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

Appeal nos: EA.2018.0164 and 0170

B E T W E E N :

PRIVACY INTERNATIONAL

Appellant

-and-

THE INFORMATION COMMISSIONER'S OFFICE

Respondent

COMMISSIONER OF THE METROPOLITAN POLICE[1]

POLICE AND CRIME COMMISSIONER FOR WARWICKSHIRE[2]

Second Respondents

SKELETON ARGUMENT OF THE APPELLANT

A. Preliminary Matters

- References to the open hearing bundles are given as **[bundle number / page number]**. There are two different open bundles entitled "*Open Bundle of Documents Folder 1 of 2"*. The Appellant proposes to describe "*Folder 1 of 2"* in the MPS appeal as bundle number 1A and "*Folder 1 of 2"* in the Warwickshire PCC appeal as bundle number 1B.
- Time estimate: 2 days (hearing); 3 hours (pre-reading).
- Representation:
    - Appellant: Jude Bunting and Keina Yoshida (instructed by Liberty);
    - ICO: Christopher Knight (instructed by the ICO);
    - MPS: Robert Talalay (instructed by MPS Legal Service);
    - Warwickshire PCC: unknown representative.
- Suggested pre-reading (3 hours):
    - Skeleton arguments of the parties;
    - Decision in MPS appeal, 10th July 2018 **[1A/1-17]**;
    - Decision in Warwickshire appeal, 10th July 2018 **[1B/1-12]**;

[1] The Second Respondent in appeal reference EA.2018.0164.
[2] The Second Respondent in appeal reference EA.2018.0170.

- Witness statement of DS Steve Williams **[1A/184-196]**;
- Witness statement of DCC Nicholas Baker **[1A/197-8]**;
- Witness statement of DCS Robert Fordham **[1A/199-200]**;
- Witness statement of DS Andrew Nolan **[1A/201-229]**;
- Witness statement of Ulf Buermeyer **[2/1-8]**;
- Witness statement of Silke Holtmanns **[2/9-23]**;
- Witness statement of Nathan Freed Wessler **[2/24-38]**;
- Witness statement of Ailidh Callander **[2/125-136]**.

B. Introduction and summary

1. In this appeal, the Appellant seeks access to information relating to the purchase and use of mobile surveillance equipment known as "International Mobile Subscriber Identity ("**IMSI**") Catchers", and to the regulatory and oversight regime that exists to monitor the use of such equipment.

2. IMSI catchers are remarkably intrusive. They permit the police to monitor the operations of mobile telephones throughout an area, including to track the location of individuals and to see all communications and data going to and from the network, such as calls and messages. Using IMSI catchers, police can also change the content of communications and data or prevent them from being transmitted **[2/11-22]**. The fact that numerous police forces, including the Metropolitan Police Service ("**MPS**") and Warwickshire police, have purchased IMSI Catcher equipment is in the public domain **[2/126-130]**. There is an overwhelming public interest in ensuring that the purchase and use of such equipment is justified, proportionate, and sufficiently regulated.

3. The Appellant initially sought information from a number of police forces and Police and Crime Commissioners ("**PCC**").[3] Each of the police forces and public bodies who responded to the Appellant's information requests refused to confirm or deny that they held the information requested by the Appellant (both initially[4] and after a second internal review[5]). They relied on exemptions

[3] The MPS request is at **[1A/108-110]**. The Warwickshire PCC request is at **[1B/95-96]**. The other police forces and PCCs contacted were: Avon and Somerset PCC, Avon and Somerset police, Kent police, South Yorkshire police, Staffordshire PCC, West Mercia PCC, and West Midlands PCC.
[4] The MPS decision is at **[1A/111-115]**; the Warwickshire PCC decision is at **[1B/97-99]**.
[5] The MPS review decision is at **[1A/122-129]**; the Warwickshire PCC review decision is at **[1B/106-113]**.

from having to confirm or deny under ss.23(5), 24(2), 30(3), and/or 31(3) Freedom of Information Act 2000 ("**FOIA**"). The Respondent ("**ICO**") upheld an initial appeal against these decisions, but only in respect of ss.23(5) and 24(2).[6] The MPS appeal has been chosen as the "*lead case"* to determine these issues **[1A/84]**.

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(1)(a) and (b).[7] This refusal was upheld on review[8] and on appeal by the ICO **[1B/1-12]**. The Warwickshire PCC appeal has been chosen as the "*lead case"* for this aspect of the appeal **[1A/84]**.

5. As regards the MPS appeal, the Appellant respectfully submits:

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

   b. On the facts, the s.23(5) exemption is not made out;

   c. The ICO erred in concluding that the s.24(2) exemption was "*required for the purpose of safeguarding national security*";

   d. The MPS reliance on s.31(3) is unparticularised and unevidenced. The exemption does not apply on the facts;

   e. The public interest in maintaining either the s.24(2) exemption or the s.31(3) exemption is obviously outweighed by the public interest in confirming or denying that the information requested was held.

6. In respect of the Warwickshire PCC appeal, the Appellant submits that:

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

   b. The PCC's reliance on s.31 fails. It does not apply;

[6] The ICO decision in the MPS appeal is at **[1A/1-17]**.
[7] The Warwickshire PCC decision is at **[1B/97-99]**.
[8] The Warwickshire PCC review decision is at **[1B/106-113]**.

c. In all the circumstances of the case, the public interest in maintaining either the s.24(1) exemption or the s.31(1) exemption is obviously outweighed by the public interest in disclosing the information.

C. The Appellant's evidence

7. The Appellant relies on four witness statements. Those statements are not realistically challenged in the various statements on which the Respondents rely. It is not expected that their evidence will be subject to cross-examination. Three of them (Ulf Buermeyer, Silke Holtmanns, and Nathan Freed Wessler) live outside the United Kingdom and will not be available to attend the hearing in person. The Appellant's evidence is summarised below.

8. The Appellant is a non-profit, non-governmental organisation based in London, which defends the right to privacy around the world.[9] It has litigated regularly both domestically and in Strasbourg to seek to uphold privacy rights, particularly as regards state surveillance methods and tactics.[10] The Appellant's status as a non-governmental organisation involved in matters of public interest is important. Under article 10 of the European Convention on Human Rights, the Appellant is a "*public watchdog"* with a particular entitlement to obtain information.[11] This is a factor of particular weight in the public interest balance, as set out further below. It cannot be ignored simply on the basis that a disclosure to the Appellant under FOIA may also be disclosed more widely.

9. As Ailidh Callander explains, the Appellant has carried out significant work in respect of the police use of surveillance technology. For example, it has used FOIA to gather information in respect of the purchase and use of mobile phone extraction technology by police forces and police use of technology to examine "*Internet of Things"* devices **[2/134-5, §§28-30]**. Such publications have helped to contribute to important debates in the public interest.

10. This case relates to a particular form of police surveillance: IMSI Catchers.

[9] Statement of Ailidh Callander, §2 **[2/125]**.
[10] See, in particular, *10 Human Rights Organisations v United Kingdom* (App. no 24960/15) and a number of cases before the Investigatory Powers Tribunal.
[11] *Társaság Szabadságjogokért v Hungary* (2011) 53 EHRR 3, §35; *Youth Initiative for Human Rights v Serbia* (App. no. 48135/06), §§20 and 24; *Magyar Helsinki Bizottság v Hungary* (App. no.18030/11).

The technological capacity of such devices is set out in the witness statement of Silke Holtmanns, an expert in mobile communication security who currently works for Nokia Oy **[2/9-23]**. As Silke Holtmanns explains, such devices represent a particularly intrusive form of police surveillance. 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 (and thereby their user) by revealing their international mobile subscriber identity. 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 or preventing their transmission. Some IMSI Catchers block service, either to all mobile phones within their range or to select devices **[2/11-20, §§11-26, 33 and 37]**.

11. The use of IMSI Catchers by police forces in the USA and in Germany is well-established:

    a. Ulf Buermeyer, a judge at the Regional Court of Berlin and President of the Society for Civil Rights, a Berlin-based non-governmental organisation, explains that where IMSI Catchers are used in criminal proceedings or in Federal Criminal Police investigations, law enforcement bodies that use IMSI Catchers have a duty to notify those targeted, so as to enable the person concerned to challenge the use of IMSI Catchers as necessary **[2/2-6, §§8-11]**. In addition, federal intelligence agencies must notify the Parliamentary Control Panel of their use of IMSI Catchers, with the Panel subsequently publishing regular reports on IMSI Catcher use. From 2019, the Federal Criminal Police Office will also have to report to the German Parliament, who will also publish reports **[2/2-6, §§12-14]**. Further information relating to the use of IMSI Catchers by the police has been revealed through parliamentary questions **[2/6-7, §§18-22]**. There is no suggestion that the "*high degree of transparency"* regarding the use of IMSI Catchers in Germany has had any negative impact on national security or on police operations;

    b. Nathan Freed Wessler, of the American Civil Liberties Union, explains that police forces in the USA overwhelmingly respond to freedom of

information requests about the purchase and use of IMSI Catchers by identifying records, releasing many records in whole or in part, and withholding other records only after acknowledging their existence **[2/26, §6]**. Police forces have taken this approach even though the US equivalent of FOIA has been interpreted by the courts so as to permit 'neither confirm nor deny' ("**NCND**") responses **[2/26, §8]**. Attempts to rely on NCND in relation to IMSI Catchers have not withstood challenge **[2/28, §14]**. As a result of information requests, it is now well-known that at least 75 state and local law enforcement agencies across 27 states own IMSI Catchers, as do at least 14 federal law enforcement, military, and intelligence agencies **[2/27-28, §13]**. The documents obtained have included identical documents to those sought in this appeal, such as policy documents governing the use of IMSI Catchers, purchase records, and non-disclosure agreements **[2/30-1, §17]**. The release of these documents has enabled public debate about the propriety of the use of IMSI Catchers and has stimulated better regulation of IMSI Catchers by government **[2/35, §21]**. There is no suggestion that the release of such information has had any negative impact on national security or police operations.

12. The fact that police forces have purchased and used IMSI Catchers is not just an overseas phenomenon. There is considerable information already in the public domain about this in the UK. It is summarised in the witness evidence of Ailidh Callander, at §§5-27 **[2/126-133]**. In particular:

    a. *The Guardian* revealed in 2011 that the MPS and Hertfordshire police had purchased IMSI Catchers **[2/138-140]**. *The Times* **[2/142-4]** and *The Mail* **[2/146-148]** published similar reports in 2014;

    b. In October 2016, the *Bristol Cable* revealed that seven police forces had purchased IMSI Catchers: Avon and Somerset police, the MPS, South Yorkshire police, Staffordshire police, Warwickshire police, West Mercia police, and West Midlands police. This information was revealed, in part, through minutes published by the "*Alliance Governance Group*", which was published online by West Mercia police and which confirmed that "*both West Midlands and Staffordshire Police have recently purchased and operated 4G compatible* [Covert Communications Data Capture]

equipment". It also revealed that Warwickshire police and West Mercia police had purchased new IMSI Catchers **[2/151-2]**. In response to this publication, both West Mercia PCC and Staffordshire PCC acknowledged that their forces had used IMSI Catchers **[2/129, §16]**;

c. Similar police publications have confirmed the purchase of IMSI Catchers by Avon and Somerset police **[2/166-9]**, the MPS **[2/171-4]**, West Midlands police **[2/177-184]**, Essex police **[2/186]**, and Kent police **[2/188-9]**;

d. The Ministry of Defence confirmed in response to a FOIA request that it had contracted with an IMSI Catcher company **[2/221-2]**. To equal effect, the Scottish Prison Service has confirmed the purchase of IMSI Catchers in response to requests under the Freedom of Information (Scotland) Act 2002 **[2/249-278]**.

13. The use of IMSI Catchers by police forces and other public bodies in the UK has also been addressed in Parliament: see, for example, the statements made by a Minister of State within the Home Office on 7th July 2015 and on 11th January 2018, set out in the Appellant's grounds of appeal, at §§11 and 20 **[1A/27-31]**.

D. The Respondents' evidence

14. The Respondents' open evidence is largely based on assertions of risk (to national security and police operations) made by senior police officers. It is difficult to go behind these assertions of risk, as the evidence upon which they are based has not been revealed. In the circumstances, the Appellant is unlikely to seek to cross-examine the Respondents' witnesses but will rather invite the Tribunal to assess those assertions on the basis of the available evidence.

15. None of the Respondents' witnesses realistically dispute that it is in the public domain that a number of police forces in England and Wales have purchased and used IMSI Catchers:

a. The witness evidence of DS Williams of the MPS **[1A/184-196]**, DCC Baker of Staffordshire police **[1A/197-8]**, and DSC Fordham of Kent

police **[1A/199-200]** does not address this issue at all;

b. Warwickshire PCC's witness, DS Nolan, acknowledges that "*there is a certain amount of information about covert policing tactics that is already in the public domain"* **[1A/203, §7]**, although he does not particularise what information about IMSI Catchers he accepts is already in the public domain. Describing the publication of the Alliance Governance Group minutes as "*unfortunate"*, he confirms that this means "*there is now further information in the public domain relating to a confidential business case for covert equipment"* **[1A/203, §8]**.

16. Much of the Respondents' evidence is given over to assertions about the quality of the oversight regime for IMSI Catchers: see DS Williams **[1A/188-196, §§15-48]**, DCC Baker **[1A/198, §3]**, and DS Nolan **[1A/205-9, §§18-29]**. This evidence takes the Respondents nowhere. It is impossible to address the quality of the oversight regime without public confirmation of the police technique that is in issue: the level of safeguards would need to be proportionate to the level of intrusion. In any event, the evidence is incomplete, as the Respondents have chosen not to disclose the internal policies and regulatory framework that they apply to the use of IMSI Catchers. The Tribunal is invited to discount this evidence.

17. Realistically, the high point of the Respondents' evidence is DS Williams' assertion that disclosure of "*covert techniques"* would seriously undermine future operations and place people's lives at risk. Whilst any statement of such a senior officer commands respect, this assertion is over-stated.

18. Firstly, while IMSI Catchers, when used in individual cases, may be described as a "*covert"* technique, the reality is that the use of IMSI Catchers in general is not hidden in circumstances in which their purchase and use by numerous police forces and other public bodies is publicly known.

19. Secondly, it is difficult to understand how confirming or denying that the MPS holds the information sought by the Appellant would undermine future operations and place people's lives at risk given that:

a. The purchase and use of IMSI Catchers by numerous police forces is in the public domain;

b. The purchase and use of IMSI Catchers by other police forces internationally is well-recognised and frequently reported on (see, in particular, the undisputed evidence relating to the USA and Germany; countries that no doubt face similar, if not higher, levels of threat from terrorists and organised crime groups);

c. There is no evidence that the revelation of the purchase and use of IMSI Catchers either by police forces in England and Wales or by police forces in USA and Germany have impacted on national security or police operations in any way.

d. Police forces in the UK have disclosed information about other "*covert*" surveillance techniques, such as mobile phone extraction and hacking, without any evidence of a negative impact on national security or police operations **[2/134-6, §§28-31]** (as addressed further below).

E. The MPS appeal

i. The meaning of s.23(5)

20. The first issue is the correct construction of s.23(5) FOIA. Section 23(5) is an absolute exemption, which permits a public body not to confirm or deny that it holds information if it would involve the disclosure of "*any information … which was directly or indirectly supplied to the public authority by, or relates to"* the bodies listed at s.23(3). Those bodies include the security agencies, the special forces, the Investigatory Powers Tribunal, the Security Vetting Appeals Panel, the Serious Organised Crime Agency, the National Crime Agency, and the Intelligence and Security Committee of Parliament.

21. It is the Appellant's case that the phrase "*relates to"* ought to be given a narrow construction and the exemption only applies to information that is directly connected to one of the s.23(3) bodies. The ICO, in the decision under challenge, wrongly held that s.23(5) applies where a public body can show that the information requested is "*within what could be described as the ambit of security bodies' operations*" **[1A/8, §32]** and that the test was

"*whether or not the use of such equipment could 'relate to' any of the security bodies*" (emphasis added) **[1A/10, §38]**. This was an error of law:

a. Any absolute exemption ought to be construed narrowly. This is because of the following. The "*default setting*" in FOIA is in favour of disclosure.[12] Any absolute exemption is a serious interference with common law information rights[13] and the rights of "*public watchdogs"* such as the Appellant under article 10 (as set out above);

b. There is no authority supporting the ICO's construction of s.23(5). The authority cited does not support it[14] 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*";[15]

c. The ICO'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 or which is "*in the ambit"* of their activities;

d. "*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;

e. The ICO'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 ICO's interpretation would bring all such techniques outside the scope of

[12] *Galloway v Information Commissioner v The Central and North West London NHS Foundation Trust* (2009) 108 BMLR 50, §70.
[13] *Kennedy v Information Commissioner* [2015] AC 455.
[14] *Commissioner of Police of the Metropolis v Information Commissioner* (EA/2010/0008), which touches only on the standard of proof.
[15] 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.

disclosure under FOIA. To give an example, it is within the ambit of SVAP to consider appeals against security vetting refusals. The Home Office policy on security vetting is a policy that falls within the ambit of SVAP's jurisdiction. Yet it would be absurd to suggest it falls within s.23(5);

f. The ICO'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 ICO has directed the disclosure of that information;

g. The justification for such a wide construction is, in any event, not made out, given that information that would detrimentally impact on national security is already covered by s.24 and information that would damage police operations is already covered by s.31.

ii. Does s.23(5) apply?

22. There is no suggestion that the information sought by the Appellant was supplied, either directly or indirectly, by any of the s.23(3) bodies. In the circumstances, the key question for the Tribunal will be whether, on the balance of probabilities, the information sought is directly connected to one of those bodies. No open evidence has been served on this point. The ICO does not address any argument on the point in its response **[1A/53, §§16-17]**. The MPS response does "*not provide any open submissions as to whether the ss.23(5) and 24(2) exemptions are made out"* **[1A/68, §25]**.

23. In an absence of any evidence (or even of any argument), the Appellant invites the Tribunal to resolve this point against the Respondents. The rationale for the application of s.23(5) in the decision does not withstand scrutiny:

a. The ICO suggests that, if the information described in the Appellant's request did exist, "*this would be a field of work which is likely to have been done in conjunction with, and with the knowledge of, other parties within the policing field, and also that this type of work is likely to include the security bodies"* **[1A/10, §37]**. This is the application of the wrong test. Whether or not other policing bodies work in conjunction with the

Respondents in the purchase and use of IMSI Catchers is not a point that resolves whether the information is closely connected to one of the s.23(3) bodies;

b. The suggestion that "*this type of work is likely to include the security bodies"* once again casts the net too wide. Equally flawed is the ICO's suggestion that, if an IMSI Catcher is used, "*it could realistically be deployed in joint operations between the police service and security bodies"* **[1A/10, §38]**. So too could a pen and paper. An actual connection to the s.23(3) bodies is required, not a possibility that a technique may be used by a security body.

iii. Does s.24(2) apply?

24. Section 24(2) permits a public body to neither confirm nor deny that it holds information where this "*is required for the purpose of safeguarding national security*." Three preliminary points on the law arise:

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;[16]

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*".[17] 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);

[16] *Savic v Information Commissioner and others* [2016] UKUT 535 (AAC), at §70.
[17] *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 scrutinise this issue with particular care. Otherwise, there would be a weakening of public trust in the proper oversight of the FOIA regime.[18]

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

a. The test adopted by the ICO, namely "*ensuring that matters which are of interest to the security bodies are not revealed"* **[1A/11, §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;

b. The fallacy of the ICO's approach is underlined by the fact that it has permitted public bodies to neither confirm nor deny that they hold the information sought even in circumstances in which numerous police forces have publicly confirmed the existence of such information, as set out above, and in which there is actual evidence that confirming the existence of equivalent information sought has not impacted on national security in any way in the USA and in Germany;

c. The decision to uphold the reliance on s.24(2) is said to be justified because confirming or denying the existence of the information sought would reveal whether or not IMSI Catchers are being used. However,

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

there is actual evidence on the use of IMSI Catchers before the Tribunal. In the Warwickshire appeal, the PCC has confirmed that it does hold a business case in respect of IMSI Catchers. There is no suggestion that this confirmation impacted on national security in any way;

d. The ICO's decision is inconsistent with the past practice of public bodies which have disclosed information on covert surveillance techniques without considering the confirmation of the existence of these techniques a threat to national security. Techniques that have been publicly confirmed include bulk surveillance techniques, equipment hacking,[19] and, as Ailidh Callander explains, the use of mobile phone extraction technology by police forces, the police use of technology to examine "*Internet of Things"* devices, and predictive policing **[2/134-6, §§28-31]**. It is not understood why the use of some surveillance techniques, including "*covert*" ones, can be confirmed, while the use of IMSI Catchers cannot;

e. 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 **[1A/13, §51]**. 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.

iv. s.31(3)

26. The ICO placed no reliance on s.31(3) in its decision. Nevertheless, the MPS seeks to resurrect it in its response to the appeal **[1A/62-3 and 65-6, §§5 and 14]**. Despite this, the MPS has not set out any specific argument in respect of this exemption and has not specified which of the s.31(1) matters would be prejudiced by confirming or denying that it holds any of the information sought.

27. Overall, the s.31(3) exemption is not engaged:

[19] Which has been subjected to public regulation – see Part 5 of the Investigatory Powers Act 2016 and the Equipment Interference Code of Practice.

a. No adequate basis has been pleaded as to why confirming or denying the information sought would, or would be likely to, prejudice any of the police purposes in s.31(1). The pleadings of the MPS are predicated on a bare assertion and the Respondents' open witness evidence takes matters no further. It is unclear how confirming or denying the information sought by the Appellant would enable offenders to develop countermeasures in respect of IMSI Catchers;

b. It does not inherently follow that disclosing the capabilities and uses of a particular technique or tool reveals information that would negatively impact upon the policing purposes set out at s.31(1). 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 no such negative impact has arisen (as set out above);

c. Paragraph 25(b)-(e), above, is repeated. There is no suggestion, let alone evidence, that the public revelation of so much detail about IMSI Catchers in the national press and in official police publications has led to any prejudice to police purposes.

v. The public interest balance

28. Even if s.24(2) or s.31(3) does apply, which is denied, the public interest in confirming or denying overwhelmingly favours the Appellant:

a. 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 in the particular case and then consider what weight attaches to those factors on the particular facts;[20]

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

[20] *Cabinet Office v Information Commissioner* [2014] UKUT 0461 (AAC), §67; approved in *Keane v Information Commissioner and others* [2016] UKUT 461 (AAC), §57. *Keane* was a s.24(1) case, not a s.24(2) case.

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

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, development and deployment of IMSI Catchers in the UK. It is wrong for the ICO to suggest that because there has been some public debate about the appropriateness of the use of IMSI catchers, this should reduce the public interest in confirming or denying and therefore being able to have a fuller, more informed debate concerning, for example, how IMSI Catchers should be regulated **[1A/58, §41]**. While there is some interest in a debate about the theoretical use of IMSI Catchers, it is a different matter to have a properly informed debate that is based on actual awareness of the extent of their use;

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. It is a relevant factor in the public interest balancing test that the Appellant is a "*public watchdog"* with a right to obtain information under article 10. The suggestion that this is undermined because FOIA is "*applicant blind"* **[1A/14, §57]** is wrong in principle. If the Appellant has an article 10 right to obtain this information as a public watchdog, this should

not be reduced to an irrelevance because other people may then get the information as well. Where else does article 10 arise in the argument? There is no alternative mechanism for seeking this information, such as the common law open justice principle, which has arisen in other cases;

d. The public interest factors in favour of confirming or denying far outweigh the public interest factors underlying the s.24(2) and s.31(3) exemptions in this particular case. The ICO has provided no, or no adequate, reasons for its decision in this regard. The fact that the current national security level of risk is "*severe"* **[1A/15, §59]** assists no more than the generalised assertions in the Respondents' evidence. It is a general risk assessment, not an individual assessment of any risk attached to confirming or denying the existence of the information sought. For the reasons set out above, the Respondents' open evidence takes the analysis no further.

F. The Warwickshire appeal

29. The starting point is a recognition of the narrow scope of this appeal. At issue is simply a business case in respect of the purchase of IMSI Catchers, which the PCC has confirmed that it holds. The argument reflects the submission set out above, albeit that the PCC relies on exemptions relating to the disclosure of the information itself (set out in s.24(1) and s.31(1)) as opposed to the equivalent exemptions relating to confirming or denying.

30. Neither exemption was engaged in this case. It does not inherently follow that disclosing this business case reveals information that would negatively impact upon national security or on policing purposes. Paragraph 25(b)-(e), above, is repeated.

31. In any event, the public interest in disclosure far outweighs the public interest in maintaining the exemption, for the reasons set out above, at paragraph 28. These factors apply with still greater force to the provision of the information itself (as opposed to merely confirming whether such information is held). 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.

32. It was therefore wrong for the ICO to conclude only that there was "*some valid"* public interest **[1B/10, §40]**. There is an overwhelming 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 positive benefits of transparency in improving public debate and regulatory oversight in the USA and Germany are well-established.

G. Conclusion

33. The Tribunal is respectfully invited to allow this appeal.

JUDE BUNTING
KEINA YOSHIDA
Doughty Street Chambers

26th July 2019