Introduction

1. This is the Response of the Second Respondent to the appeal by Privacy International (hereinafter “the Appellant”) to the Decision Notice (hereinafter “the DN”) issued by the Information Commissioner (hereinafter “the Commissioner”) in respect of nine separate requests under the Freedom of Information Act 2000 (“the FOIA”).

2. This Response is produced in accordance with rule 23 of the Tribunal Procedure (First-Tier Tribunal) (General Regulatory Chamber) Rules 2009 (“the Rules”).

3. Although the Second Respondent is the direct subject of only one of the conjoined appeals, given the largely identical nature of the Appellant’s original requests, the material similarity of the DNs and of the grounds of appeal, the Second Respondent herein responds collectively to “the appeals.”
4. The Second Respondent endorses and adopts the use of the term “the Forces” for all the police forces and Police and Crime Commissioners for the reasons stated in footnote 1 of the Commissioner’s Response.

**Summary**

5. For the reasons stated herein, in the Second Respondent’s earlier responses to the Appellant’s FOI requests and in the Commissioner’s DN and appeal Response, it is submitted that the appeals should be dismissed in full.

**Relevant background**

6. The general background is covered fully in the Commissioner’s Response and is only set out in brief herein where it is specific to the Second Respondent.

7. The information request was sent by the Appellant to the Second Respondent on 1st November 2016. The request was for:

1. **Records relating to the purchase of CCDC equipment by Kent Police**, including purchase orders, invoices, contracts, loan agreements, solicitation letters, correspondence with companies and other similar records.

2. **Marketing or promotional materials received by Kent Police relating to CCDC equipment.**

3. **All requests by any corporation or any government agency to Kent Police to keep confidential any aspect of Kent Police’s possession and use of CCDC equipment**, including non-disclosure agreements between Kent Police and any corporation or government agency, regarding Kent Police’s possession and use of CCDC equipment.
4. Legislation, codes of practice, policy statements, guides, memoranda, presentations, training presentations or other records governing the possession and use of CCDC equipment by Kent 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.

8. The Second Respondent responded on 9th December 2016 and stated that it could neither confirm nor deny whether it has the information, citing the exemptions in sections 23(5), 24(2), 30(3) and 31(3) FOIA. The exemption in section 30(3) is no longer relied upon by the Second Respondent.

9. The Appellant subsequently requested an internal review of the decision. The Second Respondent carried out the requested review, and by letter dated 21st February 2017, confirmed its original decision.

10. Following the Appellant’s appeal to the Commissioner, the DN issued in respect of the appeal to the Commissioner against the Second Respondent’s refusal of the information request (“the request”) bears the number FS50728054.

The scope of the appeal

11. The Commissioner has found that the Second Respondent needs to disclose to the Appellant a limited amount of the information requested [DN 23], as below:

a) The marketing and promotional materials received by the Second Respondent in paragraph 7(2) above;

b) The legislation and codes of practice referred to in paragraph 7(4) above.

12. As anticipated in the Commissioner’s Response, the Second Respondent relies herein on the exemption in section 31(3) notwithstanding the Commissioner’s
decision not to consider it in the DN. As stated in paragraph 5 of the Commissioner’s Response, such reliance by the Second Respondent is entirely proper.

13. The issues for this appeal are therefore whether the Appellant has shown that the Commissioner erred in law in upholding the Second Respondent’s reliance on sections 23(5) and 24(2) in respect of the remaining information in this case, and whether reliance can be placed on section 31(3).

Response on Section 23(5) FOIA

14. So far as relevant, section 23 FOIA provides as follows:

“23.— Information supplied by, or relating to, bodies dealing with security matters.

(1) Information held by a public authority is exempt information if it was directly or indirectly supplied to the public authority by, or relates to, any of the bodies specified in subsection (3).

(2) A certificate signed by a Minister of the Crown certifying that the information to which it applies was directly or indirectly supplied by, or relates to, any of the bodies specified in subsection (3) shall, subject to section 60, be conclusive evidence of that fact.

(3) The bodies referred to in subsections (1) and (2) are—

(a) the Security Service,
(b) the Secret Intelligence Service,
(c) the Government Communications Headquarters,
(d) the special forces,
(e) the Tribunal established under section 65 of the Regulation of Investigatory Powers Act 2000,
(f) the Tribunal established under section 7 of the Interception of Communications Act 1985,
(g) the Tribunal established under section 5 of the Security Service Act 1989,
(h) the Tribunal established under section 9 of the Intelligence Services Act 1994,
(i) the Security Vetting Appeals Panel,
(j) the Security Commission,
(k) the National Criminal Intelligence Service,
(l) the Service Authority for the National Criminal Intelligence Service,
(m) the Serious Organised Crime Agency,
(n) the National Crime Agency,
(o) the Intelligence and Security Committee of Parliament.

[...]

(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).

Submissions

15. The point here is remarkably simple: given the obviously close working relationship between the Forces and the National Crime Agency, if the Second Respondent, or the Forces in general, confirmed their purchase and/or use of IMSI equipment, it would be patent that the section 23(3) agency above was also in possession of and using such equipment. Similarly, if the Second Respondent and/or the Forces denied the purchase and/or use of IMSI equipment, it would place into the public domain a high likelihood that the same was true of the section 23(3) agency above.

16. The Appellant continually asserts that it is insufficient for the Second Respondent to justify its reliance on the section 23(5) exemption on the basis of
hypotheticals. In its grounds of appeal, it asserts that the test is whether the information “relates” to one of the bodies listed in section 23(3), not whether the information “could relate”. It is trite to point out that should the Second Respondent respond in anything other than hypothetical terms, it would thereby inadvertently answer the Appellant’s request as to whether or not IMSI Catchers are used by the Force and by the agency in question. This would entirely defeat the purpose of the exemption by unintentionally putting into the public domain highly sensitive information regarding the surveillance tactics and equipment of the bodies charged with keeping UK residents safe. By phrasing the test in the way it has, the Appellant is clearly trying to obtain the information requested “by the back door”. For the reasons given, the only interpretation of the test to be applied under section 23(5) in this specific case is the one the Commissioner has applied in the DNs.

17. The Second Respondent’s case is further supported by an earlier judgment handed down by the First-Tier Tribunal which considered the correct interpretation of section 23(5). In Callus v The Information Commissioner and The Home Office, 6th May 2014, Case No. EA/2013/0159, the Tribunal heard argument as to the meaning of “relates to” the agencies in section 23(3). In the instant case, the Appellant argues [GA 32] that the section 23(5) exemption and the term “relates to” must be given a narrow meaning. On the question of whether “relates to” has a narrow or a broad meaning, the Tribunal held as follows:

“The expression “relates to” is a broad term, whatever its context, and does not require to be qualified by the addition of “directly”. While not following earlier First-tier Tribunal decisions as precedent, we agree with the general approach adopted by them to a provision which was clearly intended to provide security bodies with extensive protection from disclosure.” [para 39]

18. It is clear, therefore, that the Commissioner made no error in taking a broad approach to the exemption and to the need for the information request to “relate to” one or more of the section 23(3) agencies.
19. The Appellant equally argues that the Commissioner erred in considering the term “relates to” to mean that the requested information is “within the territory” of one of the security bodies. The First-Tier Tribunal equally considered this point in Callus. It held that:

“In our view the Information Commissioner was correct to base his decision on the broad principle that, to be exempt, the requested information would need to be “within the territory” of one of the security bodies.”

20. Following Callus, there was no error by the Commissioner in her interpretation of section 23(5) in the instant case. Information that, if disclosed, would by implication reveal a high probability that a highly specialist surveillance technique – IMSI - is or is not employed by the National Crime Agency, is unequivocally information that is “within the territory” of the security bodies.

21. The decision in Callus also supports the Second Respondent’s case on this point. Callus concerned a request for a list of Single Points of Contacts (SPoC) with responsibility for authorising the obtaining of telecommunications data for investigatory purposes. The First-Tier Tribunal held that the Commissioner, although correct in its interpretation of section 23(5), had misapplied it to the facts of Mr Callus’ request because a list of SPoC who might, at some future point, have some dealings with a specialist agency on the section 23(3) list was “too remote” to come within the section 23(5) exemption. The FTT stated that:

“We think that, although the Information Commissioner correctly identified the test to be applied he fell into error in his Decision Notice in its application to the facts of this case. The SPoC list contains information about individuals performing a particular role within the RIPA regime. Their actions may lead, on occasions, to a Security Body becoming involved in the broad investigation of which the acquisition of Communications Data was a part. In those and other circumstances an individual SPoC may find himself or herself working in cooperation with the staff of a Security Body. While information about those activities would certainly be properly described as relating to the Security Body,
22. The information requested by the Appellant of the Second Respondent relates to “activities” carried out by the Forces in the area of surveillance; the close relationship between the Forces and the National Crime Agency means those “activities” necessarily involve the “activities” of that specialist section 23(3) agency (and possibly others). As the FTT stated in Callus, “information about those activities would certainly be properly described as relating to the Security Body”. The section 23(5) exemption unambiguously applies in this case, and the Commissioner fell into no error in so concluding in the DN.

Response on section 24(2) FOIA

23. So far as relevant, section 24 FOIA provides as follows:

“24.— National security.

(1) Information which does not fall within section 23(1) is exempt information if exemption from section 1(1)(b) is required for the purpose of safeguarding national security.

(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.”

Submissions

24. The Second Respondent endorses the relevant principles set out at paragraphs 19-23 of the Commissioner’s Response. Three of them are cited at paragraphs 33(a), (b) and (c) of the Appellant’s Grounds of Appeal and the Second Respondent therefore takes no issue with these parts of the Grounds.
25. As a primary submission, the Second Respondent contends that at a time when the UK’s security alert is “severe” and the country is facing probably the most acute terror threat in its history, the mere fact of information entering the public domain as to whether or not police forces are in possession of specialist IMSI equipment that can be used to detect and prevent terror plots and other serious crimes undeniably compromises national security.

26. As cited at paragraph 19(4) of the Commissioner’s Response, there is a clear line of authority for the principle that national security “is a matter of vital national importance in which the Tribunal should pause and reflect very carefully before overriding the sincerely held views of public authorities” – see Quayum v Information Commissioner & The Foreign and Commonwealth Office [2012] 1 Info LR 332 at para 42. The sincerely held view of the Second Respondent is that the use of NCND as to whether or not it possesses IMSI equipment is required to safeguard national security. This is also clearly the sincerely held view of the other Forces conjoined in this appeal, and the sincerely held view of the Commissioner.

27. In terms of the principle cited at paragraph 33(a) of the Grounds of Appeal, as the Second Respondent has repeatedly stated to the Appellant in written correspondence, the information requested is of such a nature that the confirmation or denial itself would jeopardise national security. This is for the following reasons.

28. As the Appellant’s requests have been directed at multiple police forces, and no doubt would be sent to others if this appeal succeeds, a confirmation or denial would enable terrorists and serious criminals to build up a comprehensive national picture of which forces potentially do not have and use IMSI, and which potentially do. This would enable such groups and individuals to exploit possible weaknesses in the UK’s national security armour, and would therefore place the public at increased risk.

29. The Appellant asserts that because police forces use a variety of surveillance techniques to obtain operationally sensitive information, if a police force is
known not to have IMSI Catchers, it does not mean that it cannot obtain such information through other means. This assertion is completely flawed because it overlooks the fact that the raison d’être of IMSI Catchers is precisely because they can obtain information with the speed and accuracy that other covert surveillance techniques cannot do. IMSI Catchers are not interchangeable with or equal to other covert surveillance techniques. It is the sophistication and accuracy of IMSI Catchers which means that if a police force area, or the Forces as a whole, are known to use them, terrorists and serious criminals whose activities threaten national security will be able to plan to use tactics and technology to avoid being detected by them. Similarly, if a police force area, or the Forces as a whole, are known not to use IMSI Catchers whilst other areas are known to, the former risks being selected as a relatively easy target.

30. Furthermore, as the Second Respondent has also stated, the reliance on NCND in respect of the instant information request is a national response to a national security threat from terrorists and other serious criminals whose activities the IMSI Catchers could assist in detecting. This was recognised by the Commissioner in the DN, and as noted therein, it has also been found to be the case by the FTT which has held that “only a consistent use of a NCND response on matters of national security can secure its proper purpose” [DN 45]. Consequently, the Forces nationally are entirely justified in taking a common approach between them in the interests of national security.

31. The Appellant’s assertions that the Commissioner erred because she considered that the fact of IMSI constituting “covert surveillance” was enough to engage section 24(2), that she took a “blanket approach” and failed to scrutinise the request properly are unsustainable on the facts. It is patent from the DN that the Commissioner did not simply decide that the exemptions apply because IMSI can be categorised as “covert surveillance”. Rather, the fact of IMSI being “covert surveillance” was considered to be one of the factors indicating that the equipment could be used in the detection and prevention of the most serious crimes and terror plots, invariably involving section 23(3) agencies, and therefore revealing whether or not police forces possess IMSI equipment inevitably poses a risk to national security.
32. Further, in the DN, the Commissioner took issue with what she felt to be the “blanket approach” taken by the Forces in relying on the NCND exemptions in respect of all the information requested. Having taken this view, the Commissioner considered each type of information sought separately, and decided that some of them were not covered by the exemption. It is therefore apparent that the Commissioner has taken the exact opposite of “a blanket approach” to this case. Similarly, it is clear that she has fully scrutinised the information request and the relevant statutory provisions.

33. The Appellant is also mistaken in its contention that the test applied by the Commissioner to the application of section 24(2) was one of whether exempting the information ensures that “matters of interest to security bodies are not revealed” [DN 46]. Nowhere in the DN is it stated or implied that this was the test applied by the Commissioner; the fact of something being mentioned as a relevant consideration does not make it the overarching test that was applied. The Second Respondent considers that the Commissioner was simply stating that the fact that information requested relates to a matter of interest to security bodies is an indication that national security is engaged.

34. The Appellant additionally contends that the Commissioner’s approach is flawed because it has allowed the Forces to maintain NCND despite some Forces publicly confirming the existence of such information. Further, the Appellant claims that such information is already in the public domain through media reports.

35. These arguments are thoroughly misconceived. First, the statements made by Warwickshire and West Mercia do not, in the Second Respondent’s view, confirm or deny their possession and/or use of IMSI equipment. They imply at most that the future use of such equipment is contemplated. Second, even if they had confirmed its possession and use, or the reverse, that would not in any way undermine the lawfulness of other police forces relying on section 24(2) and NCND. The Appellant’s argument is in effect to contend that if one body reveals a piece of information, all other bodies in the same position must do likewise.
Such a proposition is obviously nonsense, the irony being that this argument proffers the taking of a “blanket approach” to the provision or withholding of information; precisely the conduct for which the Appellant criticises the Commissioner. Whilst the Second Respondent considers that each piece of information released by the Forces into the public domain regarding IMSI at this time compromises national security, it is trite that national security is safeguarded far more by the majority of forces applying NCND in this regard than none of them doing so.

36. Second, the parliamentary questions and speeches relied upon by the Appellant in its grounds [GA 11 and 20] do not, as the Commissioner correctly states in her Response [at 7], confirm or deny the use of IMSI in the UK by the Forces. They are simply general statements that do not reveal any sensitive matters that jeopardise national security.

37. The Appellant’s correct assertion that covert surveillance techniques such as IMSI can be used for ordinary law enforcement purposes takes their appeal nowhere. On this basis, all specialist technology and equipment used by the Forces would enter the public domain regardless of the impact on section 23(3) agencies, national security or any of the other exemptions in the FOIA simply because it is also used for purposes that do not engage these specialist bodies or considerations. This would significantly undermine the statute and its purpose.

38. Public bodies having previously admitted into the public domain the fact of other covert surveillance techniques being used, such as hacking and mobile phone data extraction, is not probative of whether information about the possession and use of IMSI Catchers should be provided by the Forces in the instant case. Such matters are clearly to be determined on a case-by-case basis and turn on their specific facts, together with the national security context at the time. It is trite that at a time of the UK’s security alert being “severe”, more stringent measures to safeguard national security are required than at times where the security threat is lower. The Appellant’s grounds entirely fail to acknowledge the context- and temporal-specific nature of dealing with
information requests which engage questions of national security and the public interest.

The public interest test

39. The Appellant is correct to assert that section 24 does not carry “inherent weight” per the Upper Tribunal’s decision in *Keane v Information Commissioner, The Home Office & The Metropolitan Police Service* [2016] UKUT 461 (AAC). Nevertheless, the Upper Tribunal gave a very clear statement of great relevance to the instant case, that:

“the reality is that the public interest in maintaining the qualified security interest in section 24(1) is likely to be substantial to require a compelling competing public interest to equal or outweigh it” (para 46).

40. While the Second Respondent acknowledges the important public interest in the protection of privacy and promotion of openness and transparency, it is submitted that at a time of extreme insecurity and heightened terror threat, the overriding public interest in this case lies in the safeguarding of national security. As the Commissioner puts it in her Response, the considerations advanced by the Appellant are “weighty ones”, however the safeguarding of national security is a “contextually very weighty one”. The Second Respondent submits that this is entirely correct – safeguarding national security at the present time involves protecting UK residents from a high threat of death and/or serious physical injury. Considerations of transparency, accountability and privacy, whilst obviously very significant matters of public interest, do not equal or outweigh the public interest in protecting human life in the face of a concerted and sophisticated effort to kill, maim and injure through terror attacks and other serious crime.

41. Further, as the Commissioner avers in her Response, the public interest in a debate about covert surveillance techniques used by the Forces is mitigated by there already being sufficient information in the public domain about the existence and potential use of these techniques for a debate to have been
triggered. However, per the case of Savic v Information Commissioner, Attorney General’s Office and Cabinet Office [2016] UKUT 535 (AAC), the Upper Tribunal has held that it is inappropriate for the Commissioner or the Tribunal to assess the appropriateness of the reliance on NCND by reference to the substantive information in the request. The question is whether the countervailing public interest lies in the public having a “yes” or “no” answer to the request, and not in the underlying information being revealed [at paras 47-48].

42. In the instant case, it is submitted that the public interest in knowing whether or not the Second Respondent and/or any other Forces possess information on the purchase and use of IMSI Catchers is far outweighed by the harm this would cause to national security. The “yes” or “no” answer would not in itself contribute greatly to the public debate that is already taking place. By contrast, it would indicate to terrorists and other serious criminals whether or not such equipment is used and enable them to adapt their tactics accordingly and exploit any potential weaknesses in the UK’s security armour.

43. As above, it is not essential for it to be known whether particular Forces, or the Force as a whole, are actually in possession of such equipment in order for the use of IMSI Catchers to be discussed and considered in the public domain. The relevant legislation being in the public domain, it is perfectly possible for the public to know and debate how IMSI Catchers might be used, and to make representations to their elected members on this if they feel so inclined.

44. The Second Respondent fully endorses paragraph 40 of the Commissioner’s Response and the assertion that in the specific context of this case, the release into the public domain of the existence of policy statements and guidance on the use of IMSI Catchers would in itself provide a strong indication of their use by the Force(s) in question. As above, this would undermine national security by enabling terrorists and other serious criminals to ‘map’ the possession and use of such equipment across the UK and to adapt their tactics accordingly.
45. For all the reasons above, the Second Respondent submits that the Commissioner correctly applied the public interest test on the facts of this case.

Response on section 31(3) FOIA

46. So far as relevant, section 31 FOIA provides that:

“31.— Law enforcement.

(1) Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice—

(a) the prevention or detection of crime,
(b) the apprehension or prosecution of offenders,
(c) the administration of justice,
(d) the assessment or collection of any tax or duty or of any imposition of a similar nature,
(e) the operation of the immigration controls,
(f) the maintenance of security and good order in prisons or in other institutions where persons are lawfully detained,
(g) the exercise by any public authority of its functions for any of the purposes specified in subsection (2) […]

(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).

47. As stated above, the Second Respondent relies in addition on the exemption in section 31(3) FOIA for the following reasons.

48. If the Second Respondent were to affirm or deny its possession and/or use of IMSI Catchers, this would significantly prejudice the prevention and detection of terrorist and other serious criminal activities. Section 31(1)(a) is therefore
engaged in this case. Similarly, there would be significant prejudice to the Forces’ exercise of its crime prevention and activities under section 31(1)(a) above due to the information being in the public domain. This is for essentially the same reasons as stated in respect of the other two exemptions relied upon in this case, namely that the information in question – the mere confirmation or denial that such information exists - would enable terrorists and other serious criminals to build a map of which Force areas possess and/or use IMSI Catchers, and which do not. If it was revealed that some Forces use the equipment and others do not, this would enable terrorists and others to target and exploit any areas where IMSI Catchers are not used, and to modify their activities to avoid detection by IMSI Catchers in any areas where the equipment is used. It would therefore create a real and significant, not remote or theoretical, risk of such activities going undetected and human life being endangered. It would cause substantial prejudice to the Force’s law enforcement activities and to law enforcement itself (s. 31(1)(a)).

49. Support for the Second Respondent’s position can be derived from the Court of Appeal’s decision in the case of Willow v The Information Commissioner & The Ministry of Justice [2017] EWCA Civ 1876. Mrs Willow, an experienced social worker, sought the disclosure of an unredacted version of a Ministry of Justice manual detailing restraint techniques to be used in Secure Training Centres for juvenile offenders. She argued that it was necessary in the public interest for reasons of transparency and to ensure that young people were treated humanely and decently. This was in the context of two deaths of youths in Secure Training Centres during or following physical restraint. It is therefore clear that there was heightened public interest in disclosure at the time.

50. The MOJ refused, relying on section 31(1)(f) FOIA, and contending that the disclosure of the unredacted copy, and thereby the detail of the restraint techniques, would enable juvenile offenders to develop countermeasures that could result in an increase in violence and insecurity in STCs. The MOJ further argued that the techniques were also used with older young offenders in Young Offenders Institutions, and were also similar to control and restraint techniques applied in adult prisons. Disclosure of the information would therefore
significantly prejudice the maintenance of good order in penal institutions across the country by, as in the instant case, allowing the development of countermeasures to subvert the techniques in question.

51. Mrs Willow countered this, in the same manner as the Appellant, by contending that there was no evidence that the disclosure of previous manuals had led to the development of any such countermeasures. Nevertheless, the FTT, the UT and the CA all agreed with the MOJ and with the Commissioner that the disclosure of the unredacted manual and therefore the detail of the techniques would be likely to cause real and significant prejudice to the maintenance of good order, such that the MOJ could rely on section 31(1)(f).

52. Willow demonstrates that the likely development of countermeasures to security techniques deployed by law enforcement agencies is a valid reason for the application of the exemption in section 31(3). It further demonstrates that such a justification, which engages security and order nationally, outweighs a compelling public interest in transparency, even in a situation where young people have died through the application of measures of the type being withheld. Willow is therefore binding authority that is strongly supportive of the Second Respondent’s case on this point.

53. The Second Respondent notes the Commissioner’s endorsement of the Second Respondent’s reliance on section 31(3) FOIA expressed in paragraphs 45-46 of its Response, and agrees with the observations stated therein.

Conclusion

54. For all the reasons stated herein above, the Tribunal is invited to dismiss the appeals.
Procedural matters

55. The Second Respondent shares the Commissioner’s view that an oral hearing is required.

FRANCES LAWSON
22nd October 2018

Chambers of Stephen Hockman QC
Six Pump Court
Temple
London
EC4Y 7AR