Applications for approval of warrants by the Home Office

[REDACTED]

Fulford LJ

5 April 2019

Decision: the [TE] and Compliance

The Facts

1. I have based this introductory section to a significant extent on the narrative to be found in the IPCO inspection report entitled "MI5 (Audit of [TE]) Version 2, issued 29 March 2019".

2. [*MI5 uses different technology environments. One of these technology environments will be referred to as "the Technology Environment, or TE". This TE holds operational data*].

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

4. An Executive Board paper on [*the TE*] compliance risks in October 2018 set out many of these problems in greater detail. It included a stark assessment of the compliance risks:

001

> "MI5 is unable to provide robust assurances to its oversight bodies [*REDACTED*]. The risk is that the IPC may be unwilling to authorise further warrants until this is rectified, especially for [*one category of]* data.
>
> [...]
>
> Effective RRD has not been implemented across all data stores in the [*TE*], potentially including warranted material... [this could] lead to successful IPT challenges, loss of confidence of ministers/JCs and consequently restrictions in warrants or reputational damage."

5. The paper envisaged that MI5 would communicate these risks to the IPC:

> "we anticipate that MI5 will want to pre-emptively brief oversight bodies on these challenges and our plans to address them".

6. However, liaison with the IPC did not appear in the list of actions. By section 235(6) IPA, MI5 is required to report any relevant error of which it is aware to the IPC. It seems to me that to have provided assurances to the Secretary of State regarding safeguarding warranted data that, in hindsight, did not comply with MI5's obligations under the various safeguarding sections amounts to an error of notable gravity. As soon as MI5 became aware of this, it should have reported the matter and explained what it intended to do by way of rectification. In short, MI5 did not have the option of seeking privately to devise a strategy before reporting the matter. Moreover, it is impossible sensibly to reconcile the explanation of the handling arrangements the Judicial Commissioners were given in briefings and the JC Handbook with what MI5 knew over a protracted period of time was happening.

7. On 21 February 2019, the IPC received a letter from [*the Director of Policy and Information*] at MI5, in advance of a meeting that was due to take place on 27 February 2019, organised by MI5, the purpose of which was simply described as relating to historic compliance challenges. In the letter it was suggested that the meeting on 27 February was envisaged as being "a discussion as the next step in briefing you more broadly on our approach to data. There will be future opportunities for our technical experts to discuss the detail but we consider an initial overview briefing to you is the right place to start. I look forward to discussing these issues in more detail with you on the 27th". Otherwise, the author principally stressed the importance to MI5 of the [*TE*], whilst simultaneously making veiled reference to potential problems. As to the latter, first:

> "We would now like to explain more about the architecture on which many of [the] systems sit; to provide a clear sense of how that architecture is sited in a context of [*an overall IT estate]*; and to give an appraisal of the some of the more specific legal compliance and [*other*] challenges we have discovered and are working to address."

Second:

> "The [*TE has been and will continue to be important to the delivery of our national security mission*] [*REDACTED*] presents some challenges in maintaining assurance in terms of legal compliance and [*REDACTED*]."

8. Thereafter, [*Director of Policy and Information*] made reference to unspecified compliance challenges.

9. On 27 February 2019, MI5 briefed me and Sir John Goldring, along with other representatives of IPCO, for the first time about – to use the agency's somewhat misleading euphemism – the extensive "compliance difficulties" which had been identified within the [*TE*], the existence, scale and duration of which were entirely unheralded.

10. By way of summary, the key compliance risks highlighted in MI5's briefing were that MI5 has inadequate control over where data is stored; [*R E D A C T E D*] ; and the deletion processes which applied to it. Two specific aspects of the [*TE*] exemplify the undoubted unlawful manner in which data has been held and handled. First, **file shares**: files within [*TE*] can be written to file shares, either in an automated way as data flows between systems within [*TE*], or manually by an analyst [*REDACTED*]. Second, **data stores**: data stores are used to store [*d a t a*] required by applications in [*TE*]. MI5 "have, or will have, automatic RRD process[es] for our main Data Stores although the RRD rules vary according to the [*n a t u r e*] of that data or, in some cases, are system specific. Some [Data] Stores and other areas may not have an RRD process." This was specifically referenced in the [*d a t a s t o r e*] error letter dated 4 March 2019, in relation to [*p r o d u c t*] that was retained beyond the [*p e r i o d o f t i m e*] set out in the RRD policy.

11. At the end of the meeting on 27 February 2019, I requested that the briefing which we had been provided should be reduced to writing (the only written materials were a "slide pack", which was collected before we left). It was impossible to make a full note of the complicated account set out by MI5 during the briefing. The prose description of the matters raised on 27 February 2019 was received on 11 March 2019, and it contained a full and clear description of all the matters that had been discussed.

12. I immediately ordered an inspection of [*TE*], and between 18 and 22 March 2019 a number of inspectors visited [*REDACTED*] for this purpose, focussing on the extent to which [*TE*] complies with the relevant IPA safeguards for warranted data. Additionally, I asked the inspectors to consider the extent of MI5's institutional knowledge of the issues, given the statement in MI5's letter that compliance risks in [*TE*] had been identified as early as January 2016. The report, as set out above, is dated 29 March 2019. The key findings are as follows:

[REDACTIONS A, B AND E BELOW INCLUDE COPYING OF DATA AND ACCESS CONTROLS, BUT NOT NECESSARILY IN THAT ORDER]

"A. [*R E D A C T E D*]

B. [*R E D A C T E D*]

C. Review, retention and deletion (RRD): [*REDACTED*]. However, MI5 will soon be applying an automated RRD process to operational data within [*a suite of systems*], which holds a large proportion of [*TE's*] operational data.

D. LPP: MI5 has a manual process in place for deleting LPP material from its systems if required to do so, [*R E D A C T E D*] .

E. [*R E D A C T E D*]

F. Institutional knowledge: we judge that, by January 2018 if not earlier, MI5 had a clear view of some of the compliance risks around [*TE*], to the extent that they should have carefully considered the legality of continuing to store [*REDACTED*] operational data in [*TE*]. The risks were also sufficiently clear that they should have been communicated to the IPC."

The Legislation

13. Section 2(2) of the IPA sets out the requirements of privacy. The Secretary of State can only lawfully sign off a warrant if, having regard to those requirements, he is satisfied that the warrant in question is necessary and proportionate.

14. Section 53 deals with "Safeguards relating to retention and disclosure of [intercepted] material." Subsection 1 stipulates that the Home Office has to ensure that there are arrangements in force to secure compliance with the requirements of subsections 2 and 5 (subject to subsection 9). The obligation on MI5 is to act in accordance with those arrangements. . By subsection 2, the promulgation of product must be limited to the least necessary for the purpose authorised. That covers the number of people to which it is disclosed or made available and the extent to which copies are made. Subsection 4 requires that similar protections apply to each copy.

Subsections 5 and 6 require destruction of the material as soon as it is no longer needed. These are mandatory requirements.

15. Section 129 requires similar safeguards in respect of product obtained from the execution of a targeted equipment interference warrant, section 150 for bulk interception, section 171 for bulk acquisition, and section 191 for bulk equipment interference. For bulk personal datasets under Part 7, there is not directly equivalent provision although the Secretary of State must ensure there are satisfactory arrangements for storing bulk personal datasets and protecting them from unauthorised disclosure.

16. There are also safeguards in respect of all product which contains, or may contain, LPP.

17. 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.

The Current Position

[Data Type 1]

18. As a result of the recent inspection, we have confidence in the way in which [*one category of*] warranted material "enters" the [*TE*] and the way it is handled ("ingress" and "storage"). [*This*] product is stored and analysed within [*a suite of systems*] . Various user interfaces are deployed to analyse the data, and [*key*] data stores are drawn on for this purpose. At an early stage a check is made to ensure there is a valid IPA warrant in place for the data.

19. [*For one category of data*] the risks are over [*REDACTED*] and the lack of assurance that such data is being appropriately deleted. There is a lack of assurance that LPP material has been appropriately deleted [*REDACTED*] .

[Data Type 2]

20. [*REDACTED*] it is unnecessary for the purpose of this Decision to explain how this data enters the [*TE*] and how it is handled. Suffice it to say, that we do not, at present, have concerns about ingress and initial storage.

21. Data in this category can be exported into file shares in [*TE*] [*REDACTED*] . Typically this will happen for further analysis. [*Some data*] may be passed on [*REDACTED*], and in these particular circumstances automated deletion will not occur [*REDACTED*] .

22. [*As with another category of data*] the risks are over [*REDACTED*] and the lack of assurance that data is being appropriately deleted.

There is a lack of assurance that LPP material has been appropriately controlled and deleted [*R E D A C T E D*] .

[Data Type 3]

23. We are presently satisfied that the ingress and storage arrangements are appropriate. [*R E D A C T E D*]

24. [*R E D A C T E D*]

[Data Type 4]

25. [*R E D A C T E D*] A similar situation to that set out above applies to ingress and storage. Similar weaknesses exist [*R E D A C T E D*] .

[Data Type 5]

26. [*R E D A C T E D*]

[Data Type 6]

27. [*R E D A C T E D*]

The Mitigations proposed by MI5 for those areas of weakness and concern

Introduction

28. On 3 April 2019, we received the proposed new Annex H to the MI5 Handbook for the Judicial Commissioners. This contained, first, [*Director of Policy and Information*]'s letter to me dated 11 March 2019 in its entirety and, second, a section entitled "Section II: further information about the [*TE*]and the mitigations being progressed, issued 1 April 2019". We sent through a request for additional information to which we received a prompt and helpful response that was followed up by a meeting at IPCO's offices on 4 April 2019 in order to discuss the enduring areas of uncertainty. What is set out below is taken from Section II and the additional information we requested. I suggest that consideration should be given to adding the latter, as appropriate, to Section II. The paragraph references below are to Section II.

29. It is undoubtedly right to bear in mind that at paragraph 12, we are reminded that all [*TE*] users are DV cleared.

30. I have been careful to distinguish between, on the one hand, data currently within the [*TE*] about which there is – for a substantive element of it – real uncertainty as to [*R E D A C T E D*] and whether it was, or is going to be, destroyed timeously and new warranted material (*i.e.* data acquired under warrants approved from this date onwards), on the other.

Copying (including file-sharing) and access to warranted material

31. [*R E D A C T E D*]

32. [*R E D A C T E D*]

33. Local records will be linked with the [*r e g i s t e r*] to ensure effective oversight of the copying and retention of warranted data. This will enable, *inter alia*, [*R E D A C T E D*] and testing by those responsible for audit [*R E D A C T E D*] .

34. [*R E D A C T E D*] Furthermore, as revealed in the information received on 4 April 2019, whenever [*R E D A C T E D*] , it must [*f o l l o w p r o c e s s e s*] in line with the processes established by the [*i n f o r m a t i o n t e a m s*] , and each [*information team*] will from this point onwards hold a log [*R E D A C T E D*] that will be available for inspection. [*R E D A C T E D*] .

35. [*R E D A C T E D*]

36. [*R E D A C T E D*].

[*R E D A C T E D*] .

37. [*R E D A C T E D*] .

Destruction of warranted material

38. By the end of April 2019, automated RRD will be in place across the system to delete, when appropriate, [*a c a t e g o r y o f m a t e r i a l*] , and until [*this time*] this will be done manually to ensure that none is held for longer than the relevant RRD policy.

39. For all other [*a r e a s*] , automated RRD will be delivered [*d u r i n g 2 0 1 9*] . Such material is currently within its agreed retention period.

40. Users have been reminded that it is their responsibility to delete data when there is no longer any need to retain it (paragraph 44).

41. It follows that for new warranted [*d a t a*] it will not be held for longer than the time stipulated in the relevant RRD policy and it will be deleted either automatically or manually.

Legal Professional Privilege

42. Although there is real uncertainty as to whether [*LPP material has in the past been deleted*] or whether there has been compliance with conditions imposed by Judicial Commissioners on the use or retention of such material, the position of new warranted material in the future will be markedly different. Most particularly, a

new naming convention is being introduced for file shares; this will require users to identify in the title of the file whether the copy of the data they have obtained includes LPP material (paragraph 51). Although a small number of specialist systems in the [TE] do not reveal whether LPP material has been flagged (paragraph 53), the new naming convention will circumvent this problem, by ensuring that it is clear that the data is within the LPP category.

43. In the interim, until the new naming conventions are in place, the new measures in place [*R E D A C T E D*] should provide proper control over the handling and destruction of LPP material.

Analysis

44. Albeit not strictly relevant to the present application, it is clear that for warranted material in [TE] there has been an unquantifiable but serious failure to handle warranted data in compliance with the IPA for a considerable period of time, and probably since IPCO first became operational. Assurances that have been made to the Secretary of State and the Judicial Commissioners of such compliance were, in hindsight, wrong and should never have been made. Warrants have been granted and judicially approved on an incomplete understanding of the true factual position. Indeed, I am concerned that on this important subject we were incompletely briefed during the Commissioners' induction programme, including that most recently provided to Lord Hughes and Sir Colman Treacy. To date, therefore, MI5's retention of the warranted material in [TE] cannot be shown to have been held lawfully and the failure to report these matters timeously to IPCO is a matter of grave concern which I will be addressing separately. The critical question, however, on this application is whether the data to be covered by the present warrant will be appropriately safeguarded.

45. On the basis of the mitigations set out in Section II, combined with the answers to the questions that I have received, subject to certain critical caveats, I am satisfied that MI5 have the capability **henceforth** to handle warranted data in a way which is compliant with the IPA. The protection in the immediate future is that, following the Guidance recently issued and repeated to staff, there can now be no doubt that all [TE] users are aware of the ways in which they need to handle warranted material, and particularly as regards "minimisation" and destruction. This means that the position relating to the [TE] is now consistent with many areas over which IPCO has oversight, in the sense that we are dependent on staff being trusted to act in a lawful manner and the role of the inspectors is to ensure *ex post facto* that their approach is in accordance with the law. The key caveat is that all the relevant activities must be susceptible to inspection and audit – in other words, MI5 and IPCO must be able to check in sufficient detail that there has been compliance with the legislation.

46. [*R E D A C T E D*] . I do not intend in this Decision to set out the precise nature of the inspection regime and the various forms of monitoring that will need to take place, but I want there to be no doubt as to the gravity of the situation and the need for IPCO to be reassured that breaches of the legislation are not ongoing. This will involve frequent inspections by IPCO, beginning on 15 April 2019, and I expect the inspectors to be afforded direct access to members of staff. It will be unacceptable for the inspectors to be asked to rely on hearsay accounts of internal conversations between members of MI5. I am confident that a method of undertaking this form of inspection can be secured without causing undue anxiety for members of MI5. The

inspectors will discuss with MI5 the kind of [*m o n i t o r i n g*] that we will expect to take place.

47. In the longer term, MI5 are developing ways of introducing and enhancing [*R E D A C T E D*] and otherwise ensuring compliance, for instance by the new mandatory naming conventions. It is planned that automated RRD will be in place by the end of April 2019 for [*a c a t e g o r y o f*] material (paragraph 41) and otherwise the new handling arrangements should ensure that material will be identified for destruction within the relevant timeframes.

48. As set out above, until the new naming conventions are in place, the [*n e w m e a s u r e s*] should provide proper control over the handling and destruction of LPP material.

49. This is a serious and inherently fragile situation. The future will entirely depend on compliance by MI5 with the legislation **and** the adequacy of the internal and external inspection regimes. IPCO will need to be reassured on a continuing basis that new warranted material is being handled lawfully. In the absence of this reassurance, it is likely that future warrant applications for data held in [*TE*] will not be approved by the Judicial Commissioners, and I will expect that the proposed mitigations are progressed at pace. The weaknesses outlined above are of sufficient magnitude to mean that the immediate mitigatory steps, which will be sufficient for the short term, cannot be expected to provide a long term solution, and the proposals made by MI5 in Part II must be implemented in their entirety in the shortest reasonable timeframe. Without seeking to be emotive, I consider that MI5's use of warranted data in [*TE*] is currently, in effect, in "special measures" and the historical lack of compliance with the law is of such gravity that IPCO will need to be satisfied to a greater degree than usual that it is "fit for purpose". It is of importance to add by way of postscript that now this problem has been ventilated, MI5 appear to be using every endeavour to correct the failings of the past and to secure compliance. The organisation has cooperated in every way with the inspection we recently conducted and the questions that I posed.

50. I have decided the separate applications listed above against the background of this generic decision.

010