Appeal No. EA/2018/0164

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

AND IN THE MATTER OF TWO APPEALS PURSUANT TO SECTION 57 OF THE FREEDOM OF INFORMATION ACT 2000

B E T W E E N:

PRIVACY INTERNATIONAL

Appellant

- and -

THE INFORMATION COMMISSIONER

First Respondent

- and -

THE COMMISSIONER OF POLICE OF THE METROPOLIS

Second Respondent

- and -

(1) CHIEF CONSTABLE OF KENT POLICE
(2) CHIEF CONSTABLE OF SOUTH YORKSHIRE
(3) WEST MIDLANDS POLICE AND CRIME COMMISSIONER
(4) CHIEF CONSTABLE OF AVON & SOMERSET CONSTABULARY
(5) CHIEF CONSTABLE OF WARWICKSHIRE POLICE
(6) STAFFORDSHIRE POLICE AND CRIME COMMISSIONER
(7) CHIEF CONSTABLE OF WEST MERCIA POLICE

Interested Parties

RESPONSE OF THE SECOND RESPONDENT

INTRODUCTION

1. This Response is filed on behalf of the Second Respondent ("the MPS") in respect of the appeal brought by Privacy International. Pursuant to the Tribunal's Case Management Directions of 28 September 2018 this Response addresses the appeal

against the Information Commissioner's decision of 10 July 2018 (decision notice reference number FS50728051).

2. The MPS has not had sight of any response from the Information Commissioner, but understands that she maintains her position as set out in the decision notice. The Appellant's Reply to the Information Commissioner's Response will be filed with its Reply to all Responses lodged by the various forces together on 16 November 2018.

3. The MPS understands that the Appellant has sought to appeal multiple decisions of the Information Commissioner concerning eight separate police forces. The subject matter of each appeal is likely to be, if not identical then, fundamentally similar in nature for each force and the MPS agrees that with the Appellant's suggestion that the appeals be heard together. By directions dated 3 October 2018, the nine appeals are to be listed for a Case Management Hearing. The directions at §5 set out the issues to be considered at the Case Management Hearing. The MPS's position is that:

   (i) The issues in this appeal should be decided after a hearing;

   (ii) The hearing is likely to take 2 days;

   (iii) The Tribunal will be invited to direct under Rules 14 and 35 of the Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (hereafter "the 2009 Rules") that certain documents and information not be disclosed to the Appellant and be considered as 'closed material' and that part of the hearing be conducted in private to consider the closed material and to consider closed submissions;

   (iv) The MPS (and any other force as appropriate) be permitted to lodge closed material with the Tribunal.

SUMMARY OF THE MPS'S RESPONSE

4. For the reasons set out herein, the MPS opposes the appeal and submits that the Information Commissioner's decision to uphold the MPS's refusal to confirm or deny in relation to the information sought pursuant to s.2(1) of the Freedom of Information Act 2000 (FOIA) was correct.

5. In general terms, and subject to those parts of the appeal that the Information Commissioner allowed, it is submitted that the MPS was correct in neither confirming

nor denying the Appellant's request for information relying together on ss. 23(5), 24(2) and 31(3) of FOIA. The MPS has adopted the correct approach in relying on all three provisions.

FACTUAL BACKGROUND

6. In a letter dated 1 November 2016, the Appellant requested from the MPS information concerning the purchasing, ownership, confidentiality and use of mobile phone surveillance technology, specifically concerning Cover Communications Data Capture (CCDC) using International Mobile Subscriber Identity (IMSI) catchers. The request was made to the MPS under four headings:

> 1. Purchase orders, invoices, contracts, loan agreements, solicitation letters, correspondence with companies and other similar records regarding the Metropolitan Police's acquisition of CCDC equipment. Please include records of all purchase orders, invoices, contracts, agreements, and communications with CellXion.
>
> 2. Marketing or promotional materials received by the Metropolitan Police relating to CCDC equipment.
>
> 3. All requests by CellXion or any other corporation, or any government agency, to the Metropolitan Police to keep confidential any aspect of Metropolitan Police's possession and use of CCDC equipment, including any non-disclosure agreements between Metropolitan Police and CellXion or any other corporation, or government agency, regarding the Metropolitan Police's possession and use of CCDC equipment.
>
> 4. Legislation, codes of practice, policy statements, guides, manuals, memoranda, presentations, training materials or other records governing the possession and use of CCDC equipment by the Metropolitan Police, including restrictions on when, where, how, and against whom it may be used, limitations on retention and use of collected data, guidance on when a warrant or other legal process must be obtained, and rules governing when the existence and use of CCDC equipment may be revealed to the public, criminal defendants, or judges.

7. By an email dated 29 November 2016, Catherine Carrington of the MPS's Information Rights Unit, responded to the Appellant's request by neither confirming nor denying whether the MPS held the requested information. Reliance was placed in that email on ss. 23(5), 24(2), 30(3) and 31(3) of FOIA and reasons were given for the decision, which can be summarised as follows:

   (i) The information would be available to the world at large.

   (ii) Revealing whether or not the MPS held this information would prejudice law enforcement by advertising the investigative techniques available or not available to the police and whether or not and how such techniques were being used.

(iii) Given the similar information requests made by the Appellant to multiple forces, it would be prejudicial to UK-wide law enforcement if criminals and terrorists were able to map out where particular law enforcement surveillance technologies were utilised, if they were being utilised at all.

(iv) It could outline the investigative priorities of the police.

(v) The public interest lay in neither confirming nor denying possession of the information requested as doing so could damage national security and/or compromise law enforcement and the balance lay against providing a response. The public interest in holding the police to account for the techniques used was amply met by other regimes under the Regulation of Investigatory Powers Act 2000, and by the Independent Police Complaint's Commissioner (now the Independent Office of Police Complaints) and the Office of the Surveillance Commissioner.

8. The MPS is aware that the Appellant made similar requests to a range of Chief Constables and Police and Crime Commissioners (PCCs). With the partial exception of Warwickshire PCC and West Mercia PCC, who confirmed only that they possessed a business case in respect of the purchase of IMSI catchers, all forces and PCCs took the same position as the MPS and neither confirmed nor denied that they held the information requested.

9. On 24 January 2017, the Appellant sought an internal review of the decision of the MPS. In a letter dated 13 June 2017, Brian Wilson of the MPS's Information Rights Unit replied maintaining the MPS's position as set out in its decision of 29 November 2016.

10. Also on 24 January 2017, the Appellant complained to the Information Commissioner in respect of the MPS's decision to neither confirm or deny. In Grounds of Appeal dated 12 February 2018, the Appellant set out its challenge to the MPS's decision. The basis of the appeal was summarised at §6:

(i) Legislation, guidance and policies governing use of such equipment could not be subject to an 'neither confirm nor deny' position under FOIA;

(ii) Sections 23(5) and 30(3) of FOIA were not engaged

(iii) Confirming or denying the existence of the information would not prejudice national security;

(iv) Confirming or denying the existence of the information would not prejudice law enforcement; and

(v) The public interest in disclosing the information outweighed the public interest in neither confirming nor denying its existence for the purposes of ss. 24(2), 30(3) and 31(3) FOIA.

11. The Information Commissioner decided on 10 July 2018 to uphold the appeal in part.

(i) The appeal in respect of parts 1 and 3 of the request was not upheld and it was determined that the MPS had correctly relied on ss.23(5) and 24(2).

(ii) The appeal in respect of part 2 of the request was upheld and the MPS was required to respond to the request.

(iii) The appeal in respect of part 4 of the request was upheld only as to the request for 'legislation' and 'codes of practice'. The appeal was dismissed as to the remainder of the request.

12. It is against that decision that the Appellant now appeals.

ISSUES FOR THE APPEAL

13. This appeal raises both questions of law and challenges to the Information Commissioner's decision on the facts.

(i) The issue of law for the Tribunal concerns the scope and interpretation of the exemption under s.23(5) FOIA (ground 1 of the Appeal); and

(ii) Further, the Appellant challenges the Information Commissioner's decision on:

(a) The reliance on s.23(5) and/or s.24(2) (ground 2 of the Appeal); and

(b) Where the balance lies in determining what is in the public interest (ground 3 of the Appeal).

14. The Appellant reserved its position as to any exemptions in FOIA that may be relied upon by the Respondents other than ss.23 and 24, which formed the basis of the

Information Commissioner's decision. The MPS highlights at this stage that it will further rely, as it has done at all stages, on the exemption in s.31(3) FOIA but not the exemption in s.30(3).

LEGAL FRAMEWORK

15. Section 23(5) FOIA provides:

> (5) The duty to confirm or deny does not arise if, or to the extent that, compliance with section 1(1)(a) would involve the disclosure of any information (whether or not already recorded) which was directly or indirectly supplied to the public authority by, or relates to, any of the bodies specified in subsection (3) *[bodies dealing with security matters]*.

16. The term 'directly or indirectly supplied' has a plain meaning. The Tribunals have, however, had to grapple more directly with what is meant by 'relates to'. All that is necessary is for there to be 'some connection' between the information and a body listed in s.23(3). As set out in *The All Party Parliamentary Group on Extraordinary Rendition v Information Commissioner* (EA/2012/0049-51) at [65]:

> Applying the ordinary meaning of the words "relates to", it is clearly only necessary to show some connection between the information and a s.23(3) security body; or that it touches or stands in some relation to such a body. Relates to does not mean 'refers to'; the latter is a narrower term. Thus, for example, a response that no information is held may create a sufficient connection between the response and a security body for the purpose of s.23(5): see *Cabinet Office v Information Commissioner* (EA/2008/0080) at [21]-[23] and [27] ("Cabinet Office").

17. The question of whether the s.23(5) requirements are met is one for the Tribunal to determine on the balance of probabilities (*Metropolitan Police v Information Commissioner* (EA/2010/0008) at [19-20]).

18. Section 24(2) FOIA provides:

> (2) The duty to confirm or deny does not arise if, or to the extent that, exemption from section 1(1)(a) is required for the purpose of safeguarding national security.

19. Section 31(3) FOIA provides:

> (3) The duty to confirm or deny does not arise if, or to the extent that, compliance with section 1(1)(a) would, or would be likely to, prejudice any of the matters mentioned in subsection (1) *[relating to law enforcement]*.

20. It is not in contention that the exemption in s.23 is absolute, whilst the exemptions in s.24 and 31 are subject to the application of a 'public interest' test.

SUBMISSIONS ON THE INTERPRETATION OF S.23(5) FOIA

21. The Appellant, at paragraphs 32(d)-(g), takes issue with the Information Commissioner's approach to the interpretation of s.23(5) as provided in her decision at §38: *"whether or not the use of such equipment could 'relate to' any of the security bodies."* However, the test applied by the Information Commissioner was, in fact, set out in full at §41: "*the evidence must suggest to a sufficient degree of likelihood (rather than certainty) that any information falling within the scope of the request would relate to, or have been supplied by, a body specified in s.23(3)."* As such, the attack on the definition applied by the Information Commissioner is misconceived.

22. Irrespective, it is submitted that the test to be applied is that set out in *Baker* at [65] and *Metropolitan Police* at [19-20]: that on the balance of probabilities is the Tribunal satisfied that the information either was directly or indirectly supplied by a s.23(3) body or that the response would (one way or the other) create a sufficient connection to a s.23(3) body as there is some connection or the information touches or stands in relation to a s.23 body.

23. It follows that the narrow approach contended for in paragraph 32(b) of the Appellant's Grounds of Appeal is misconceived and contrary to authority. It would undermine the purpose of the regime if such a narrow test were required:

    (i) First, it would significantly hamper the ability of s.23(3) or associated bodies to perform their essential functions.

    (ii) Second, it would undermine the purpose of the provisions permitting bodies to neither confirm nor deny as such an option would only be open to a body where the information *did* come from or relate to the security bodies. If satisfying the test under s.23(5) required effectively confirming that the information was 'actually connected' to the security bodies then neither confirming nor denying under s.23(5) would in itself confirm their involvement.

24. Furthermore, such an approach would run counter to the established practice that s.23(5) and s.24(2) be relied upon together precisely so as to avoid unintentionally

confirming or denying the involvement of security bodies. So that s.23(5) and s.24(2) can be applied co-extensively, the test must be a broad one so that the role of the security bodies can remain vague and unknowable. As set out in *Baker v Information Commissioner* EA/2006/0045 at [34-5] and [43-5], public bodies should rely on both precisely so that no one is able to identify the role or otherwise of security bodies. That approach is further confirmed in the Ministry of Justice's 2012 Guidance on s.23:

> In practice it is very rare that a neither confirm nor deny response will cite just section 23, as this will confirm that the question of whether or not information is held relates to one of the section 23 bodies. Therefore, to avoid releasing information about one of these bodies which has not already been released, it will be necessary to rely upon neither confirm nor deny under both section 23 and section 24. By using both exemptions it obscures the fact that a section 23 body may or may not have been involved.

SUBMISSIONS ON THE CHALLENGE TO THE FINDINGS OF THE INFORMATION COMMISSIONER

25. For the reasons set out above, the MPS will not provide any open submissions as to whether or not the ss.23(5) and 24(2) exemptions are individually made out. The MPS relies on all the exemptions in ss. 23, 24 and 31 together.

26. The MPS makes general submissions under the following sub-headings:

    (i) The need to neither confirm nor deny the existence or absence of information of surveillance techniques for reasons of national security and law enforcement; and

    (ii) Applying the public interest test in respect of policing techniques.

27. The thrust of the MPS's submissions is that the Information Commissioner came to the correct decision.

Neither confirming nor denying the existence or absence of information of surveillance techniques (Ground 2)

28. As the Information Commissioner correctly determined, if a police force were to confirm or deny that it possessed the information requested in parts 1, 3 and most of 4 of the FOI request, the police would effectively be confirming or denying whether or not they had purchased and were using the equipment in question. For example, if the MPS confirmed or denied that it possessed purchase orders then it becomes

obvious whether or not purchases had been made; confidentiality agreements would only be needed if purchases had been made; manuals and internal policy for use would make it obvious that police officers needed guidance to operate the machinery. Other than in respect of the limited areas in which the Information Commissioner allowed the Appellant's complaint, requiring the MPS to confirm or deny whether it held the requested information would have the inevitable result of the wider world knowing if the MPS had bought and were using CCDC devices and, if so, which ones.

29. The starting point, therefore, is that allowing this appeal would effectively reveal to the world whether a surveillance technique is or is not used by the police and, if so, where, by whom, and to what extent.

30. The MPS relies on the reasons set out in its refusal decision:

> Although the techniques are in the public domain, it is how and when they might be used, that are the sensitive issues for the police service. These techniques could be deployed for more high profile sensitive operations, albeit not necessarily in the MPS force area, therefore the NCND is required to protect other forces that may use them.
>
> Any disclosure under FOIA is a disclosure to the world at large, and confirming or denying the use of specialist techniques which may or may not exist, and which (should they exist) the MPS may or may not deploy in specific circumstances would prejudice law enforcement. If the requested information was held by the MPS, confirmation of this fact would reveal that the MPS have access to sophisticated communications analysis techniques. This would be damaging as it would (i) limit operational capabilities as criminals/terrorists would gain a greater understanding of the MPS's methods and techniques, enabling them to take steps to counter them; and (ii) provide an indication to any individual who may be undertaking criminal/terrorist activities that the MPS may be aware of their presence and taking counter terrorist measures.
>
> Conversely, if information was not held by the MPS, and a denial was issued, this would reveal to those same individuals that their activities are unlikely to have been detected by the MPS. It may also suggest (whether correctly or not) the limitations of the MPS'S capabilities in this area, which may further encourage criminal/terrorist activity by exposing a potential vulnerability. Disclosure of the information could confirm to those involved in criminality or terrorism that they are or have been the subject of such activity, allowing them to gauge the frequency of its use and to take measures to circumvent its use.
>
> Any compromise of, or reduction in technical capability by the MPS would substantially prejudice the ability of the MPS to police their area which would lead to a greater risk to the public. This detrimental effect is increased if the request is made to several different law enforcement bodies. In addition to the local criminal fraternity now being better informed, those intent on organised crime throughout the UK will be able to 'map' where the use of certain tactics are or are not deployed. This can be useful information to those committing crimes of drugs and terrorist activities.

31. The Appellant has referred to the dicta of Maurice Kay LJ in *Mohamed and another v Secretary of State for the Home Department* [2014] 1 WLR 4240 where at [20], the learned judge opined that: *"[NCND] requires justification similar to the position in relation to public*

interest immunity (of which it is a form of subset)." Applying that approach, it is of relevance that operational policing techniques are routinely held to be subject to public interest immunity. As *per* Lord Bingham in *R v H* [2004] 2 AC 134 at [18], public interest immunity would attach to information such as *"the use of […] operational techniques (such as surveillance) which cannot be disclosed without … jeopardising the success of future operations"*.

32. The Appellant underestimates the ingenuity and tenacity of criminals and terrorists. It is trite that the world knows (or can easily find out) what powers are available to the police, but it does not follow that the world knows how those powers are used and the specific techniques used in investigating and preventing crime and protecting the national security. Similarly, it is well-documented that police use certain methods when investigating or preventing crime but the details of, for example, how drug traffickers are surveilled (if they are) or how the police work with other partner agencies are not matters of public knowledge; were they so, those tactics would lessen in value.

33. So it is with surveillance. The police (or other bodies) have various ways to infiltrate, for example, a terrorist cell or organised criminal group. If it were known that the police did not use a specific type of surveillance technique at all it would embolden terrorists and criminals. If it were known that only some forces used such techniques, it would provide valuable information to anyone planning serious criminality or terrorism as to areas of the country where policing would be less effective. If it were known that all forces used such techniques, it would encourage terrorists or criminals to change their practices and make prevention and investigation more difficult.

34. In light of the above, it is respectfully submitted that confirming or denying the information requested could adversely impact on national security and/or be injurious to law enforcement.

35. Finally, the Appellant relies on various statements that, it is argued, undermine the MPS's neither confirm nor deny position:

    (i) Contrary to what is stated in the Grounds of Appeal, ownership by the police of IMSI catchers has not been confirmed or denied in Parliament.

    (ii) The possession of a 'business case' by any force (a) does not bear on the MPS; and (b) does not indicate the action then taken by that force.

    (iii) The 'public confirmations' relied on by the Appellant are little more than:

(a) References to the safeguards in place concerning surveillance techniques;

(b) Unconfirmed press coverage; and

(c) Comments made explicitly subject to a policy of neither confirming nor denying the information sought.

(iv) The use or otherwise of IMSI catchers in other jurisdictions, where public bodies may be subject to different rules in terms of their use and of disclosure of the source of information for the purposes of criminal trial, have little relevance to the decision of this Tribunal.

Public interest (Ground 3)

36. The Appellant commences his submissions at paragraph 34(a) of his Grounds of Appeal by citing *Keane v Information Commissioner and others* [2016] UKUT 461 (AAC) at [58] in support of the proposition that the s.24 exemption does not carry *"inherent weight"*. The full paragraph states as follows:

> Nor am I persuaded by the Appellant's arguments that the Tribunal treated either exemption as absolute in nature. The framework of analysis as set out at the start of the Tribunal's reasons make it plain that they were well aware they were dealing with qualified exemptions, as did the organisation of their reasoning, notwithstanding some rough edges. Whilst it may well be wise to avoid characterising particular exemptions as carrying "inherent weight" (see Upper Tribunal Judge Turnbull's decision in the Cabinet Office case at paragraph 66), the reality is that the public interest in maintaining the qualified national security exemption in section 24(1) is likely to be substantial and to require a compelling competing public interest to equal or outweigh it (as recognised in the First-tier Tribunal decision in *Kalman v Information Commissioner* [2010] UKFTT EA 2009 0111 (GRC), [2011] 1 Info LR 664 at paragraph [47]).
>
> [emphasis added]

37. That there is plainly substantial weight in the public interest arguments in favour of the exemption at s.24 is further set out in the Ministry of Justice's 2012 Guidance on s.24:

> There is obviously a very strong public interest in safeguarding national security. If non-disclosure is required to safeguard national security it is likely to be only in exceptional circumstances that consideration of other public interest factors will result in disclosure. The balance of the public interest in disclosure will depend in part on the nature and likelihood of the potential risk to national security, as well as the nature of the countervailing public interest considerations in making the information available. Each request for information will need to be judged on a case-by-case basis.

38. For the reasons set out above, it is submitted that the exemptions in s.24 and s.31 apply. The current national security threat is 'severe'. The most careful consideration should be given before releasing information to the world that could impact upon on the security of the nation or the ability of law enforcement to protect the public.

39. Furthermore, the arguments relied on by the Appellant as to the public's right to knowledge and ability to scrutinise are, in this arena, of minimal weight. Whilst the MPS acknowledges the fundamental importance of any matters that interfere (or have the potential to interfere) with the rights of privacy and free speech, including the right to free assembly, there are more than adequate protections in place more generally so that the public may have confidence in the oversight of any surveillance techniques without the need for the MPS to confirm or deny possession of the requested information. As set out in the MPS's refusal decision:

> There is also no requirement to satisfy any public concern over the legality of police operations and the tactics we may or may not use. Forces are already held to account by statute, for example the Police and Criminal Evidence Act and the Regulation of Investigatory Powers Act[1] and independent bodies such as Her Majesty's Inspectorate of Constabulary, the Independent Police Complaints Commission and the Office of the Surveillance Commissioner. Our accountability is therefore not enhanced by confirming or denying whether any information is held.

40. The MPS would further add that the use of any surveillance technique for the collection of evidence is subject to the scrutiny of the criminal courts.

41. In the circumstances, it is respectfully submitted that:

    (i) The public interest in maintaining the exemption is strong;

    (ii) It is of significantly more weight than the public interest in confirming or denying the existence of the information; and

    (iii) Any concerns around the oversight and accountability of surveillance techniques is amply dealt with without the need to respond to the information request.

[1] Recently, the statutory framework has been strengthened by the safeguards in the Investigatory Powers Act 2016

CONCLUSION

42. For the reasons set out above both appeals should be dismissed.

43. As set out in the Information Commissioner's decision, the MPS has relied on 'closed material' in support of its position. The MPS will seek to do so again in these Tribunal proceedings and will make an application at the appropriate time seeking permission under Rule 14 and Rule 35 to rely on closed evidence, make closed submissions, and for the Tribunal to consider evidence in private session.

Robert Talalay

Chambers of Jason Beer QC

5 Essex Court

Dated this 30th day of October 2018