S412 D1

[redacted]

Statement made on behalf of:	The Commissioner of Police of the Metropolis
Witness:	Cairo
Statement No:	3
Exhibits Referred to:	N/A
Date Statement Made:	4 August 2017

IN THE MATTER OF: PUBLIC INQUIRY INTO UNDERCOVER POLICING

~~CLOSED~~ WITNESS STATEMENT

Witness: Cairo

Occupation:

Address: c/o Directorate of Legal Services, 10 Lamb's Conduit Street, London, WC1N 3NR

I believe the facts stated in this witness statement are true

Signed..... [redacted] .....

Dated..... [redacted] .....

Introduction

1. I am currently employed by the Metropolitan Police Service. To keep this statement brief, my expertise will be set out in a supplementary statement.

[redacted]

2. In this statement I will address two main areas:

   (i) Sensitive MPS locations; and

   (ii) The expense of time and resources required in investigating whether redactions are required.

(i) Sensitive locations

3. Some MPS infrastructure is covert, meaning that there will be no official reference to it in the public domain and no public connection between the MPS and that piece of infrastructure. Maintaining a building as covert is expensive, difficult and resource-intensive. [redacted]

Example given of sensitive method used to maintain covert premises.

[redacted] A covert piece of infrastructure is always at the mercy of compromise, which can have hugely expensive consequences.

4. [redacted]

[redacted]

5. [redacted] a building (or part of a building) which hosts sensitive functions may have been adapted at considerable expense, or it may have unique features which render it particularly suitable to host sensitive functions. The MPS will always be keen to maximise the potential of a particular piece of infrastructure. [redacted]

6. Therefore, there are still risks in revealing that sensitive functions were <u>ever</u> carried out in a particular building, [redacted]

7. The specific risk in revealing that sensitive functions are or were carried out in a particular building include that:

   (i) Those who wish to obtain unauthorised access to covert infrastructure will know where to target their efforts, and will therefore become more likely to obtain such access;

[redacted]

(ii) Employees and others who use the building are more likely to be harassed, approached for corruption, and exposed to more serious risks including physical risks;

(iii) [redacted]

(iv) Sensitive police functions, including those that investigate serious and organised crime or terrorism offences, will be impeded;

(v) Money and resources will need to be spent on relocating the sensitive work carried out in the building.

8. [redacted] I believe that there is still a risk in revealing that sensitive work was ever carried out using a particular piece of infrastructure. Those who wish to obtain unauthorised access to sensitive infrastructure may not know that the specific sensitive work of which they are aware has become obsolete, [redacted] In general, to raise the profile of infrastructure used for a sensitive function carries the same risks as those set out at paragraph 7 above, and these risks might persist even where the infrastructure is, in fact, no longer used for a sensitive function.

9. Some specific examples of locations that are both public yet sensitive are:

[redacted]

(i) [redacted] and

(ii) [redacted]

10. This is not an exhaustive list.

(ii) <u>The Implications and proportionality of investigating possible risk for the purposes of applying for a Restriction Order</u>

11. I understand that under the Redaction Protocol, documents which the Inquiry deems to be "relevant and necessary" (and which the Inquiry therefore intends to publish on its website) will be assessed by the MPS for their suitability for general publication. Where the MPS considers that particular documents or words within documents will harm a public interest if published, it will apply for a Restriction Order over those documents or words. If the application is successful, those documents or words will be redacted.

12. The MPS is under a legal and moral duty to prevent and address risks to its employees. It must also strive to avoid causing harm to its ability to carry out lawful policing, its relationships with national and international partners and its ability to recruit suitable staff. The risks the MPS must consider are not just direct or serious risks, but also tangential risks, risks to third parties, and risk which may foreseeably arise in the future.

[redacted]

13. Therefore, as part of its consideration of possible Restriction Order applications over documents or words, the MPS must devote considerable resources to investigating (and, if necessary, subsequently providing evidence for) any direct or mosaic risk inherent in publication. This process is likely to involve any or all of:

    (i) Searching and analysing police records, which may be held in a number of databases and may not be easily searchable, and which include hard-copy records;

    (ii) Conducting open-source research (often requiring computers which leave no electronic footprint);

    (iii) Requiring senior MPS staff to receive the document (in hard copy, double-bagged and hand-delivered), digest it and advise on whether any direct or mosaic risk exists in its contents, provide evidence of the risk and if necessary draft a witness statement to that end;

    (iv) Conducting other enquiries within the MPS, such as interviewing staff;

    (v) Liaising with the National Police Chiefs' Council ('NPCC') and other agencies to ensure consistency and minimise consequential risk; and

    (vi) Instructing and coordinating with counsel.

14. There are some types of information whose publication presents an obvious risk – for example, the location of an observation post, or the name of a civilian covert human intelligence source ('CHIS'). There are other types of

[redacted]

information whose publication will clearly be anodyne. However, in some instances it will not be obvious whether information is anodyne or risky without at least embarking on the steps outlined above. For example, an operation name may be public or secret; a warrant number may or may not be connected with anonymous evidence in an earlier trial; a role may or may not be covert, etc.

15. While it is for the Inquiry to decide what documents are relevant and necessary, it seems to me that some words or sentences within those documents are of low relevance to the Inquiry's terms of reference or not necessary to publish, and yet require significant – and therefore disproportionate – resources devoted to the investigation of their risk.

16. To illustrate the allocation of resources to this task, I can provide the following examples.

<u>For the publication of a name which the Inquiry does not accept should be redacted on privacy grounds</u>

17. Depending on the context of the document, the MPS may have to carry out a full risk assessment of that individual. This risk assessment must examine, *inter alia,* the individual's past, present and former involvement with the MPS (and any involvement with third parties, such as organisations to which the

[redacted]

individual was seconded), and the risks such involvement may pose to either the individual or to another public interest if exposed.

18. The risk assessment process is lengthy and expensive. The independent risk assessor has estimated that, once he has been provided with a pre-prepared profile outlining the individual's background, it takes between eight and 240 man-hours per individual to carry out a risk assessment. This figure depends on how much documentation the risk assessor has to analyse himself, whether an interview with the individual is needed, and of course the nature and length of the individual's involvement with the MPS. This time estimate does not include the time taken to prepare a profile on the individual's background, supplied to the risk assessor. Using a figure of £30/hour, this amounts to a cost of between £240 and c.£10,000 for each risk assessment over an individual. This does not include the cost of counsel or DLS lawyers or any administrative costs.

19. We carry out this risk assessment because the consequences – both human and monetary – of failing to spot a risk and allowing it to materialise could be huge. The consequences to the individual could include (and this list is non-exhaustive): physical or psychological harm; damage to a career and disruption to private and family life. Monetary costs to the MPS might include relocating individuals and, if appropriate, their families, [redacted] and defending litigation.

[redacted]

20. I should stress that the risk assessment process is not simply considering what harm might arise out of someone's work with the SDS (or whatever context is mentioned on the face of the document in question). It may arise through work in other fields, such as terrorism or serious organised crime, which that individual has carried out in a different part of their career.

For the publication of details of someone's work (other than work with the SDS or NPOIU)

21. Many documents in this Inquiry will reveal either what work was carried out by a particular unit at a particular point in time, and/or that a named individual worked on that unit at a particular point in time. These references often appear in the context of an individual's career before and after their work in the SDS.

22. It is often not immediately obvious that the publication of those details would pose no risk to either the individual or the unit or the MPS in general, especially since many units of the MPS have either changed their name or materially changed their function in the period since 1968. The work of some units was very sensitive and known only to a few people. For example, if someone is said to have worked on "X" squad (I use that letter as a hypothetical example), it will not be immediately obvious whether that squad's existence or work-focus was publicly known, and if it was whether it is safe to

[redacted]

reveal that a particular individual worked there, and if it was not, what the risks would be of doing so.

23. To investigate the risk of publication properly, enquiries would have to be conducted into the nature of the unit at the time the document was published, whether the unit still exists and what it does, and the nature of the individual's work with the unit, among other things. For references that date from many decades ago, this research is likely to be either impossible or very time-consuming, relying on hard-copy records. I am not aware of any one individual who has a full knowledge of Special Branch's historic work, and there is no central index of what each part of Special Branch did at any one time. By and large there is no surviving "corporate memory" of the 1960s and 1970s, and in the era before the Freedom of Information Act 2000 and the current disclosure rules for civil litigation there were no well-established schemes set up for managing the discovery and disclosure of documents. Investigating the risk inherent in revealing someone's work history will therefore be a very time-consuming task.

<u>For the publication of the names of departments and infrastructure, unless known to be anodyne</u>

24. The explanation outlined at paragraphs 21 – 23 above applies to this topic as well.

[redacted]

For the publication of an officer's warrant number

25. It has formerly been the practice that officers in certain trials (such as terrorism trials) would give evidence using their warrant number instead of their name, where to give evidence in their real name would pose a risk to them. Therefore, a document published in this Inquiry which links a warrant number to a real name would undermine the anonymity of the officer if the warrant number had ever been used to give evidence. Undermining that anonymity could carry serious risks to the officer, depending on the reasons behind the original grant of anonymity.

26. To investigate whether any given warrant number is associated with anonymous trial evidence would be a huge (and perhaps impossible) task. There is no central index kept of people who have given evidence using a warrant number.

27. [redacted]
GIST: *further, historic, aspect of warrant numbers which means that they could be used to identify officers.*

Operation names

28. Even within the MPS, operation names are used as a way of disguising the exact direction or focus of an investigation. For example, a single

[redacted]

investigation might produce several operation names – a different name for different aspects of the operation – many of which will be revealed only on a need-to-know basis (especially where a new operation relates to possible corruption in the original operation). [redacted] There exists a general mosaic effect of revealing secret operation names; I am especially concerned that the [redacted] process might not be robust enough to prevent any mosaic effect damage triggered in this way.

29. Of course, many operation names are not secret or would be anodyne if published. It will not be immediately obvious to a reviewer on which side of the line a particular operation name will fall, and the research needed to investigate the issue will be time-consuming and could in itself cause damage.

30. I should stress that it may quickly transpire that many such references are anodyne. However, even the time that would need to be spent to establish this, when multiplied by many thousands of instances, will amount to a significant deployment of resources.