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

B E T W E E N :

PRIVACY INTERNATIONAL

Appellant

-and-

THE INFORMATION COMMISSIONER'S OFFICE

Respondent

GROUNDS OF APPEAL[1]

A. Introduction and Summary

1. The Appellant is Privacy International, a UK-registered charity which was founded in 1990 to campaign for the protection of the right to privacy at an international level.

2. On 1st November 2016, Privacy International wrote to a number of police forces, Police and Crime Commissioners ("**PCC**"), and other public bodies to seek information relating to the purchase and use of mobile surveillance equipment and the regulatory and oversight regime that exists to monitor the use of such equipment. Such equipment can be referred to using a range of terms, including "Covert Communications Data Capture" ("**CCDC**") equipment, "International Mobile Subscriber Identity ("**IMSI**") Catchers", "IMSI Grabbers", "Cell site simulators", and "Stingrays". For the purpose of these grounds, the Appellant refers to such equipment as "**IMSI Catchers**".

[1] These grounds of appeal are served in nine different appeals (appealing, respectively, ICO Decision Notices with reference numbers FS50728051, FS50728052, FS50728053, FS50728054, FS50728055, FS50728056, FS50728057, FS50728058, FS50728059). Given the overlapping issues and reasons, the Tribunal is respectfully invited to case-manage these appeals together.

3. Each of the police forces and public bodies who responded refused to confirm or deny that they held the information requested by the Appellant (both initially and after a second internal review). They relied on exemptions from having to confirm nor deny under ss.23(5), 24(2), s.30(3), and/or 31(3) Freedom of Information Act 2000 ("**FOIA**").

4. Two public bodies, West Mercia PCC and Warwickshire PCC, confirmed that they held a business case relating to the purchase of IMSI Catchers, which they refused to disclose due to exemptions under ss.24(1) and 31(a) and (b) FOIA. They refused to confirm or deny that they held other information requested by the Appellant.

5. Following appeals from the Appellant, the Respondent upheld the refusal notices in part on 10th July 2018.[2] The Respondent held that each of the police forces and public bodies was entitled to rely on ss.23(5) and/or 24(2) FOIA to refuse to confirm or deny whether they held the requested information.

6. This decision was wrong and/or unlawful, in that:

   a. The Respondent erred in its interpretation of the s.23(5) exemption. The words, "*relates to"*, should be given a narrow construction;

   b. The Respondent erred in concluding that the s.24(2) exemption was "*required for the purpose of safeguarding national security*", particularly as regards the policy and/or other records describing the safeguards regulating any use of IMSI Catchers;

   c. The Respondent erred in concluding that, in all the circumstances of the case, the public interest in maintaining the s.24(2) exemption outweighs the public interest in confirming or denying that the information requested was held (s.2(2)(b) FOIA).

[2] The Respondent upheld the Appellant's appeals in respect of some parts of the request. This appeal relates to those parts of the appeals that were rejected by the Respondent. The Appellant reserves its right to update and/or amend these grounds on receipt of any information disclosed by, or a fresh response received from, the police forces and public bodies following the Respondent's direction to them (to confirm or deny whether certain information is held, and either disclose it or issue a fresh response compliant with s.17 FOIA).

7. In respect of two public authorities, Warwickshire PCC and West Mercia PCC, the Respondent held that they were entitled to rely on s.24(1) FOIA to refuse to provide the business cases. This decision was wrong and/or unlawful in that:

   a. The Respondent erred in concluding that the s.24(1) exemption applied;

   b. The Respondent erred in concluding that, in all the circumstances of the case, the public interest in maintaining the s.24(1) exemption outweighs the public interest in disclosing the information (s.2(2)(b) FOIA).

B. The Facts

i. The Appellant

8. Privacy International was founded in 1990. It is a UK-registered charity campaigning for the protection of the right to privacy at an international level. It focuses, in particular, on tackling the unlawful use of surveillance. It is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised, and reported to, among others, the Council of Europe, the European Parliament, the Organisation of Economic Co-operation and Development, and the United Nations.

9. The Appellant's primary aims are to raise awareness about threats to privacy, to monitor and report on surveillance methods and tactics, to work at national and international levels to ensure strong privacy protection, and to seek ways to protect privacy in the context of the use of technology. Recent cases brought by the Appellant include a challenge to the lawfulness of the bulk interception of internet traffic by the UK security and intelligence services (*10 Human Rights Organisations v United Kingdom*) (App. no 24960/15)) and a challenge to the blanket exemption of the Government Communications Headquarters under FOIA (*Privacy International v the United Kingdom* (App. no. 60646/14)).

ii. IMSI Catchers

10. IMSI Catchers are surveillance devices used to collect mobile phone data and track individuals' locations. IMSI stands for "*International Mobile Subscriber Identity*", a number unique to Subscriber Identification Module ("**SIM**") cards.[3] Mobile phones communicate with a network of base stations, which enable the network provider to route calls, text messages and internet data to and from the mobile phone. IMSI Catchers function by impersonating a base station, tricking all mobile phones within their radius into connecting to them. Once connected to an IMSI Catcher, mobile phones identify themselves by revealing their IMSI. This identification process also allows IMSI Catchers to determine the location of mobile phones. Some IMSI Catchers also have the capability to intercept communications and data, including calls, text messages, and internet data, or even manipulate them, by editing or rerouting them. Some IMSI Catchers block service, either to all mobile phones within their range or to select devices.

11. The use of IMSI Catchers by police forces and other public bodies in the UK has long aroused public concern. On 2nd July 2015, David Davis MP asked the Secretary of State for the Home Department to clarify under what statute and what warranty system the use of IMSI Catchers is permitted to intercept communications and communications data. A Minister of State within the Home Office responded on 7th July 2015:

> "*The Wireless Telegraphy Act 2006 makes it an offence for a person to interfere with wireless telegraphy or to use wireless telegraphy with intent to obtain information as to the contents, sender or addressee of a message of which neither he nor a person on whose behalf he is acting is an intended recipient, without lawful authority.*
>
> *"Investigative activity involving interference with property or wireless telegraphy is regulated by the Police Act 1997 and the Intelligence Services Act 1994 which sets out the high level of authorisation*

[3] IMSI Catchers typically also collect the "*International Mobile Station Equipment Identifier*" ("**IMEI**") of mobile phones. The IMEI is unique to each mobile phone whereas the IMSI is unique to each SIM card.

required before the police or security and intelligence agencies can undertake such activity. Use of these powers is overseen by the Intelligence Services Commissioner and the Office of Surveillance Commissioners.

"Interception of communications in the course of their transmission is governed by the Regulation of Investigatory Powers Act 2000."[4]

12. There was no suggestion on the part of the Home Office that this answer was in any way operationally sensitive.

13. The use of IMSI Catchers has also been publicly confirmed in other countries in Europe, such as Germany, where their use is regulated by federal law and subject to a series of safeguards. Those safeguards include requiring prior judicial authorisation for law enforcement agencies' use of IMSI Catchers and only where there are grounds indicating that an individual has committed or is going to commit a specific serious crime and only to the extent necessary to determine that individual's mobile IMSI/IMEI or whereabouts.[5] In the United States of America, the Department of Justice has also confirmed the use of IMSI Catchers, announcing a policy requiring that all agencies obtain a search warrant supported by probable cause prior to using an IMSI Catcher.[6]

14. On 11th October 2011, *The Guardian* reported that the Metropolitan Police Service ("**MPS**") had acquired an IMSI Catcher from a Leeds-based company, Datong plc.[7]

15. On 10th June 2015, the BBC reported that a German security company had uncovered direct evidence of at least 20 instances of the use of IMSI Catchers in London.[8]

16. On 14th June 2016, VICE News reported that it had found evidence that IMSI

[4] Available online at: https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2015-07-02/5369
[5] Section 100i of the *Criminal Procedure Code* (*Strafprozessordnung*, StPO) (Germany): https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html.
[6] 2015 U.S. Department of Justice Policy, https://www.justice.gov/opa/file/767321/download.
[7] https://www.theguardian.com/uk/2011/oct/30/metropolitan-police-mobile-phone-surveillance
[8] https://www.bbc.co.uk/news/business-33076527

Catchers were being used in London, including at a protest.[9]

17. On 10th October 2016, the media cooperative, *The Bristol Cable,* published an article entitled: "*Revealed: Bristol's police and mass mobile phone surveillance*."[10] The article cited evidence that seven police forces had purchased IMSI Catchers (Avon and Somerset, MPS, South Yorkshire, Staffordshire, Warwickshire, West Mercia and West Midlands). In particular, it made reference to the unredacted minutes of an Alliance Governance Group meeting in May 2016 between Warwickshire and West Mercia Police in which the two police forces discussed the recent purchase and use of CCDC equipment. The minutes also referenced the purchase and operation of IMSI Catchers by Staffordshire and West Midlands Police. These minutes remain available online.[11] The article also cited publicly available procurement data revealing that Avon and Somerset Police have previously paid a private company, CellXion, the sum of £169,575.00 for "*CCDC equipment*" and other "*communications and computing equipment*", and that the MPS also awarded CellXion a contract worth over £1,000,000 for CCDC equipment in 2015. These procurement records also remain available online.[12]

18. On the same day, *The Guardian* published an article entitled: "*Controversial snooping technology 'used by at least seven police forces'*".[13] This article reported that a "*surveillance technology that indiscriminately harvests information from mobile phones*", also "*known as an IMSI catcher*", was being "*used by at least seven police forces across the country...according to police documents*." It quoted from John Campion, the West Mercia PCC, who said: "*It is absolutely appropriate that the police can make use of this technology in order to keep people safe. It is very important to me that civil liberties are upheld and respected. I am reassured on behalf of our local communities that the safeguards and processes in place will ensure this technology will be used appropriately and proportionately.*" It also quoted from Matthew Ellis, the then PCC for Staffordshire, who said: "*It is right that police have the tools to tackle the complex nature of crime in the 21st century. Some tactics police*

[9] https://news.vice.com/video/phone-hackers-britains-secret-surveillance
[10] https://thebristolcable.org/2016/10/imsi/
[11] https://thebristolcable.org/wp-content/uploads/2016/10/09-imsi-4.pdf
[12] https://thebristolcable.org/wp-content/uploads/2016/10/09-imsi-2.pdf; https://thebristolcable.org/wp-content/uploads/2016/10/09-imsi-3.pdf
[13] https://www.theguardian.com/world/2016/oct/10/controversial-phone-snooping-technology-imsi-catcher-seven-police-forces

use to keep people safe and bring criminals to justice can be intrusive and it is crucial that there are robust safeguards, framed by legislation, around this work, and there are."

19. On 28th October 2016, the South Yorkshire PCC attended a police and crime panel, at which he was asked a series of questions about the use of IMSI Catchers. Although the South Yorkshire PCC purported not to confirm or deny the approval or purchase of IMSI Catchers, he did provide detailed answers in respect of their oversight. His answers implied that South Yorkshire Police had used IMSI Catchers. For example, he explained what he saw as oversight mechanisms for the use of IMSI Catchers and suggested that "*South Yorkshire Police had received an outstanding grading in the inspection of this area of policing."* He also purported to correct what he saw as misconceptions about how IMSI Catchers worked and purported to set out how the use of IMSI Catchers could be "*undertaken by the police."*[14]

20. On 8th January 2018, Thangam Debbonaire MP asked the Secretary of State for the Home Department which police forces own an IMSI Catcher. A Minister of State in the Home Office provided the following answer on 11th January 2018:

> *"The Wireless Telegraphy Act 2006 makes it an offence for a person to interfere with wireless telegraphy or to use wireless telegraphy with the intent to obtain information as to the contents, sender or addressee of a message of which neither he nor a person on whose behalf he is acting is an intended recipient, without lawful authority.*
>
> *"Investigative activity by public authorities involving interference with property or wireless telegraphy is regulated by the Police Act 1997 and the Intelligence Services Act 1994, which set out the high level of authorisation required before law enforcement or the security and intelligence agencies can undertake such activity. The covert surveillance and property interference code of practice provides guidance on the use of these powers.*

[14] https://doncaster.moderngov.co.uk/documents/s9940/PCC%20Minutes%20281016.pdf

"In addition, the Investigatory Powers Act 2016 will regulate the interference with equipment for the purpose of obtaining communications, equipment data or any other information. These provisions will come into force later this year, and further guidance will be provided in a statutory code of practice.

"The use of all covert investigatory powers is overseen by the Investigatory Powers Commissioner.

"Ownership and operation of such devices by police forces and other public authorities is an operational matter for them.

iii. The Request for Information

21. On 1st November 2016, Matthew Rice, who was then an employee of the Appellant, wrote to the National Police Chiefs' Council ("**NPCC**"), Home Office, National Crime Agency ("**NCA**"), MPS, South Yorkshire Police, Avon and Somerset PCC, Kent PCC, Staffordshire PCC, West Midlands PCC, West Mercia PCC and Warwickshire PCC requesting information about the purchase and use of mobile phone surveillance equipment by the police forces and the regulatory and oversight regime that exists to monitor the use of such equipment. These grounds of appeal will focus on the request made to the MPS. This is because the Respondent adopted the MPS decision notice as the "*lead decision"* in respect of the exemptions under ss.23(5) and 24(2) FOIA. Where a relevant difference in the request history arises, this will be set out below.

22. The Appellant requested the following information from the MPS:

a. Purchase orders, invoices, contracts, loan agreements, solicitation letters, correspondence with companies and other similar records regarding the MPS' acquisition of IMSI Catchers, including records of all purchase orders, invoices, contracts, agreements, and communications with CellXion;

b. Marketing or promotional materials received by the MPS relating to IMSI Catchers;

c. All requests by CellXion or any other corporation or any government agencies to the MPS to keep confidential any aspect of the MPS' possession and use of IMSI Catchers, including any non-disclosure agreements between the MPS and CellXion or any other corporation or government agency regarding the MPS' possession and use of IMSI Catchers;

d. Legislation, codes of practice, policy statements, guides, manuals, memoranda, presentations, training materials or other records governing the possession and use of IMSI Catchers by the MPS, 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 IMSI Catchers may be revealed to the public, criminal defendants, or judges.

23. The Appellant's requests to the other police forces and public bodies matched the request to the MPS, except in the following ways:

a. The Appellant requested similar information from Warwickshire PCC with two exceptions. First, as regards the request set out at §22(a), above, the Appellant did not make a general request for records regarding Warwickshire PCC's acquisition of IMSI Catchers. Rather, the Appellant specifically requested records relating to the purchase of existing and replacement IMSI Catchers, and the decision to replace the existing equipment with a new supplier, referred to in the Alliance Governance Group minutes. Second, the request did not include the requests set out above, at §22(b) and (c);

b. The Appellant's request to West Mercia PCC was substantively similar to the request to Warwickshire PCC. In addition, the request also included a request for records relating to the "*safeguards and processes in place*" governing IMSI Catchers, that was referred to in *The Guardian* article (set out above, at §18). The Respondent adopted the Warwickshire decision notice as the "*lead decision*" with respect to its reasoning on the specific issue of the business case;

c. With respect to the Appellant's request to Staffordshire PCC, the request also included a request for records relating to "*robust safeguards*" and "*legislation*" to govern the use of IMSI Catchers by Staffordshire Police, that was referred to in *The Guardian* article (set out above, at §18). Like the request to Warwickshire and West Mercia PCCs, the request to Staffordshire PCC also did not include the requests set out above, at §22(b) and (c);

d. The Appellant's request to West Midlands PCC also did not include the requests set out above, at §22(b) and (c).

24. On 29th November 2016, the MPS informed the Appellant that it could neither confirm nor deny the existence of information relevant to the request, citing the exemptions at ss.23(5), 24(2), 30(3) and 31(3) FOIA. On 24th January 2017, the Appellant requested an internal review of that decision. On 12th June 2018, the MPS upheld its decision. During the Respondent's investigation, the MPS withdrew its reliance on s.30(3).

25. Some police forces did confirm that they held relevant information:

a. On 20th December 2016, Warwickshire PCC stated that it held a small amount of relevant information – namely, "*a business case regarding the replacement of existing CCDC equipment*" – but that such information was exempt from disclosure pursuant to ss.24(1) and 31(1)(a) and (b). It would neither confirm nor deny holding any information in respect of the equivalent requests to those set out at §22(d), above, citing s.23(5);

b. On 20th December 2016, West Mercia PCC informed the Appellant that it held a small amount of relevant information – namely, "*a business case regarding the replacement of existing CCDC equipment*" – but that such information was exempt from disclosure pursuant to ss.24(1) and 31(1)(a) and (b). It would neither confirm nor deny holding any information in respect of the equivalent requests to those set out at §22(d), above, citing s.23(5).

26. The Appellant wrote to the Respondent to bring appeals against each of the refusals. Given the similarity of the requests for information to the various public bodies, the Appellant invited the Respondent to consider all of the requests at the same time.

C. The Decision Under Challenge

27. On 10th July 2018, the Respondent refused the Appellant's appeals in respect of each of the public bodies who had rejected the Appellant's information requests (save for the limited parts of the appeals that were upheld, detailed below). The reasoning in respect of the decisions was essentially identical, save where set out below. Unless expressed to be otherwise, paragraph references in these grounds are references to paragraphs in the Respondent's decision in respect of the MPS.

28. The Respondent relied, in its decision in respect of the MPS, on material and information supplied "*in confidence"* by the MPS to the Respondent (decision, at §56). The Appellant has been provided with no explanation as to the nature of that material or as to the legal basis upon which the Respondent can lawfully resolve an information appeal on the basis of such "*confidential material"*. The Respondent has no statutory power to consider "*confidential material"*[15] and it is plainly procedurally unfair for it to do so.[16] The scheme of FOIA is aimed at ensuring that appellants do not have to litigate their requests through time and resource-consuming litigation. It is unfair for the Respondent to resolve an appeal without giving the Appellant an opportunity to understand the nature of or comment on the central material.

29. The reasons for the Respondent's decision were, in summary:

    a. The request set out at §22(b), above, seeks details regarding any marketing or promotional materials relating to IMSI Catchers which the MPS may have received. The Respondent did not accept that any of the

[15] In contrast to the Tribunal (r.14(6), Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009) and the Upper Tribunal (r.37 Tribunal Procedure (Upper Tribunal) Rules 2008).

[16] See, by analogy, the guidance provided by the Scottish Information Commissioner: "*A guide for applicants: What happens next?"*, at §14, available at: http://www.itspublicknowledge.info/nmsruntime/saveasdialog.aspx?lID=6362&sID=8727.

exemptions cited in a "*blanket*" fashion could properly apply to such material and found that confirmation or denial as to the receipt of such material does not reveal whether or not the MPS actually purchased any equipment (§20). As such, the MPS had to confirm or deny whether any information was held, and either disclose it or issue a fresh response compliant with s.17 FOIA (§23);

b. Some of the request at §22(d), above, refers to legislation and codes of practice which would cover the use of IMSI Catchers. The Respondent held that either legislation does or does not exist and, if it does, "*it clearly cannot be exempt under FOIA as it would be statute which should be publicly available, and this would be the same for codes of practice*" (§21). None of the exemptions relied upon were appropriate to justify the non-disclosure of legislation and codes of practice. The MPS therefore had to confirm or deny whether any information was held, and either disclose it or issue a fresh response compliant with s.17 FOIA (§23);

c. The absolute exemption set out at s.23(5) has a *"very wide application. If the information requested is within what could be described as the ambit of security bodies' operations, section 23(5) is likely to apply"* (§32);

d. *"The equipment being considered here is covert surveillance equipment and, put simply, the Commissioner is trying to establish the likelihood as to whether or not the use of such equipment could 'relate to' any of the security bodies; this is all she is required to do. As it is covert equipment, the Commissioner considers it is considerably more likely to 'relate' to security bodies, and if it is used, it could realistically be deployed in joint operations between the police service and security bodies."* Regarding the standard of proof of disclosure, the Respondent held that *"if it is more likely than not that the disclosure would relate to a security body then the exemption would be engaged"* (§42);

e. Following this interpretation, if information about IMSI Catchers is held, it could be related to one or more of the s.23 bodies and therefore the exemption is engaged;

f. The exemption in s.24(2) was interpreted *"so that it is only necessary for a public authority to show either a confirmation or a denial of whether requested information is held would be likely to harm national security"* (§45);

g. National security extends to ensuring that *"matters which are of interest to the security bodies"* are not revealed (§46);

h. "*If the MPS does have its own guidance then revealing this would indicate that it does use CCDC equipment, which would go against the NCND stand it has adopted here. Also, if the use of such equipment were not fully legislated for, then this will be determined by courts at some future date if evidence is gathered using this methodology"* (§50);

i. The public interest favours maintaining the exclusion from confirming or denying provided by s.24(2) (§60). It is important to note that the Respondent adopted this approach even where a public body (such as the Staffordshire PCC) had publicly stated that "*robust safeguards"* existed as regards the use of IMSI Catchers;

j. The Respondent made no decision in respect of ss.30(3) or 31(3) (§61).

30. Where Warwickshire PCC and West Mercia PCC confirmed that they held one piece of the information requested, namely *"a business case regarding the replacement of existing CCDC equipment",* the Respondent upheld the reliance on s.24(1).[17] The reasons for the Respondent's decision in this regard were, in summary:

a. In order for the s.24 exemption to apply, "*It is not necessary to show that disclosing the withheld information would lead to a direct threat to the United Kingdom"* (§27);

b. The s.24 exemption is engaged as a result of reasons arising out of the "*confidential material*" referred to at §28 above (§32);

[17] Decision Notices FS50728057 and FS50728058.

c. The Respondent noted that Warwickshire PCC had confirmed that some information is held, but only because of an *"unintentional disclosure on a website*". Any related information has since been redacted (§32); and

d. The balance of the public interest falls in favour of "*the public interest in safeguarding national security*" (§34). The Respondent recognised that there is a public interest in disclosure, but held that this was outweighed by the national security level of risk being set at "*severe*", and arguments put forward by the public authorities in a confidential setting (§40).

D. The Appeal

31. The Respondent's notices in respect of the each of the police forces and/or PCCs were not in accordance with the law. Further, the Respondent came to the wrong judgement in relation to the balance of the public interest. Finally, the findings on which the Respondent's notice was based were wrong and predicated on a series of *non-sequiturs*. The Tribunal is therefore respectfully invited to allow the appeal pursuant to s.58 FOIA. Without prejudice to the generality of those submissions, it is submitted in particular that:

32. **Firstly**, the Respondent erred in its interpretation of the s.23(5) exemption:

a. The exemption set out in s.23(5) is absolute;

b. Any absolute exemption ought to be construed narrowly. This is because of the following:

i. The "*default setting*" in FOIA is in favour of disclosure;[18]

ii. Any absolute exemption is a serious interference with common law information rights;[19]

iii. Any absolute exemption is also a serious interference with the rights of applicants under Article 10 of Schedule 1 of the Human

[18] *Galloway v Information Commissioner v The Central and North West London NHS Foundation Trust* (2009) 108 BMLR 50, at §70.
[19] *Kennedy v Information Commissioner* [2015] AC 455.

Rights Act 1998 to obtain information. In *Magyar Helsinki Bizottsag v Hungary* (App. no. 18030/11), the Grand Chamber confirmed that the right of access to information forms part of the right to Article 10, particularly where the individual is seeking access to information "*on matters of interest for society as a whole"*, (§161), and with a view to informing the public in a capacity as a public or social watchdog, (§167), as in this appeal. The Grand Chamber specifically referred to a previous decision, in which the European Court had previously found that the denial of access to information concerning the use of electronic surveillance measures constituted an interference with Article 10 (§160).[20]

c. There is no authority supporting the Respondent's construction of s.23(5), which is that it only requires a public body to show, on the balance of probabilities, that "*the use of such equipment could 'relate to' any of the security bodies."* There is no support for this construction in the authority cited[21] and the Respondent's own guidance recognises that its phrase, "*in the territory of national security"*, is "*a phrase used by the ICO. It does not appear in the legislation and has not been routinely used by the Tribunal or by public authorities*";[22]

d. The Respondent's construction is inconsistent with the wording of s.23(5). The exemption set out in s.23(5) applies to "*information … which … relates to … any of the bodies specified"*. It does not apply to information which "*could"* relate to any of the security bodies (§38);

e. "*Relates"* is an ordinary English word, which means "*connected to"*. Information must actually be connected to the security bodies to fall within s.23(5). The theoretical possibility that information may fall within the territory of a security body is insufficient. This stretches the ordinary language of the statute too far;

---

[20] See, further, *Társaság a Szabadságjogokért v Hungary* (2009) 53 EHRR 130, at §38; and *Youth Initiative for Human Rights v Serbia* (App. no. 48135/06), at §24.

[21] *Commissioner of Police of the Metropolis v Information Commissioner* (EA/2010/0008), which touches only on the standard of proof.

[22] ICO Guidance: "*Security bodies (section 23)"*, at footnote 1, available at: https://ico.org.uk/media/for-organisations/documents/1182/security_bodies_section_23_foi.pdf.

f. The Respondent's construction opens s.23(5) up to absurd interpretations. There are many techniques, ranging from the simple to the sophisticated, that both police forces and the s.23(3) bodies may deploy. The Respondent's interpretation would bring all such techniques outside the scope of disclosure under FOIA;

g. The Respondent's construction is inconsistent with its own decision. The Appellant's requests for legislation and codes of practice plainly also falls within the category of material that "*could relate to any of the security bodies"*, and yet the Respondent has rejected any reliance on s.23(5) in this regard.

33. **Secondly**, the Respondent wrongly concluded that the s.24(2) exemption from s.1(1)(a) was "*required for the purpose of safeguarding national security*":

a. In s.24(2) cases, what is in issue is not the impact of disclosing the material requested itself, but rather the impact of simply confirming whether or not the information is held. This reflects the language of the statute, which requires it to be shown that "*exemption from section 1(1)(a) is required for the purpose of safeguarding national security."* This submission also reflects the Upper Tribunal's approach to the public interest balancing exercise in neither confirm nor deny cases;[23]

b. "*Required*" in this context "… *means reasonably necessary. It is not sufficient for the information sought simply to relate to national security; there must be a clear basis for arguing that disclosure would have an adverse effect on national security before the exemption is engaged*".[24] Applying this *dicta* to the facts of this case, there must be a clear basis for arguing that merely confirming whether or not the material sought is held would have an adverse effect on national security in order to engage s.24(2);

[23] *Savic v Information Commissioner and others* [2016] UKUT 535 (AAC), at §70.
[24] *Philip Kalman v Information Commissioner and the Department of Transport* (EA/2009/111 8 July 2010).

c. It is therefore clear that a decision to "*neither confirm nor deny"* requires a clear justification and merits close scrutiny. This submission reflects the approach taken to "*neither confirm nor deny"* in parallel contexts. A decision to "*neither confirm nor deny"* "… *requires justification similar to the position in relation to public interest immunity ... It is not simply a matter of a governmental party to litigation hoisting the NCND flag and the court automatically saluting* it". This *dicta* reflects the requirements of the rule of law: in order for this Tribunal to be satisfied that the s.24(2) exemption has been appropriately relied upon, the Tribunal must scrutinize this issue with particular care. Otherwise, there would be a weakening of public trust in the proper oversight of the FOIA regime;[25]

d. The Respondent failed to approach the decisions under challenge in these appeals with sufficient scrutiny. Rather, the Respondent appears to have been satisfied that the decisions were justified given that they related to a "*covert surveillance"* technique. Such a blanket approach is inconsistent with the requirements of s.24(2);

e. The test adopted by the Respondent, namely "*ensuring that matters are of interest to the security bodies are not revealed"* (decision, at §46) is not the application of the test in the statute. The statute requires an analysis of what the material is and how and to what extent its disclosure would have an adverse impact on national security. The fact that information sought falls within the territory of, or is *"of interest to",* the security bodies is not enough and is impermissibly wide;

f. The fallacy of the Respondent's approach is underlined by the fact that it has permitted public bodies to neither confirm nor deny the existence of information sought even in circumstances in which public bodies have publicly confirmed the existence of such information:

    i. West Mercia PCC has publicly suggested that there are "*safeguards and processes in place [that] will ensure this technology will be used appropriately and proportionately*." Staffordshire PCC has publicly suggested that there were "*robust*

[25] *Mohamed and another v Secretary of State for the Home Department* [2014] 1 WLR 4240, per Maurice Kay LJ, at §40.

safeguards" covering the use of IMSI Catchers. Notwithstanding these public confirmations, the Respondent permitted the West Mercia and Staffordshire PCCs to neither confirm nor deny that they held any policy or other safeguards regulating the use of IMSI Catchers, referring back to its MPS decision notice;

ii. Equally, the Respondent has upheld the reliance on s.24(2) in respect of some public bodies, even where others have confirmed that they do hold a "*business case"* in respect of IMSI Catchers;[26]

g. The use of IMSI Catchers by public bodies across England and Wales has been publicly confirmed, both in Parliament (see, §§11 and 20, above) and in press coverage (see, §§14-18, above). Their use in Germany and the USA is a matter of public record (see §13, above). The answers of the South Yorkshire PCC in 2016 (set out above, at §19) strongly infer that South Yorkshire police has used IMSI Catchers. There is no evidence that these public disclosures have, in any way, impacted on national security. It is unclear how further confirmation would increase any adverse impact on national security;

h. Many covert surveillance techniques, including IMSI Catchers, may be used for ordinary law enforcement purposes, such as tracking a suspect for a variety of offences, rather than to safeguard national security;

i. The Respondent's decision is inconsistent with the past practice of public bodies who have disclosed information on covert surveillance techniques without considering the confirmation of the existence of these techniques a threat to national security;[27]

[26] Decision Notices FS50728057 and FS50728508, at §32.
[27] The Government has admitted to hacking and subjected it to public regulation – see Part 5 of the Investigatory Powers Act 2016; and Equipment Interference: Code of Practice, available here: https://www.gov.uk/government/publications/equipment-interference-code-of-practice. Police forces have also disclosed information on their use of mobile phone extraction – see Privacy International's report, "*Digital stop and search: how the UK police can secretly download everything from your mobile phone*" (March 2018), available here: https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf.

j. It is a *non sequitur* to suggest that confirming or denying the existence of information on IMSI Catchers would heighten the vulnerability to crime of particular police force areas (decision, at §51). The Respondent states that if FOIA responses revealed certain police force areas not to have IMSI Catchers, these areas would be "*obviously more vulnerable to the types of crimes that could be subject to this type of surveillance* [i.e. surveillance by IMSI Catchers]". The Respondent also states that, if it were revealed that no police forces possessed IMSI Catchers, "*this would again show vulnerability and criminals would be more knowledgeable as to what means of communication were least likely to be intercepted*". Police forces use a variety of surveillance techniques to obtain operationally-sensitive information; because a force does not possess IMSI Catchers does not mean they cannot obtain such information through other surveillance means. Knowing which police forces possess IMSI Catchers would not allow an individual to map or be aware of how such information is obtained, or identify more vulnerable areas to commit crime.

34. **Thirdly**, or in the alternative, the Respondent erred in its approach to the public interest balance:

a. As the Upper Tribunal emphasised in *Keane v Information Commissioner and others* [2016] UKUT 461 (AAC), the balancing exercise is fact-sensitive and the s.24 exemption does not carry "*inherent weight"*. The Tribunal must consider to what extent the public interest factors potentially underlying the relevant exemption are in play <u>in the particular case</u> and then consider what weight attaches to those factors <u>on the particular facts</u>;[28]

b. There is a strong and overwhelming public interest in confirming or denying the existence of the information sought as:

i. It makes an important contribution to an on-going public debate on surveillance and privacy rights;

[28] *Cabinet Office v Information Commissioner* [2014] UKUT 0461 (AAC), at §67; approved in *Keane*, at §57. It is also important to note that *Keane* was a s.24(1) case, not a s.24(2) case.

ii. The fact that IMSI Catchers have been purchased and/or used by UK police is already in the public domain;

iii. It would promote public participation in an informed debate about IMSI Catchers and the existence and development of IMSI Catchers in the UK;

iv. There is a clear public interest in the public being informed about whether public money is being spent on something which is or is not regulated;

v. There is a clear public interest in the public being informed about police use of surveillance technology that may pose serious interferences with a range of civil liberties and human rights, including the rights to privacy, freedom of expression and freedom of assembly and association. In particular, there is a particularly compelling public interest in surveillance technology, such as IMSI Catchers, which conduct indiscriminate surveillance and can therefore interfere with the rights of many persons simultaneously;

c. These public interest factors far outweigh the public interest factors underlying the s.24(2) exemption in this particular case. The Respondent has provided no, or no adequate, reasons for its decision in this regard. It was wrong to suggest that there was only "*some valid"* public interest and that these points were increasing public knowledge on the purchase, replacement and use by the police service as a whole;[29]

d. The fact that the current national security threat is "*severe"* (decision, at §59) does not assist. That is a general risk assessment, not an individual assessment of any risk attached to confirming or denying the existence of the information sought;

e. It is not understood in particular how the Respondent came to its decision that the public interest exemption applied to policy statements, and other guidance on the use of IMSI Catchers, such as when a warrant or other

[29] Decision Notice FS50728057, at §40.

legal processes must be obtained, and rules governing when the existence and use of IMSI Catchers may be revealed to the public, criminal defendants, or judges;

f. It is not understood how the Respondent could come to such a conclusion in circumstances in which some public bodies have confirmed the existence of some of the information sought (as set out above).

35. **Fourthly**, as regards Warwickshire PCC and West Mercia PCC, the Respondent erred in its approach to s.24(1) FOIA:

a. The exemption was not engaged:

i. It does not inherently follow that disclosing the capabilities and uses of a particular technique or tool reveals information that would negatively impact upon national security. This is evidenced by the approach of a number of public bodies in relation to other forms of surveillance technology, including hacking and mobile extraction, where s.24 has not been engaged;[30]

ii. The Alliance Governance Group minutes had specifically stated that "*Both [Warwickshire and West Mercia] PCCs agreed to Replacing the existing equipment with a new supplier*". The fact that IMSI Catchers have been purchased by UK forces is already in the public domain and these bodies have already been named in this regard;

b. The public interest in disclosure far outweighed the public interest in maintaining the exemption, on the narrow facts of this application. There is an important public interest in how public funds are spent, and a natural concern to ensure that any covert activities are proportionate to the risks that a public authority may be seeking to address. This is an important factor in holding public bodies to account, and increasing transparency about how they perform their functions;

[30] See footnote 27, above.

c. Further, there is a public interest in citizens being informed about methods of surveillance that may have a profound impact on their fundamental rights, such as their right to privacy. There is a significant public interest in the topic of IMSI Catchers and the regulation of related communication surveillance technologies. IMSI Catchers engage the public interest because their use implicates the fundamental rights of many citizens, due to their indiscriminate nature. The Respondent gave this factor insufficient weight;

d. Insufficient reasons have been provided as to why there is a public interest in refusing to disclose the information held, when weighted against the rights of access to information, and principles of transparency.

E. Conclusion

36. For the reasons set out above, the Tribunal is respectfully invited to allow this appeal. The Respondent's reliance on ss.23(5), 24(1) and 24(2) was wrong, for the reasons set out above. There has been no consideration by the Respondent of any alternative exemption. Insofar as any reliance is now placed on any alternative exemption, the Appellant reserves its rights to respond.

37. In the event that the Tribunal is not minded to allow this appeal on the papers, it is respectfully invited to list this appeal for an oral hearing.

JUDE BUNTING
KEINA YOSHIDA
Doughty Street Chambers

7th August 2018