risk, it was to be regarded only as covering a potential risk of future failure, implying that there had not actually occurred any failures in compliance in the past.

106. Throughout the history of this matter up to 2019 MI5 had categorised the issue in relation to failing to comply with statutory safeguards as a "non-compliance risk". The Home Office adopted the same approach by assuming that a risk factor was only a risk "in the moment" and as such it could be accepted and need not call into question the underlying lawfulness of warrants. A very similar use of language was adopted by the Canadian Intelligence Service and considered by Gleeson J in the Canadian Federal Court in *(In the matter of an application by REDACTED for warrants pursuant to s.12 and 21 of the Canadian Intelligence Service Act RSC 1985 C C-23 and in the matter of Islamic Terrorism* ("the Canadian Case") [2020] FC 616, where he considered how the characterisation of legal "risk" and statutory safeguards related. At [129]-[131] Gleeson J said:

> *"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 an 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 authorised 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 also have contributed to the failure of those involved in the warrant approval process to identify the information collected as a result of this process as having been unlawfully collected. Lack of awareness of illegality has been advanced as one explanation for the breach of candour."*

The error in the approach of the Home Office was to accept the references to serious risks in the QPR as not having any consequences for MI5's compliance with its statutory obligations. Statements in the form of risk factors could not be relied upon as excusing any actual compliance breaches.

107. On that evidence, the Tribunal finds that adequate enquiries were not made as to the longstanding compliance risk which had been reported to the Home Office on several occasions from December 2016. No explanation was sought or offered or reported to the Home Secretary as to the scale and seriousness of the risk to the handling arrangements required by RIPA and IPA, nor any advice as to the effect of that risk on the power of the Home Secretary to authorise warrants. It was not until 27 March 2019 that the Home Secretary was advised that there was an immediate concern that some warranted data held by MI5 had not been handled as required under the provisions of the Investigatory Powers Act.

Facts – the scope of the failings beyond TE and beyond RRD

108. The Claimants raise an issue whether the MI5 failings in compliance extended beyond the TE to Areas 1 and 2 of TE2, and beyond RRD to other safeguards required by statute, including access controls, data copying and protection of LPP.

109. This issue will be considered in the CLOSED judgment.

Facts – the BPD/BCD Claim and the duty of candour

110. The Claimants allege that MI5 breached its duty of candour to the Tribunal in the proceedings brought in 2015 by Privacy International in respect of handling arrangements for BPD/BCD ("the BPD/BCD Claim"). The basis of that contention is that MI5 failed to disclose to the Tribunal The manner in which BPD and BCD held in TE and TE2 Areas 1 and 2 had been handled, which was unlawful and and only disclosed to the Tribunal by letter to the President on 7 June 2019. The issue to be determined at this stage is whether there was unlawful handling of BPD/BCD. The question whether the BPD/BCD Claim should be re-opened will be dealt with subsequently.

111. This section addresses the factual questions whether BPD or BCD were actually held in TE or TE2 Areas 1 or 2, and, if so, whether the handling arrangements were not properly applied. These questions are also covered in the CLOSED judgment.

BPD

112. The Respondents' evidence is that no instances of BPD being held non-compliantly were identified within the TE and/or TE Area 1 and/or Area 2 until May 2019. A dataset held within TE2 Area 1 was wrongly identified as a BPD. On the basis of that evidence the Respondents assert that there was no unlawful use or retention of BPD within TE 2 Area 1. There were two BPDs held within TE2 Area 2 but only for training purposes. There were some minor instances of misapplication of BPD but those were not sufficiently serious to require any further consideration by the Tribunal.

BCD

113. The Respondents' evidence is that no BCD, obtained under section 94 directions, was ever held within TE or TE2 Areas 1 or 2. For the reasons given in the CLOSED judgment the Tribunal has accepted that there was a substantial failure in the use of BCD. That was an error which gave rise to the duty to make disclosure to the Tribunal in the BPD/BCD Claim, which MI5 failed to do.

114. The Tribunal will consider, following written submissions from the parties, whether the BPD/BCD Claim should be re-opened.

Submissions on the Issues of Law

Unlawfulness of warrants

115. References in this judgment to warrants shall be taken to include not only warrants issued under RIPA and IPA, but also directions and authorisations which were made under section 94 of the Telecommunications Action 1984 or section 5 and 7 of the Intelligence Services Act 1994.

116. The Claimants submit that the failure to meet statutory safeguards leads to the warrants granted being unlawful on three bases: mistake; failure to assess the applications properly and failure to conduct a proper enquiry. The Respondents accepts the unlawfulness of the warrants in cases where material might realistically have been held in the TE between 2016-2019, but no greater unlawfulness. There is therefore an issue both as to the time period in which warrants were granted unlawfully and the breadth of the class of unlawful warrants.

117. The Claimants firstly submit that warrants under RIPA and IPA were unlawful because the decision to make them by the SoS was based on a mistake as to an established and relevant fact, on the principles set out in *E v Secretary of State for the Home Department* [2004] EWCA Civ 49. The mistake in question being the apparent belief that the material gathered was being held in compliance with the statutory safeguards. The SoS therefore granted warrants in ignorance of relevant facts.

118. They refer to the statutory safeguards, set out above, and as one example the duty under section 138 IPA that the SoS must "consider" that satisfactory arrangements are in force for the purposes of section 150 and 151. Those purposes include that "arrangements are in force for securing", inter alia, the destruction of data when there are no relevant grounds for retaining it, see section 150(5).

119. In the *Generic Warrants Decision* at [14] the IPC said:

> *"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."*

120. The Respondents concede that RRD issues within the TE were a relevant matter for the SoS when determining warrant applications for material which might realistically be held within the TE. The SoS therefore needed to be aware of those problems when deciding whether to issue such warrants. On that basis the Respondents accept that warrants for such material were issued unlawfully prior to the IPC's *General Warrants Decision* of 5 April 2019 because the SoS had failed to take into account a mandatory relevant consideration.

121. Further, the Respondents submit that there will necessarily in a field as complex as this be questions of judgement and degree and not every error has to be included when assessing compliance risk. The role for the IPT is not to stand in the shoes of the primary decision maker, but only to interfere with the judgements of the decision maker if they are irrational.

122. Further, and closely related, the Claimants say secondly, that there was no adequate assessment by the SoS as to whether satisfactory arrangements were in force. The duty under section 150 IPA and its analogues is a mandatory one and as such the SoS's failure led to the unlawful grant of warrants.

123. The Claimants submit that the SoS was under a duty of enquiry pursuant to the principle in *Secretary of State for Education v Tameside MBC* [1977] AC 1014. In our view this covers the same issues as the submission on no adequate assessment. The Claimants accept that the obligation on the decision maker is only to take such steps to inform herself of the information necessary for her to make the relevant decision, and that judgement can only be challenged on a *Wednesbury* basis, see *R (Plantagenet Alliance) v Secretary of State for Justice* [2014] EWHC 1662 at [100]. However, unlike the factual position in *Plantagenet Alliance*, here there is a detailed statutory scheme in the IPA, particularly in section 53, as to what matters the SoS is obliged to consider and therefore what information the SoS needs to have.

124. The Respondents say that the *Tameside* duty is subject only to a rationality challenge. The SoS was entitled to rely on MI5's expertise and knowledge of the information and to assume that she was being given the relevant and correct information. She was therefore under no duty to take any further steps.

125. Our conclusion is that the SoS did breach the *Tameside* duty in not making adequate enquiries as to whether the statutory safeguards were or were not being met. Given the reports of

longstanding non-compliance risks, it was irrational of the SoS to fail to make enquiries as to the scale and nature of the non-compliance.

126. On the basis of the factual findings set out above, warrants were issued after late 2014 through to 5 April 2019 which were unlawful in that they did not meet the safeguarding requirements imposed under RIPA or IPA.

Full and frank disclosure

127. The Claimants submit that MI5 had a duty of full and frank disclosure in respect of each request made to the SoS for a warrant. MI5 breached that duty in applying for warrants without informing the SoS about the non-compliance issues. It must follow that the warrants were therefore granted unlawfully.

128. They rely upon the terms of the IPCR Note 1/2018 which states:

> *"31. 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 information which militates against the grant of the application, which includes material which weakens the case for the warrant, authorisation or notice. Where such material is identified by the applicant, it will be provided to both the Secretary of State and Judicial Commissioners in the application, where appropriate.*
>
> *1. In fulfilling their duty to provide information which militates against the granting of the decision, those seeking warrants can be expected to consider and, where necessary, explain in the application:*
>
> *...*
>
> *d. any other factor which materially weakens the case for the warrant, authorisation or notice of which they are aware.*
>
> *...*
>
> *34. Those requesting a warrant will confirm as part of the application that, in accordance with the applicable Codes of Practice, they have made all reasonable efforts to take account of information which may weaken the case for a warrant."*

129. The Claimants rely on the well-known principles on full disclosure relating to without notice applications for search warrants. In *R (Chatwani) v National Crime Agency* [2015] EWHC 1283, Davis LJ (in the Divisional Court) stated at [106(iv)]-[107]:

> *"106(iv). However, that is not the full extent of the applicant's duty. When applications are made without notice – particularly those that involve the potentially serious infringement of the liberty and rights of the subject, inherent in the grant and execution of a warrant to search and seize – there is a duty of candour. There must be a full and accurate disclosure to the court, including disclosure of anything that might militate against the grant (Energy Financing Team Limited v The Director of the Serious Fraud Office [2005] EWHC 1626 (Admin) ("Energy Financing"); see also, to the same effect, Golfrate at [27] per*

Lord Thomas). In Golfrate (at [24]), Lord Thomas quoted with approval from [191] of the judgment of Hughes LJ (as he then was) in In re Stanford International Bank Limited [2010] EWHC Civ 137 ("Stanford") (at [191]), a case concerning a restraint order in support of confiscation proceedings under section 42-47 of POCA, that full paragraph reading as follows:

"... [It] is essential that the duty of candour laid upon any applicant for an order without notice is fully understood and complied with. It is not limited to an obligation not to misrepresent. It consists in a duty to consider what any other interested person would, if present, wish to adduce by way of fact, or to say in answer to the application, and to place that material before the judge. That duty applies to an applicant for a restraint order under POCA in exactly the same way as to any other applicant for an order without notice..."

Those comments apply equally to the duty of an applicant for a search warrant. That obligation was described by the President in Tchenguiz (at [88]) as "a very heavy duty ... to ensure that what is put before the [court] is clear and comprehensive so that the [court] can rely on it and form [its] judgment on the basis of a presentation in which [it] has complete trust and confidence as to its accuracy and completeness". The duty extends to all known information that may be material to the court's decision, i.e. that might affect the court's decision. In a case involving complex financial matters, that presentation requires particular skill and experience (Tchenguiz at [88]). Legal advice should be sought at an appropriate level in every case of financial complexity (Golfrate at [28]).

...

107. As I have said, those principles – derived from the statutory scheme, and in particular reflecting the checks and balances which Parliament has incorporated in that scheme where without notice procedures for draconian measures are made – are well – and long-established. Every agency that applies without notice for search warrants, or other similar support from the court, should be aware of these principles; and have systems to ensure that they are respected in practice. The courts have, time and again, stressed the need for awareness of, and compliance with, these principles (e.g. Hughes LJ in Stanford at [191], quoted above). The Lord Chief Justice emphasised in Golfrate (at [28]) that, in respect of the nature and importance of an applicant's duties in such applications as these:

"If and to the extent that it is not well-known and understood by police officers seeking orders such as those sought in this case, it is time that the message was brought home clearly to applicants...".

130. In *R (Haralambous) v Crown Court at St Albans* [2018] UKSC 1, the Supreme Court when considering a challenge to a search warrant said at [34]:

"It is also relevant that the statutory procedure under section 8 is subject to a number of protections, expressed or inherent in the statutory language and in the current rules summarised in para 25 above. It only applies when a

magistrate is on reasonable grounds satisfied by a constable that an indictable offence has been committed. A constable, when seeking ex parte to satisfy the magistrate that the requirements of section 8 are met, owes a duty of candour, meaning that the 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: compare for example In re Stanford International Bank Ltd [2010] EWCA Civ 137; [2011] Ch 33, esp at paras 82-83 and 88, per Morritt C and para 191, per Hughes LJ".

131. Where the procedure for the grant of warrants is entirely without notice, and there is no subsequent opportunity for a court to scrutinise, then the Claimants submit that the duty of proactive disclosure is even stronger.

132. The Respondents submit that there is only a duty to disclose material of which "they are aware", see Practice Note paragraph 32(d). Further, it is for MI5 to make rational judgements about what information should be escalated to the SoS. MI5 did not have sufficient understanding of the nature, scale and scope of RRD failures such as would have made it clear they required disclosure until shortly before February 2019.

133. The Respondents do not accept that the principles set out in the caselaw relied upon by the Claimants, which relate to matters such as search warrants, apply in the present context.

134. We accept the Claimants submission that the principles set out in *Chatwani* apply in this context. Applications for warrants are made without notice to individuals affected by a warrant who may never be aware that their privacy rights have been interfered with. In those circumstances it is of particular importance that the person granting the warrant, namely the SoS, is given full information about any significant non-compliance issues.

135. It is for MI5 to make a rational judgement about what needs to be disclosed. We accept that not every record of a breach or potential breach of the statutory safeguards has to be reported to the SoS. However, where MI5 is aware of serious and longstanding issues of non-compliance with statutory safeguards, there is a duty to bring that to the attention of the SoS when seeking a warrant.

Human Rights Act 1998

136. The Claimants make two claims under the Human Rights Act 1998 ("HRA"). That there has been a breach of their Article 6 and Article 8 rights by the failure to act "in accordance with law"; and a systemic challenge to the scheme under IPA and RIPA, being in breach of Articles 8 and 10.

137. The Respondents had conceded the Claimants had standing in relation to bulk data but disputed that they had standing in respect of targeted data. However, during the course of the hearing they accepted that the IPT should not dismiss the ECHR claims on the grounds of standing.

Individual breach under Articles 6 and 8

138. The Claimants submit that interferences under Article 8 were not "in accordance with the law", as required by Article 8(2). The Respondents accept that to the extent that warrants were unlawful under domestic public law, they were not in accordance with law under Article 8. They repeat the same arguments under Article 6 in respect of legal privilege.

139. The Respondents concede that the warrants between 2016-2019 were granted unlawfully and as such do not meet the "in accordance with law" requirement. As such, they concede breach of the HRA in this respect. They do not make a concession in respect of Article 6.

140. We do not consider it necessary to determine a separate Article 6 challenge given that it adds nothing to the conceded breach of Article 8.

Challenge to the effectiveness of the IPA

141. The Claimants submit that the failure of the statutory safeguards, as shown on the facts of this case, establish that there was a systemic failure which rendered the statutory regime (both in RIPA and IPA) incompatible with Articles 8 and 10 ECHR. The Respondents say this is an attempt to re-run the case that was rejected by the Divisional Court in the *Liberty JR*.

142. The Claimants submit that the unlawful conduct by MI5 in the handling of data persisted for years without the statutory safeguards operating effectively. The system was reliant on MI5's own assessment of its systems and its own self-reporting without any meaningful independent oversight. As a result, MI5 was able to conceal systemic deficiencies from the Commissioners and then the IPC and IPT, thus revealing the limitation of the system of oversight.

143. The problems were systemic because the systems to hold and process data were designed without RRD built in. The oversight in the statutory schemes was not effective, in large part because it was wholly reliant on the oversight bodies being informed by MI5 of problems. There was a culture within MI5 not to notify, and to consider whether "risks" of non-compliance should be accepted rather than acknowledging the long-standing and continuing breaches of the relevant duties.

144. The Claimants rely on *R (P) v Secretary of State for Justice* [2019] UKSC 3 at [24] in respect of the need for safeguards as part of the requirement for legal foreseeability. The importance of considering whether the safeguards are respected in the "actual operation" of a secret surveillance regime was set out by the European Court of Human Rights ("ECtHR") in *Zakharov v Russia* [2016] 63 EHRR 17 at [284]. At [232] the Court said the safeguards had to be *"adequate and effective"*.

145. In *Big Brother Watch v United Kingdom* (2022) 74 EHRR 17 at [349], [350] and [356], the ECtHR Grand Chamber considered compliance of the legal framework in RIPA for bulk interception and the necessary requirements to meet the terms of the ECHR.

146. The Respondents submit that effectively identical arguments have been considered and dismissed by the Divisional Court in the *Liberty JR*. In those proceedings the Defendants disclosed information to the Court about the notification to the IPC in 2019 of non-compliance in TE and Areas 1 and 2 of TE2. They submit that there is nothing in any new material disclosed in this litigation that could reasonably have led the Divisional Court to a different conclusion.

The Court proceeded on assumed facts that were, if anything, more favourable to the Claimants than the facts now disclosed. Further, the facts show that the IPC is an effective regulator with the power and ability to address issues that arise. As soon as it was notified of the issues with TE in 2019, the IPC moved swiftly and effectively to address them.

147. The Claimants submit that the factual position is now much more serious than was the case before the Divisional Court. The Divisional Court did not have access to any CLOSED material which is now before this Tribunal, and had a much more limited amount of the OPEN evidence. They did not have the material concerning Sir Anthony May's consideration in 2013; and they did not have the material from MI5 on the positive decision not to report non-compliance to the SoS. Further, they did not have the material post-dating 2019, with more recent error reports from 2022.

148. We do not consider that the relevant evidence gives rise to any valid challenge to the effectiveness of IPA. Nor is there reasonable ground to question the issues determined in the *Liberty JR*. That case considered the compatibility of the IPA on the grounds of insufficient safeguards. We agree with the Respondents that the evidence before the Tribunal does not suggest that any different decision would now be made.

149. The evidence does suggest that there was a significant period under the previous statutory scheme of RIPA where the full extent of the issues of non-compliance was not properly considered, as is set out in the findings of fact above. However, this was not by reason of the fundamental features of the statutory scheme, but rather MI5's failure to act in accordance with their legal duties.

150. Implicit in the Claimants' argument is the assertion that the safeguards were not "adequate and effective" due to the failings of the IPC to detect serious and systemic compliance failures which had not been disclosed by MI5 before 27 February 2019. The robust steps taken by the IPC once his office had been alerted to the seriousness of the issues and investigations had been carried out, demonstrates the effectiveness of the safeguards regime and the adequacy of the measures available to IPCO. There is no substance in the Claimant's assertion that the systemic failings, which MI5 had failed to report or correct in accordance with its statutory duties, demonstrate that the legal regime was not in accordance with the law.

EU Law

151. The Claimants say that EU law is engaged because the compulsory acquisition of bulk communications data falls within Article 15(1) of Directive 2002/58/EC ("the ePrivacy Directive") as per C-623 *Privacy International*, and falls within the Charter of Fundamental Rights ("CFR"). The proceedings were commenced before 31 December 2020 and therefore section 5(4) of the European Union (Withdrawal) Act 2018 does not apply.

152. The only relevance of the EU law issues is that if a breach is found, then there is a right to a remedy. The Respondents submit that the EU law arguments add nothing to the domestic arguments because the substantive issues raised are precisely the same.

153. Article 47 of the CFR provides for an "effective remedy" where rights and freedoms guaranteed by EU law are violated. Articles 52(1) and (3) equate those rights to those in the ECHR.

154. The Claimants submit that the test for an effective remedy in EU law is whether it (i) provides real and effective protection of any EU law right that has been violated; (ii) may be effectively invoked before the national courts, and (iii) has the effect of preventing the continuation of the alleged violation and provides adequate redress for its continuation. These principles are based on *Van Colson v Land Nordheim Westfalen* (Case 14/83). In *Kudla v Poland* (2002) 35 EHRR 11 at [158] an "effective remedy" was said to be one that will either prevent the alleged violation or its continuation, or provide adequate redress for any violation that has already occurred.

155. The Claimants refer to the ordinary remedy for unlawfulness of a warrant being quashing, see *R (Van der Pijl) v Kingston Crown Court* [2013] 1 WLR 2706 at [66]-[68]. In *Belhaj v Security Service* [2015] UKIP Trib 13, where information had been obtained unlawfully or continued to be retained, the Tribunal required that the information be destroyed.

156. The Claimants submit that any unlawfulness must as a minimum be marked by declaratory relief, relying on *R (ClientEarth) v Secretary of State for the Environment, Food and Rural Affairs* [2013] UKSC 25.

157. We accept the Respondents' submissions that the effectiveness of remedy is a context and fact specific issue. The caselaw that the Claimants rely upon does not support any unconditional right to a particular remedy. Both *Van der Pijl* and *Belhaj* involved situations where the continued existence of the warrant and the holding of the data potentially caused continuing prejudice to individuals concerned. For the reasons that are explained in this judgment, that is not the position in the present case. Therefore, those cases do not support a requirement for an order to destroy the data held, nor that that the warrants themselves are required to be quashed for the purposes of achieving an effective remedy.

158. Equally, on the facts of *ClientEarth*, there was clear evidence of an ongoing breach, which required legally enforceable orders in order to provide an effective remedy to ensure compliance with EU law in the future. The factual situation here is entirely different. Critically in the present case, the evidence shows that the IPC is working effectively to minimise the risk of future breaches.

159. For these reasons, we do not consider that EU law adds to or changes our analysis of the appropriate remedies in this case.

Conclusions

160. On the evidence, the Tribunal finds:

(1) There were serious failings in compliance with the statutory obligations of MI5 from late 2014 onwards. The holding and handling of data in those circumstances was unlawful on the basis that under the relevant provisions of RIPA and IPA satisfactory safeguards relating to RRD were not in place. MI5 accepts that it was in breach of the safeguarding obligations at least

from 2016 and that it was under a duty to have notified the IPC of compliance failings from 2018.

(2) Adequate enquiries were not made by the Home Office as to the longstanding compliance risks which had been reported on several occasions from December 2016. No explanation was sought or offered or reported to the Home Secretary as to the scale and seriousness of the risk to the handling arrangements required by RIPA and IPA, nor any advice as to the effect of that risk on the power of the Home Secretary to authorise warrants. In those circumstances the Secretary of State did not have grounds to be satisfied that effective safeguards applied to warrants where there had been no assessment or effective investigation into compliance with RRD.

(3) The Claimants raise an issue whether the MI5 failings in compliance extended beyond the TE to Areas 1 and 2 of TE2, and beyond RRD to other safeguards required by statute, including access controls, data copying and protection of Legal Professional Privilege. This issue will be considered in the CLOSED judgment.

(4) There was a breach in the duty of candour in the conduct of the BPD/BCD Claim in failing to disclose use made of BCD.

The scope of the "similar fact" claim in respect of systemic failings

161. In the Claimants' skeleton argument at paragraphs [149]-[150] it is submitted that the pleaded "similar fact" claim extends to all systemic defects in MI5's holding of data and that such "similar fact" failings are relevant. It is submitted that the Tribunal should direct the Respondents to make further disclosure of systemic failings, to be followed by directions as to how any further issues are to be determined.

162. At paragraph 154 of the Amended Grounds of Claim it is pleaded that the "new claim", which is undefined, should be managed with the existing BPD/BCD claim. From the solicitor correspondence, in particular the letter dated 25 March 2022, the Claimants' argument is that the new claim extends to:

"any failure by MI5 to have adequate safeguards ... from at latest 2010, whether or not the failure had been identified in the notification to the IPCr, whether or not it relates to TE or TE2".

The basis for requiring further disclosure is put as follows:

"It is clear that all similar fact breaches are required to be disclosed for candour reasons as they amount to systemic failures. Proper compliance with the duty of candour in these proceedings requires disclosure of non-compliance beyond TE and Areas 1 and 2 of TE2, not least because each and every further material failing of safeguards that went unreported to either the Home Secretary or IPCO (or its predecessors) is further proof to the Claimants' allegation that the IPA

and RIPA safeguards were failing systematically, or were "paper restraints" with little practical impact or controlling effect".

163. The response of the Respondents in their skeleton argument is that at the directions hearing in April 2022 it was accepted by the Claimants that the scope of the issue relating to systemic failings did not extend beyond BPD and BCD. The Respondents state that they are willing to give further disclosure in relation only to MI5's holding of BPD and BCD data.

164. It is relevant first to consider the steps that were taken by the Home Office after April 2019 to ensure that there was an independent and thorough inquiry into compliance failings in MI5. The steps taken were:

(1) On 9 May 2019 the Home Secretary informed Parliament that he had established the independent review to be conducted by Sir Martin Donnelly who would have access to all relevant documents in relation to compliance risks within certain technology environments used to store and analyse data.

(2) The terms of reference of the CIR were wide ranging, to review compliance risk management and reporting of the TE issue, including the legal requirements of safeguards related to warranted data.

(3) The CIR involved a comprehensive review of events and 16 key findings. Sir Martin interviewed a number of officials of MI5. As noted above, the CIR identified the first major compliance issue as arising in 2014.

(4) On 1 February 2021 the Compliance Improvement Review, verified by Mary Calam, was completed. That report covered completion of the 14 Donnelly Recommendations and was also wide ranging in its ambit and general in its requirements. For example, at page 30 MI5 was to ensure that all its data was to be held in accordance with legal compliance requirements by June 2020. In the event, the work was not complete by December 2020 but MI5 was able to state that it had a high degree of confidence that a high number of the higher risk systems would be fully compliant by a certain date. It is relevant to note the terms in which the author expressed her views as to the changes which had taken place in the compliance with the IPA by MI5:

"While there is more to be done, the broader changes that MI5 has made to strengthen its legal compliance risk management processes, instill 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."

That judgment by Mary Calam does not support the Claimants' case that there might be continuing systemic compliance failures after 2019 which were not capable of being addressed by MI5 and reviewed by the IPC.

165. It is clear that after 2019 MI5 had understood the requirements of IPCO and had agreed the basis on which error reports would be made. From 2020 there were a number of error reports made by MI5 to IPCO. On 8 November 2021 and 23 June 2022 IPCO issued inspection reports on the IPA safeguards. The error reports by MI5 and the inspection reports from IPCO do not provide any evidence of systemic failings after 2019 in relation to the handling of data held by MI5. If there were any substantial and continuing systemic errors, these are matters for consideration by IPCO. It is the Commissioner who has powers under IPA to keep under review by way of audit, inspection and investigation of, in particular, privacy safeguards. In this context the inspection reports of IPCO and the annual published reports are an important element of the oversight conducted by the IPC.

166. The question then is whether there were undiscovered systemic failings between 2010 and 2019 which had not been disclosed to the IOCC or IPCO. Given the seriousness of the CIR it seems wholly improbable that if there were indeed concealed systemic errors which had facts similar to any of the compliance failings considered in this case, then those similar facts would not have been brought to the attention of Sir Martin Donnelly or the relevant Commissioners.

167. The letter dated 25 March 2022 from the Claimants' solicitors makes clear the width of the disclosure sought as extending to:

> *"other "similar fact" failings, in TE and Areas 1 and 2 of TE2 and across MI5's systems, including RRD, access, copying or LPP breaches or other breaches of obligations which materially bear on the adequacy of the systemic IPA and RIPA safeguards (e.g. breaches of MI5's own sharing rules or "action on" principles) that are fully documented and which have either been reported to IPCO (or its predecessors) or considered for such".*

This would require a very extensive disclosure exercise, on a speculative basis.

168. In the absence of any evidence of systemic failings beyond those which were investigated by IPCO between March and October 2019, and an absence of any evidence that IPCO might have omitted to deal properly with any serious systemic failings, there are no grounds for requiring MI5 to make further disclosure of documents in relation to the "similar fact" claim. It is noted that the Respondents did, at the directions hearing in April 2022, state that they were under an obligation to give disclosure relating only to MI5's holding of BPDs or BCD. In light of the reasons for its decision in CLOSED in relation to the duty of candour in the IPT BPD/BCD Claim, the Tribunal does not consider that any further disclosure by MI5 is required.

<u>Relief - the section 31 (2A) issue</u>

169. There is an issue in relation to what relief, if any, the Tribunal should order. The Respondents submit that relief should be refused based on section 31(2A) of the Senior Courts Act 1981. The Claimants submit that section 31(2A) does not apply to the IPT; and in any event its terms would not be met on the facts of the present case.

170. Section 31(2A) states:

> ***"31 (2A) Application for judicial review.***
>
> *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".*

171. Section 67(2) and (3) of RIPA provides:

> ***"67. Exercise of the Tribunal's jurisdiction.***
>
> *(2) Where the Tribunal hear any proceedings by virtue of section 62(2)(a), they 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.*
> *(3) Where the Tribunal consider a complaint made to them by virtue of section 65(2)(b), it shall be the duty of the Tribunal –*
> *(a) to investigate whether the persons against whom any allegations are made in the complaint have engaged in relation to –*
> *(i) the complainant,*
> *(ii) any of his property,*
> *(iii) any communications sent by or to him, or intended for him, or*
> *(iv) his use of any postal service, telecommunications service or telecommunications system, in any conduct falling within section 65(5);*
> *(b) to investigate the authority (if any) for any conduct falling within section 65(5) which they find has been so engaged in; and*
> *(c) in relation to the Tribunal's findings from their investigations, to determine the complaint by applying the same principles as would be applied by a court on an application for judicial review."*

172. There is no authority that deals with the application of section 31(2A) to the IPT. However, there are a number of decisions in other Tribunals under similar but slightly different statutory provisions. In *MB v SSHD* SI No 47/2015 in the Special Immigration Appeals Commission ("SIAC"), Mitting J together with UTJ Rintoul and Roger Golland, held that section 31(2A) did apply to SIAC. His reasoning is at [25]:

> *"Miss Knight submits that SIAC is not the High Court. Her submission is obviously correct; but it does not follow that s31(2A) has no application to applications of this kind determined by SIAC. SIAC is obliged by s2D(3) of the SIAC Act 1997 to,*
>
> *"apply the principles which would be applied in judicial review proceedings."*
>
> *S31(2A) sets out a principle which the High Court must apply in judicial review proceedings, not just a practice which it may or should follow. When it appears*

to the High Court to be highly likely that the outcome for an applicant would not have been substantially different it must refuse to grant relief. Parliament is free to establish or alter rules of principle to be applied by the High Court in judicial review proceedings. Now that it has done so, the requirements in s31(2A) is a principle which must be applied by the High Court in judicial review proceedings. SIAC is required by s2D(3) of the SIAC Act 1997 to apply the same principle."

173. In the Proscribed Organisations Appeal Commission ("POAC") in *Arumugan & ors* [PC/04/2019] the Commission (Elisabeth Laing J, Richard Whittam QC and Philip Nelson CMG) held at [100] that considering the relevant statutory provision for relief under section 5(4) of the Terrorism Act 2000, section 31(2A) did not apply to the Commission.

174. POAC relied on the decision of SIAC in *LA & ors v SSHD* [2018] UKSIAC 1, in which SIAC held that section 31(2A) did not apply to SIAC, relying on the obiter reasons given by Singh LJ in *MWH v SSHD* (SI No 57/2015). The reasons are set out at [60]-[64] as follows:

"60. 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 do expressly. We note that is precisely what Parliament has done in the case of the Upper Tribunal when it considers an application for judicial review.

61. Section 84(1) of the 2015 Act amended the Senior Courts Act 1982, as we have noted earlier. The very same section, in subsections (4) and (5), amended sections 15 and 16 of the Tribunals, Courts and Enforcement Act 2007 so as to introduce similar provisions in that context as were being introduced in the context of the High Court. For example, there was introduced a new section 15(5A), which provides:

"... subsections (2A) and (2B0 of section 31 of the Senior Courts Act 1981 apply to the Upper Tribunal when deciding whether to grant relief under subsection (1) above as they apply to the High Court when deciding whether to grant relief on an application for judicial review."

62. The fact that there has not been any similar amendment to the 1997 Act, which created this Commission and confers jurisdiction upon it, is telling.

63. 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.

64. 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 and (where the statutory criteria are met) imposes a duty to refuse a remedy, unless the "escape clause" in subsection (2B) is available, for reasons of exceptional public interest."

175. In *Meta Platforms v CMA* [2022] CAT 26 (14 June 2022) the Competition Appeal Tribunal ("CAT") (Marcus Smith J, Professor John Cubbin and Simon Jones) held that section 31(2A) did not apply to the CAT. Their reasoning was set out at [167]-[171]:

"(2) Application of section 31(2A) of the Senior Courts Act 1981

167. As Fordham notes, a judicial review claim may fail at common law if lacking in substance, as where it is non-material, non-prejudicial, futile, academic or premature. The common law rules regarding materiality have been augmented by section 31(2A) of the Senior Courts Act 31(2A) which provides:

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".

168. We say nothing about the difference between the common law and statutory tests as regards remedy, and nothing about whether such difference would or would not be determinative in the present case. We are simply seeking to determine whether this provision applies in the case of this application. We do, however, proceed on the basis – for the purposes of the question of statutory interpretation that arises - that section 31(2A), which was inserted into the Senior Courts Act 1981 by the Criminal Justice and Courts Act 2015, was intended to make a material change in the law.

169. Section 120(4) of the Enterprise Act 2002 provides that in determining applications such as the present, "the Competition Appeals Tribunal shall apply the same principles as would be applied by a court an application for judicial review". The question is whether this wording causes section 31(2A) of the Senior Courts Act 1981 to apply. In their written submissions to us, the CMA contended that section 31(2A) did apply, whereas Meta contended that it did not.

170. As to this:

(1) Both Meta and the CMA were agreed that this was an open question, and that although similar points had arisen in proceedings before other tribunals, there was no decision binding on this Tribunal.

(2) More to the point, such discussions and determination as there had been before other tribunals in relation to analogous, but not identical, provisions to section 120(4) of the Enterprise Act 2002 do not speak with a single voice. Thus, in MB v Secretary of State for the Home Department, Mitting J considered that section 31(2A) did apply to proceedings before the Special Immigration Appeals Commission ("SIAC"). Contrary views were expressed in MWH v Secretary of State for the Home Department and LA v Secretary of State for the Home Department. In both of these latter cases, the tribunal

noted that in other cases (e.g., in the case of the Upper Tribunal) express legislative changes had been made to render section 31(2A) of the Senior Courts Act 1981 applicable. The CMA helpfully referred us to dicta in three Court of Appeal decisions, but these, too, relate to different statutory provisions and also point in different directions. The most that we derive from the case law is that it is significant that in some cases Parliament has expressly extended the ambit of section 31(2A) to non-High Court proceedings, which we take as an indicator (but no more than that) that section 31(2A) does not apply without some explicit legislative indicator. But we do not consider this point to be of great moment: at the end of the day, this is a question of statutory construction.

(3) We conclude that section 31(2A) of the Senior Courts Act 1981 does not apply to the determination of applications such as this pursuant to section 120(4) of the Enterprise Act 2002:

(i) the schema of section 120 of the Enterprise Act 2002 draws a distinction between (a) principles applied on an application for judicial review, and (b) remedies where a claim for judicial review has succeeded:

(4) In determining such an application the Competition Appeal Tribunal shall apply the same principles as would be applied by a court on an application for judicial review.

(5) The Competition Appeal Tribunal may –

(a) dismiss the application or quash the whole or part of the decision to which it relates; and

(b) where it quashes the whole or part of that decision, refer the matter back to the original decision maker with a direction to reconsider and make a new decision in accordance with the ruling of the Competition Appeal Tribunal".

If remedies on a successful judicial review were to be determined strictly according to "the ... principles as would be applied by a court on an application for judicial review", section 120(5) would be redundant. The presence of an express discretion regarding remedy ("may") strongly suggests a discretion informed by the jurisprudence of the United Kingdom, but which is the Tribunal's own.

(ii) That is consistent with the fact that the Tribunal is a Tribunal of the United Kingdom. We accept, of course, that in all cases proceedings before it, the Tribunal is required to determine whether the proceedings or any part of them are to be treated as proceedings in England and Wales, in Scotland or in Northern Ireland. In this case, as we have noted, the Tribunal has ordered that these proceedings are to be treated as proceedings in England and Wales. But the significant lessening of competition

> *that we have been considering has been in markets in 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 remedies are different in one jurisdiction rather than another.*
>
> *171. For these reasons, we hold that section 31(2A) of the Senior Courts Act 1981 does not apply in this case. We say nothing about the question of remission of otherwise: that, as it seems to us, is a matter on which we will need to hear submissions at a later date."*

176. The Respondents rely on the difference in statutory wording in respect of SIAC and POAC to that in the RIPA, where they submit the language is wider in referring to determination of "the claim" or "the complaint" generally.

177. They submit that the Parliamentary intent was to alter the common law principle set out in *Simplex* because it was considered to be too broad. There is no reason why Parliament would have intended to exclude the IPT from that legislative change. The Tribunal does not need to imply words into RIPA, it should simply apply the words *"the same principles"* with the obvious Parliamentary purpose in mind.

178. Parliament amended the 2007 Act in respect of the Upper Tribunal to expressly apply section 31(2A) simply for the avoidance of doubt, not to create a distinction between the Upper Tribunal's powers and those of the IPT (or other tribunals). Further, Scottish and English principles of judicial review can be different, so the analysis in *Meta Platforms* does not follow.

179. Firstly, the language of section 120(4) of the Enterprise Act 2002 is very similar to that in section 67 of IPA. The same distinction exists in section 67 RIPA as in section 20 Enterprise Act 2002. In particular, the reference to the same principles being applied as in judicial review is in the section dealing with the Tribunal's findings, rather than in the section dealing with relief. This is the point made by Marcus Smith J at paragraph 170(3)(i). Secondly, if it had been Parliament's intention to restrict the scope of relief by applying section 31(2A) then they could have been expected to have done so expressly, as they did in the UTIAC.

180. Thirdly, the IPT has jurisdiction across the whole of the United Kingdom but section 31(2A) does not apply in Scotland. The IPT should apply consistent principles of law, save where there are clear statutory differences. The public law principles set out in section 67(2) IPA should apply to the entirety of the IPT's jurisdiction.

181. Further, and in any event, the Claimants submit that even if section 31(2A) applies in principle, it would have no application on the facts of the present case. Section 31(2A) requires that it is highly likely that the same decision would have been made at the time, not whether the warrants would be granted now. Therefore, the Court should not take

into account all the changes and mitigations that have taken place since the unlawful decisions that were made, but rather consider the matter in the light of the position at the time. Further the *Generic Warrants Decision* makes it clear that Sir Adrian Fulford would not have accepted the resumption of the grant of warrants without the changes that were made immediately after that Decision.

182. The Respondents submit that it is not contended by the Claimants that it was unnecessary or disproportionate to obtain any of the data in the first place. The vice relied upon is the retention of that data for too long and the failure to ensure that it was deleted at an appropriate point. It is therefore inconceivable that the SoS would have refused the warrants where it was necessary and proportionate for MI5 to collect the data for the purposes of national security. The Respondents submit that it is highly likely that warrants would have been issued, but with further conditions attached.

183. We do not refuse relief under section 31(2A), in respect of the unlawful authorisations which were granted and implemented because:

(a) In our judgement, that provision does not apply to the Investigatory Powers Tribunal for the reasons given by Marcus Smith J in *Meta Platforms* referred to above, and, in particular, because the IPT is given statutory jurisdiction over the whole of the United Kingdom. This creates obvious difficulties in the application of section 31(2A) which does not apply in Scotland. A system of law in which a Scottish claimant recovered a remedy which was denied to an English claimant in an otherwise identical case has nothing to commend it. RIPA section 67(2) should be construed so that the Tribunal is required to *"apply the same principles for making their determination in those proceedings as would be applied by a court on an application for judicial review"* in so far as those principles are common law as between all parts of the United Kingdom.

(b) It is, in any event, simply impossible in a case like this for the Tribunal to be satisfied that *"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"*. The conduct complained of was the failure to give proper disclosure to the Secretary of State when making applications for authorisations as from October 2014, and the failure of the Secretary of State at a point after that to make proper enquiries when on notice that these were necessary. Had those failures not occurred, matters would have developed in an entirely different way. Some authorisations may have been refused in the course of that process and it is likely that by some point long before early 2019 the applications would have been made and dealt with on a proper basis. It is simply impossible to construct the necessary counterfactual narrative which section 31(2A) requires in order to trigger the statutory duty to refuse to grant relief

184. We accept the Claimants' submissions on this point. We are not satisfied that if proper disclosure had been given to the SoS by MI5, and/or proper inquiry carried out, the result would have been the same in terms of granting of all of the warrants. Such a conclusion would involve a high degree of counter factual deduction, concerning a process of decisions across many years. We do not think it is safe to assume that the decisions would have been the same.

Relief - discretionary

185. The Claimants submit that to fail to grant relief would be to undermine the oversight role of the IPT. The ECtHR in *Big Brother Watch* at [413]-[415] has relied upon the effectiveness of the IPT as a safeguard. Such safeguard would be jeopardised if the IPT was unable, or failed, to grant a remedy in a case of unlawful activity of this magnitude.

186. In terms of appropriate relief, the Claimants argue firstly for declaratory relief as to the unlawfulness of the warrants. Secondly, that all warrants, authorisations and directions that were unlawfully obtained should be quashed. Thirdly, that all data that has been unlawfully obtained should be destroyed.

187. The Respondents submit that if any relief is to be granted, it should be a declaration, not the quashing of the warrants or the destruction of the data still held. The information from the warrants has already been obtained and processed, so quashing the warrants serves no useful purpose.

188. For the reasons given in the CLOSED judgment the Tribunal is satisfied that any order made which had the effect of

(a) quashing warrants, authorisations, or directions which had been issued by the Secretary of State, or

(b) directing that MI5 should destroy all data which had been unlawfully retained,

would be very damaging to national security.

189. It would be very difficult to carry out an extensive search of warrants issued over a period of several years, which would require detailed analysis of all types of data which had subsequently been obtained under the relevant warrants. In view of this, it would be impractical effectively and reliably to identify which warrants had been unlawfully issued and to what extent. Carrying out such an exercise would serve no useful purpose, but would have a deleterious effect on the efficiency of MI5. Any such order would be extraordinarily difficult, if not impossible, to implement following the principles set out by Green J in *Business Energy* paragraph [97].

190. Essentially for the reasons given by the Respondents, we do not consider it is appropriate to grant a quashing order. Relief is discretionary in public law. The information held by the Respondents was properly thought to be obtainable, and the RRD failures do not undermine that consideration.

191. The events of 2019 onwards show the effectiveness of IPCO and the current statutory regime. We do not consider that a quashing order is necessary to deal with any matters hereafter. The IPC has sufficient powers to regulate the safeguards required under IPA in the future and to ensure that there is no repetition of the serious and wide ranging compliance failures.

192. The grant of relief in judicial review proceedings is discretionary. Further, the duty in EU law to grant an effective remedy is addressed to a substantial extent towards ensuring that individual rights are vindicated and future compliance enforced. In our judgement, it is possible to grant an effective remedy without quashing the authorisations and ordering

the destruction of the material which resulted from them. Further, and in any event, we refuse to make those orders as a matter of the exercise of the discretion vested in the court when determining an application for judicial review. The factors which we have weighed in the balance when reaching this conclusion are:

(a) The failure which lies at the root of the unlawfulness we have identified is the failure to have and to apply a proper system for review retention and deletion of material. It was not a failure which means that MI5 should never have had the material at all. It is a failure which means that a small proportion of the material was retained for longer than it should have been. To hold that all of the product of all of the warrants should be destroyed would be disproportionate to the unlawfulness which we have found. This does not minimise the seriousness of that unlawfulness, which should be obvious to all readers of this judgment.

(b) There is no evidence that any individual has suffered any harm as a result of that unlawfulness. That being so, compensation as a means of remedying harm is not required. The Claimants have brought these proceedings as a matter of public service and have, by doing so, secured the findings we have made above. It does not follow from that that any compensation should be awarded to anyone.

(c) The material has been processed over a number of years from time to time and has generated product which is of continuing value to national security. We accept that the orders which we decline to make would be very damaging to national security. We have dealt with this further in the CLOSED judgment. Although the Claimants submit that this factor is irrelevant, we do not agree.

(d) A remedy has already been supplied which is effective. After the disclosure made to IPC in February 2019, vigorous action by IPCO has resulted in a full understanding of what went wrong. We are satisfied that the role of IPC in the modern regulatory system has been shown to be an effective remedy by the history which we have set out above.

193. This judgment itself is part of the remedy. We have made findings of serious failures by MI5 and also by the Secretary of State. These findings have been set out in a public document by the Tribunal. Both the IPC and the IPT will have continuing oversight of the conduct of MI5 and the Secretary of State in the future and will exercise that oversight expecting the Respondents to have learnt the lessons of this damaging series of events.

194. We do not consider that it is appropriate or necessary to single out any individual at MI5 or the Home Office for any blame. There was a widespread corporate failure, as recorded in our findings of fact above. It would be unfair to single out individuals who have been identified in these proceedings.

195. By RIPA section 68(5) we are required to make a report of our findings to the Prime Minister, which we will do. This is a statutory mechanism designed to ensure that the Executive has in place proper procedures for dealing with applications for authorisations in cases where that is found not to have been the case in the past. It is designed to secure better ministerial conduct in the future, which is a matter for the Prime Minister.

196. The relevant appellate court in this case is the Court of Appeal in England and Wales.