

**OPEN** Statement made on behalf of: The Commissioner of Police of the Metropolis

Witness: Detective Superintendent Steve Williams

Statement No: 1

Exhibits Referred to:

Date Statement Made: 20th May 2019

---

**IN THE FIRST-TIER TRIBUNAL  
(GENERAL REGULATORY CHAMBER)  
INFORMATION RIGHTS**

**Appeal reference:  
EA.2018.0164, 0165,  
0166, 0167, 0168, 0169,  
0170, 0171, 0172**

Between

Privacy International

Appellant

-and-

Information Commissioner

Respondent

-and-

Commissioner of the Metropolitan Police Service (joined to EA.2018.0164)  
Chief Constable of Avon and Somerset (joined to EA.2018.0166)  
Chief Constable of Kent Police (joined to EA.2018.0167)  
Chief Constable of South Yorkshire Police (joined to EA.2018.0168)  
Police and Crime Commissioner for Staffordshire (joined to EA.2018.0169)  
Police and Crime Commissioner for Warwickshire (joined to EA.2018.0170)  
Police and Crime Commissioner for West Midlands (joined to EA.2018.0172)  
Second Respondents

---

**Witness:** Detective Superintendent Steve Williams

**Occupation:** Police Officer

**Address:** C/O Directorate of Legal Services, Metropolitan Police Service, 10 Lamb's Conduit Street, London WC1N 3NR

---

1. I am a Detective Superintendent employed by the Metropolitan Police Service (“MPS”). For the last three years I have been head of the Technical Surveillance Unit (“TSU”) within Covert Policing. Prior to this I have been employed as a Detective Superintendent as head of the Child Abuse Command and also the head of Specialist Investigations within the Directorate of Professional Standards. I have 27 years’ service and during this time have performed a variety of proactive and reactive policing roles.
2. I have been asked to make this statement to outline the reason we ‘neither confirm nor deny’ the use or capabilities of certain covert tactics.
3. I shall divide this statement into two parts:
  - a. Operational policing and covert tactics; and
  - b. Oversight of the use of covert tactics.

### **Operational Policing and Covert Tactics**

4. The first point I would like to make is that Covert Policing, by its nature, regularly works closely with and undertakes joint operations with the National Counter Terrorism Policing Headquarters (NCTPHQ) and bodies covered by s.23 FOIA. In this way, Covert Policing works alongside s.23 Bodies to disrupt terrorism and serious criminality. Given that Covert Policing works so closely with s.23 Bodies, confirmation or denial of information held in relation to covert policing tactics would undermine that close relationship with s.23 Bodies.
5. The fact that police use covert tactics to target criminality and terrorism is widely known. The exact detail and extent of law enforcement capabilities are not widely known. To put this in context, the use of certain types of covert capabilities are only known about by a small number of people within the MPS. These people work within dedicated teams and are appropriately vetted.

6. Covert policing tactics are used by police forces and law enforcement agencies across the world. These tactics target the most serious criminality and terrorism. The use of the tactics results in the arrest and prosecution of the most dangerous individuals and disruption of criminal networks. These people are often aware that police use covert tactics but do not know which covert tactics police and law enforcement use or have access to. This is even more significant when someone has been arrested and prosecuted. The defendants will often attempt to find out how police come into possession of the intelligence that resulted in their arrest. Disclosure of our capabilities or tactics (or lack thereof) would seriously undermine future operations and place people's lives at risk.
7. Where cases involving covert types of tactics lead to prosecution there is a recognised framework for applying to prevent the disclosure of the tactics and capabilities by way of Public Interest Immunity applications. The Judge will normally hear an application from police or law enforcement in closed chambers. If the Judge decided it was necessary for the trial to proceed to disclose the use of the tactics or capability the police and the Crown Prosecution Service would consider making a decision not to proceed to prevent disclosure of the tactics.
8. The prevention of disclosure of covert tactics is a national and international concern. Within UK policing any disclosure of a covert tactics would have to be discussed at a national level to see how it would impact on UK policing. This would cover both disclosure at court or responding to Freedom of Information requests.
9. Criminal Networks and terrorists are actively trying to find out which covert tactics and their capabilities law enforcement utilise. The internet is scattered

with pages and forums dedicated to people speculating on police tactics and the capabilities of law enforcement. Much of this information is guesswork, incorrect or based around what is seen in the 'movies'. Even when specific tactics are discussed, people are not aware of their capabilities, limitations or true nature of how they are used.

10. In relation to covert technology utilised by police, maintaining secrecy is even more important. Technology changes rapidly and what could be done one day may be superseded or altered by the events of the near future. If criminals or terrorists know about the capabilities of covert technology, they will adjust their behaviour accordingly.

11. If we were to disclose the ownership or use of specific tactics or equipment, or that the same are not owned or used, it would allow criminal networks and terrorists to build up an accurate picture of our ability to respond to the most serious criminality. In addition to this, if the MPS responded to requests on the use or otherwise of specific technologies or tactics it would significantly damage our relationships with other police forces and law enforcement agencies. The capabilities of this type of covert technology by law enforcement and partner agencies are closely guarded within an extremely small community. Development of these capabilities and/or tactics is shared within this community on the basis of trust that it will only be used by trained and vetted staff.

12. The ability to deploy these types of tactics not only supports the investigation and prosecution of criminals and terrorists but ultimately protects the lives of the communities that we serve. If we disclosed our tactics and capabilities, this would seriously damage our ability to respond to criminality and put in danger the lives of the communities that we are here to protect.

13. Accordingly, I fully endorse the Tribunal's reasoning in paragraph 10 of *Mathieson v IC & Devon & Cornwall Constabulary* (EA/2010/0174):

*"All these points have some validity and we accept that disclosure of the requested information may only have tipped the scales in favour of terrorists and serious organised criminals slightly. But we are bound also to take account of the fact that, although the risk may have been small, if disclosure of the information requested meant, for example, that a terrorist incident took place which might otherwise have been avoided, the results could be catastrophic. We have considerable sympathy with Mr Middleton's plea that the police '...need to stay one step ahead' and with his rhetorical question: 'Why would we want to give one of our tools back to the criminals?'"*

14. If we provide detail on how we fight crime and terrorism, we engage in that fight with one hand tied behind our back.

### **Oversight of the Use of Covert Tactics**

15. There are separate oversight regimes regulating:

- a. Targeted Interception (i.e. for communications)
- b. Targeted Equipment Interference

16. Historically, targeted interceptions were governed by RIPA and targeted equipment interference was governed by Part 3 Police Act 1997. Both are now governed by one act: the Investigatory Powers Act 2016. However, any application for a warrant must differentiate between a request for targeted interceptions and targeted equipment interference.

17. There are a number of administrative roles and functions both within and without the MPS to ensure that the use of covert authorities, technologies and tactics is lawful and proportionate. Many, but not all of these functions are

replicated at a national level across other Police Services and Law Enforcement agencies.

18. In the remainder of this section, I shall recount how matters of a covert nature are regulated and overseen.

### Training

19. An application for a warrant cannot be made before an officer or member of staff has attended training, which provides a basic overview of the need to obtain an authority to undertake this activity. Even in basic training the fundamentals of the Human Rights Act 1998 particularly areas of legality, proportionality and necessity are addressed (for example, with regard to rights of privacy), with officers and staff being aware in simple terms that these areas need to be addressed prior to undertaking any planned covert action.

20. Following basic training, other more bespoke training is provided to officers and staff dependent upon the role they are performing or the career path they are following. By way of example, there is College of Policing accredited training in relation to surveillance operatives. Similarly there is training for intelligence officers, for those who provide technical support or services and for senior officers who are required to approve or authorise covert activity.

### Application

21. Any request for an authority to conduct covert activity or use covert investigatory powers starts by an officer (or member of staff) submitting an application to a “gatekeeper”.

### Gatekeepers and Central Authorities Unit

22. Gatekeeping and central authorities units are responsible for quality assuring and managing the authorisation processes for applications made to conduct Property Interference and Intrusive Surveillance requiring a chief officer's (or in the case of the MPS, Assistant Commissioner's) authorisation. They are also responsible for providing specialist advice, quality assuring and processing all applications relating to Directed Surveillance at both Superintendent and Chief Officer/AC level for all of the Met Operations and Frontline Policing commands.

### Authorisation

23. Any authority in this field has to be authorised by an officer of at least Superintendent rank and the higher level, more intrusive authorities have to be authorised by a Chief Constable (or AC in the MPS).

### Covert governance Command MO5

24. The MPS has a dedicated command – MO5 Covert Governance – which encompasses the gatekeepers detailed above and in addition provides the following internal oversight and governance functions.

#### **(i) Inspection & Review**

25. The Inspection & Review (“I&R”) Team is responsible for conducting inspections of covert activity by MPS operational teams. These inspections include assessment of the documents and records associated with undertaking this activity and compliance with internal policies and procedures.

#### **(ii) Peer Inspection**

26. MO5 has dedicated Covert Operational Security Advisors (“OpSy”) who provide advice and guidance to operational teams. Furthermore, they now conduct peer inspections of all departments in the MPS that issue and administer covert authorities, this includes the Directorate of Professional Standards (“DPS”) and Counter Terrorism Command (“CTC”). Additionally, they undertake thematic inspections e.g. the Undercover Policing Unit. These inspections are undertaken between formal external inspections of the MPS by the Independent oversight body to ensure any recommendation from that body are being implemented and other areas of organisational learning are identified ahead of the annual external inspection.

**(iii) Error reporting**

27. A fundamental element of covert activity within the MPS is the need to have openness and transparency when mistakes or errors are made.

28. When mistakes are identified, the operational team is required to submit a detailed report via their OCU Commander to MO5. This matter will then be investigated by one of the OpSy cadre to identify how the error occurred and to make recommendations to prevent a similar error recurring.

29. If the error is assessed as serious, a report will be submitted to the Senior Responsible Officer (“SRO”) for the MPS (AC - Met Ops). The report will detail the circumstances of the error and the recommendations to prevent a recurrence. The SRO will write a letter to the Investigatory Powers Commissioner explaining the error and the remedial action being undertaken.

30. If the error is assessed as minor, i.e. an administrative oversight, the matter is presented to the independent oversight body at the time of their next inspection of the MPS.



## IPCO

31. The Investigatory Powers Act 2016 amalgamated a number of precursor bodies into a new powerful oversight body in relation to covert powers. The Investigatory Powers Commissioner's Office ("IPCO") comprises a number of former and serving High Court Judges who are required to approve the applications for higher level authorities (referred to as a "double lock") in addition it employs a team of Inspectors who will conduct an annual inspection of the MPS (and other relevant police services and agencies) and make recommendations in relation to their findings. The Investigatory Powers Commissioner is required to report their findings annually to the Prime Minister.

## Oversight

32. It should be noted that at the time of the submission of the original FOIA, covert operations involving equipment interference were governed by Part 3 of the Police Act 1997. However, since September 2018 the relevant regime is Part 5 Investigatory Powers Act 2016.

33. If an application for a targeted equipment interference warrant were made, it would start with the applicant from an operational team having been accredited to submit an application (see paras 19-21 above). All applicants and others engaged with Equipment Interference have to have signed an undertaking that they acknowledge the safeguards contained within the legislation.

34. The application would be submitted to a Central Authorities Bureau ("CAB") gatekeeper to quality assure the application to ensure the serious crime threshold (or vulnerability aspects) have been met. The gatekeeper will also assess the intelligence case and the proportionality and necessity of the case

prior to submission to the chief officer/AC for authorisation. This may entail the CAB seeking clarification or additional information from the applicant. If the case is felt to be insufficient it will not be sent to a chief officer for authority.

35. If the application is considered to meet the appropriate standard it will be sent to the Chief Officer (or Assistant Commissioner or the Deputy Commissioner for authority in the MPS). The Chief Officer/AC will then either approve or disapprove the application. If rejected, the operation will not be progressed. If authorised, the application will be sent to the Investigatory Powers Commissioners Office where it will be reviewed by a Judicial Commissioner.

36. The Judicial Commissioner, a retired or serving High Court Judge, will again review the intelligence case, proportionality and necessity of the application.

37. The Judicial Commissioner will either approve or disapprove the application. This is the “double lock” referred to above at paragraph 31. Subject to the following paragraph, no police operational deployment can take place until an approval has been received from the Judicial Commissioner.

38. In an urgent case, e.g. a kidnap, similar threat to life or very vulnerable missing person, the Chief Officer/AC (or Deputy Commissioner) may authorise the operational deployment to proceed without referring the case to a judicial commissioner. However, the case will have to be referred to a judicial commissioner within 5 days. The Judicial Commissioner can order the discontinuance of any activity and the destruction of any material obtained should they decide the case failed to meet the required standard.

39. Under the old, Part 3 Police Act 1997 regime, the process for applying for a warrant was the same, save that there was no judicial oversight. Inasmuch as the applicant would submit an application to the CAB, the CAB would undertake the same due diligence checks in relation to legality, i.e. did the application

meet the serious crime threshold, proportionality and necessity. The application may have been declined at this stage if it failed to meet the required standard. If it was of an acceptable standard it would be sent to the AC (or Deputy Commissioner) who would either approve or disapprove the application. These authorities would then be subject to annual inspection by the former oversight regime, (The Office of Surveillance Commissioners).

### MOPAC (Dara) & HMICFRS

40. The Police and Crime Commissioner (PCC) function for the MPS is devolved to the Mayor of London. The Mayor has established a department, The Mayors officer for Policing and Crime (MOPAC) and created a specific portfolio with a Deputy Mayor to manage this responsibility.
41. The Mayor's office also has a Directorate of Audit & Risk Assurance (Dara) who will review specific areas of interest to the Mayor which may include areas of covert activity for example the Covert Finance Unit (CFU). This is to reassure the public that there is independent oversight of the funding in relation to covert activity and proper accountability in this area.
42. Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services may also be called upon to conduct external thematic inspections of specific areas of policing activity. They have previously inspected surveillance activities. HMICFRS will also submit their findings in a report to the Commissioner of Police and make recommendations for improvement.

### Court Proceedings

43. The final arbiter of the police use of covert authorities is a trial judge in a court of law. Section 78(1) of the Police & Criminal Evidence Act 1984 states:

*'In any proceedings the court may refuse to allow evidence on which the prosecution proposes to rely to be given if it appears to the court that, having regard to all the circumstances, including the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it.'*

44. This would include a case where the court felt that covert activity was disproportionate or hadn't been properly authorised.

#### "Hoovering up" Protesters' Data

45. The Appellant has suggested that the police might, if the police did have CCDC equipment, use it to "hoover up" vast amounts of IMSI or IMEI data, for example at a peaceful demonstration. I would like to say two things about this:

46. First, even if the police were inclined to do this (which we are not) the oversight regime would absolutely preclude us from doing so.

47. Second, in those extremely rare occasions where we need to collect all data in a location at certain time (for example, to ascertain who was in a specific location at the time of a murder), we could, for example, make a communications data application under RIPA (at the time of writing), to obtain a download of cell tower activity data, which would provide us with (among other things) the IMEI and IMSI data of all the equipment.

#### Conclusion

48. Accordingly, the deployment of any covert technique or technology is subject of multiple checks and balances to ensure that the rights of the citizenry are protected. The MPS and, generally, UK Policing take the rights of individuals

seriously. The importance of the work undertaken by covert units nationwide cannot be overstated. It is of utmost importance that the capabilities of these units remain secret in the face of concerted efforts by criminal networks and terrorists to piece together their methodology in order to adapt their behaviours and stay ahead of law enforcement. For this reason, the MPS and UK law enforcement correctly asserts the right to reply "NCND" to requests which would demonstrate either the capabilities available, or their lack thereof (as the case may be).

I believe the facts stated in this witness statement are true

Signed.....

A solid black rectangular box redacting the signature of the witness.

Dated .....

*20th May 2019*