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

Case Number EA/2018/0164

PRIVACY INTERNATIONAL

Appellant

and

THE INFORMATION COMMISSIONER

First Respondent

COMMISSIONER OF POLICE FOR THE METROPOLIS

Second Respondent

Heard in public at Field House on 27 and 28 August 2019

Before

Judge Alison McKenna (CP)
Rosalind Tatam
Marion Saunders

Attendances:

For the Appellant: Jude Bunting, counsel, instructed by Liberty

For the First Respondent: Christopher Knight, counsel, instructed by The Information Commissioner's Office

For the Second Respondent: Robert Talalay, counsel, instructed by the Directorate of Legal Services, Metropolitan Police Service

DECISION ON EA/2019/0164

The Tribunal upholds the decision notice dated 10 July 2018 and dismisses the appeal.

REASONS

Introduction

1. Privacy International is a charity which campaigns for the protection of the right to privacy. On 1 November 2016, it made a number of information requests, under the Freedom of Information Act 2000 ("FOIA"), to police forces, Police and Crime Commissioners and other public authorities seeking information relating to the purchase, use and regulation of equipment falling under the umbrella term of "Covert Communications Data Capture" ("CCDC"), in particular equipment known as "International Mobile Subscriber Identity ("IMSI") Catchers".

2. This appeal concerns the response of the Commissioner of the Metropolitan Police ("MPS") to that request. MPS neither confirmed nor denied whether it held the requested information, citing the FOIA exemptions at s. 23(5) for information supplied by, or relating to, bodies dealing with security matters; s. 24 (2) the national security exemption; and s.31 (3) the law enforcement exemption. Privacy International complained to the Information Commissioner.

3. The Information Commissioner issued Decision Notice FS50728051 on 10 July 2018, in which she decided that MPS was entitled to rely on s.23 (5) and s. 24 (2) FOIA to neither confirm nor deny whether it held the requested information and that the public interest favoured maintaining the exemption under s.24(2). She did not determine the engagement of s. 31 (3) FOIA. Privacy International appealed to the Tribunal.

4. The Tribunal directed an oral hearing of two cases, of which this is one. They were heard together on 27 and 28 August 2019. There are seven more extant appeals arising from the original series of information requests. These have been stayed pending the determination of these two appeals.

5. The Tribunal received open and closed evidence in this appeal and heard open and closed submissions. Privacy International was not provided with the closed bundle. Privacy International's representatives left the hearing room for the closed evidence and submissions but were provided with a "gist" when the Tribunal resumed in open session. Accordingly, there is a closed annexe to this Decision which deals with the closed witness evidence and submissions and our conclusions about it. This will not be disclosed to Privacy International.

6. This is the Tribunal's decision in relation to MPS only. Our Decision in the other case we heard, EA/2018/0170*,* will be issued separately. In case they are not promulgated together, the time limit for making an application for permission to appeal in both cases is extended so that it is 28 days after the date of promulgation of the second of the Tribunal's Decisions.

The request for information

7. On 1 November 2016, Privacy International made the following request to MPS:

> *"I am writing on behalf of ...to seek records ...relating to the purchase and use of mobile phone surveillance equipment by the Metropolitan Police.*

I refer, in particular, to the recent article written by the journalist collective The Bristol Cable "Revealed: Bristol's police and mass mobile surveillance". The article makes reference to the purchase of equipment from the company CellXion by the Metropolitan Police under the item "CCDC" for the cost of £1,037,223.00. The article links to the original document dis-closing the purchase, which can be found on the Metropolitan Police website [. . .]. The article also explains that the acronym "CCDC equipment" appears to refer to 'covert communications data capture' as spelled out in the minutes of an Alliance Governance Group meeting in May 2016 between Warwickshire and West Mercia Police.

I also refer to the 10 October 2016 article published by the Guardian 'Controversial snooping technology used by at least seven police forces'. That article reported that 'surveillance technology that indiscriminately harvests information from mobile phones', also 'known as an IMSI catcher' is being 'used by at least seven police forces across the country ... according to police documents'. One of the forces understood to be using this technology is the Metropolitan Police.

[Name]... requests the following records:

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

[Name] seeks records regardless of how CCDC equipment is identified. In this respect,.. . notes that CCDC equipment can be referred to using a range of other terms, including 'IMSI catchers', 'IMSI grabbers', '"Cell site simulators', and 'Stingrays'.

Please include copies of material that you hold either in the form of paper or electronic records, including emails. If possible, please provide all requested records in electronic format.

Upon locating the requested records, please contact us and advise us of any costs of providing copies, so that we may decide whether it is necessary to narrow our request".

8. In its responses to the request, initially in November 2016, and subsequently on review in January 2017, MPS would neither confirm nor deny holding the requested information,

citing exemptions at sections 23(5), 24(2), 30 (3) and 31 (3) FOIA. Hereafter, we refer to neither confirming nor denying as "NCND".

The Decision Notice

9. Privacy International complained to the Information Commissioner, whose office conducted an investigation. During the investigation, MPS ceased to rely on s. 30 (3) FOIA.

10. The Decision Notice concluded that MPS was entitled to rely, in respect of parts (1), (3) and some of part (4) of the request, on ss.23(5) and 24(2) FOIA so that MPS was not obliged to confirm or deny whether the requested information was held.

11. In respect of part (2) and some aspects of part (4) of the request, the Decision Notice records that the exemptions were relied on incorrectly so that MPS was obliged to confirm or deny whether the information was held and either disclose it or issue a fresh response citing a relevant exemption. As noted above, the Decision Notice did not determine the engagement of s. 31(3) FOIA.

12. The Decision Notice noted at paragraph 15 that the "link" to information referred to in the body of the request was no longer available at the time of the Commissioner's investigation. Accordingly, she was unable to verify whether the information referred to had been in the public domain at the time of the request.

13. At paragraphs 16 and 17, the Decision Notice recorded MPS's position as follows. Firstly, that it had made no formal statements in respect of the subject matter of the request and secondly that ' ...*confirming or denying that the MPS hold any information regarding these techniques would in itself disclose exempt information. Stating information is held would confirm usage and the opposite if there is no such information."*

14. The Decision Notice considered at paragraphs 25 to 52 the engagement of s. 23 (5) and 24 (2) FOIA and concluded at paragraph 53 that:

"The Commissioner is satisfied that the public authority was entitled to rely on section 23 (5) and 24(2) in the circumstances of this case. She accepts that revealing whether or not information is held about CCDC would be likely to reveal whether information is held relating to the role of the security bodies. It would also undermine national security and for that reason section 24(2) also applies because neither confirming nor denying if additional information is held is required for the purpose of safeguarding national security."

15. Having considered the public interest balancing test arguments relevant to s. 24 FOIA at paragraphs 54 to 59 of the Decision Notice, the Commissioner concluded at paragraph 60 that:

"The Commissioner considers it to be clearly the case that the public interest in *confirming* or *denying whether information is held does not match the weight of the public interest in safeguarding national security by maintaining* a *consistent NCND stance* ... "

Appeal to the Tribunal

16. Privacy International's Grounds of Appeal in respect of the MPS Decision Notice may be summarised as follows. The Decision Notice is said to be wrong and/or unlawful because it is said to have erred in its interpretation of s. 23(5) FOIA. This is because the phrase *"relates to"* should be given a narrower construction; further that s. 24 (2) FOIA was not

engaged by the particular information requested and, if it was, then the balance of public interest did not support a NCND response.

17. The Information Commissioner's Response to the Grounds of Appeal may be summarised as follows. It was submitted that the Decision Notice was correct in its application of s. 24 (2) FOIA. However, the Commissioner had reconsidered her position in respect of s. 23 (5) and recognised the force of the Appellant's ground as to the construction of the phrase *"relates to",* so that she intended to keep the issue under review. The Commissioner also indicated that she anticipated supporting additional reliance by MPS on s. 31 (3) FOIA at the hearing.

18. MPS's Response to the appeal may be summarised as follows. The Decision Notice was correct in relation to both s. 23 (5) and s. 24 (2) FOIA, but MPS also wished to rely on s. 31 (3) FOIA, which it had raised at an earlier stage but the engagement of which had not been determined by the Decision Notice.

The Law

19. The Freedom of Information Act 2000 relevantly provides as follows:

S.1

(1) Any person making a request for information to a public authority is entitled -
(a) to be informed in writing by the public authority whether it holds information of the description specified in the request, and
(b) if that is the case, to have that information communicated to him.
(2) Subsection (1) has effect subject to...section 2 ...

S. 2 provides that:

(2) In respect of any information which is exempt information by virtue of any provision of Part II, section 1 (1) (b) does not apply if or to the extent that -
(a) the information is exempt information by virtue of a provision conferring absolute exemption, or
(b) in all the circumstances of the case, the public interest in maintaining the exemption outweighs the public interest in disclosing the information.

S. 23 (5) provides that:

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 sub-section (3).

S. 24 (2) provides that:

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.

S. 31 (3) provides that:

The duty to confirm or deny does not arise if, or to the extent that, compliance with s. 1(1)(a) would, or would be likely to, prejudice any of the matters mentioned in subsection (1).

20. Both sections 24 (2) and 31 (3) are qualified exemptions and so engage the public interest balancing exercise under s. 2(2)(b) FOIA. S. 23 (5) is an absolute exemption.

21. The Tribunal's role in determining an appeal against a Decision Notice is set out in s. 58 FOIA as follows:

> *(1) If on an appeal under* s. 57 *the Tribunal considers-*
> *(a) That the notice against which the appeal is brought is not in accordance with the law, or*
> *(b) To the extent that the notice involved an exercise of discretion by the Commissioner, that he ought to have exercised his discretion differently,*
>
> *The Tribunal shall allow the appeal* or *substitute such other notice as could have been served by the Commissioner; and in any other case the Tribunal shall dismiss the appeal.*
>
> *(2) On such an appeal, the Tribunal may review any finding of fact on which the notice in question was based.*

Evidence

22. The Tribunal is grateful for their assistance to all of the witnesses in this appeal, some of whom gave evidence on paper only and others of whom attended to give evidence in person. We record here only the open evidence, as the closed evidence is considered in the closed annexe to this Decision.

23. Privacy International relied on four witness statements, including one from Ulf Buermeyer, a Judge of the Regional Court of Berlin and the co-founder and President of the Society for Civil Rights known as GFF. His evidence referred to the publicly available information about IMSI catchers in Germany, and explained the framework under German law governing their use. In particular, he explained that the German system required notification to be given to a person whose data was caught by an IMSI catcher. He concluded that:

> *"As shown above, there is a high degree of transparency regarding the use of IMSI catchers in Germany, both at the individual and the institutional level. This includes individual notifications, public reporting mechanisms and information revealed in parliamentary questions. Important key figures have been published, including the specific bodies that have used IMSI catchers. This information has facilitated a public discussion, as evidenced by several news articles on the matter".*

24. Privacy International also relied on a witness statement from Silke Holtmanns, who is a Security Expert and Distinguished Member of Technical Staff for Nokia, although her evidence was provided in a personal capacity and not on behalf of Nokia. She has an academic background and has published widely on the subject of mobile network and phone security. She explains what an IMSI catcher is, how it operates and its impact for mobile phone users, as follows:

> *“11. An IMSI catcher, also called a 'stingray' or a 'false base station' is a small mobile base station. IMSI catchers vary in size, range, capabilities and price ...*
>
> *15. An IMSI catcher can act in either a passive mode or an active mode. The operator of the IMSI catcher chooses which mode to use.*

16. In the passive mode an IMSI catcher checks which mobile towers are within its vicinity and it may, by tuning into a particular base station, intercept mobile phone data travelling between the phone and that base station.

17. In the active mode, the IMSI catcher acts as what is called a 'man-in-the-middle' in the communication path by presenting itself as a base station amid the mobile phone network. By presenting itself as a base station emitting the strongest signal, it entices mobile phones within its vicinity to connect to it and forces them to transmit date, in particular their IMSI and IMEI [International Mobile Equipment Identity].

32. An IMSI catcher can be used to 'catch all' devices within its given vicinity, which is a common default setting when installing typical IMSI catcher software.

33. An IMSI catcher can also be used to target a particular mobile phone user, in which case you would need to know that particular user's IMSI. But even in this scenario, all other phones in the vicinity of the IMSI catcher would attempt to connect to it. When trying to connect to the IMSI catcher, these phones would transmit their IMSI and potentially IMEI data (depending on the network protocol used) which would be retained in the logs of the IMSI catcher. If properly configured, the IMSI catcher would reject the connection attempt by the phones of non-targeted users. But there remains a risk, dependent on the configurations of the IMSI catcher and the skill of the person configuring it, that the phones of non-target users will successfully connect to the IMSI catcher and have their communications and data compromised, in addition to being unable to make calls, including emergency calls.

43. There exist certain methods for detecting the use of IMSI catchers, for example by observing network anomalies or a strange handover between base stations. However, some of the signs that an IMSI catcher is in use may also be signs that a network is configured badly .... So it is unclear how effective methods for detecting IMSI catchers are as it is not easy to differentiate between misconfigurations and IMSI catcher activities. "

25. Privacy International additionally relied on a witness statement from Nathan Freed Wessler, who is a staff attorney at the American Civil Liberties Union's Privacy and Technology Project in New York. He describes his significant litigation experience in relation to surveillance technology and explains how American police forces have responded to Freedom of Information requests about the use of IMSI catchers. His evidence is that *"Very few law enforcement agencies in the United States have responded to such requests by stating that they could neither confirm nor deny...whether they held the requested information, and even fewer have maintained that position after being challenged".* His evidence is that responses to information requests have put a considerable amount of information into the public domain, for use in litigation and to inform public debate.

26. Privacy International relied on a witness statement from Ailidh Callander, its in-house legal officer. She describes the information in the public domain about the use of IMSI catchers in the UK, referring to press reports, information published by police forces themselves (such as the information referred to in the information request), and the technical information published by manufacturers of IMSI catchers. She exhibits material in each of these categories.

27. MPS relied on the open and closed witness statements of Detective Superintendent Steve Williams, who is head of the Technical Surveillance Unit within the Metropolitan Police. His open witness statement included the following evidence:

4. ....*Covert policing, by its nature, regularly works closely with and undertakes joint operations with the National Counter Terrorism Policing Headquarters and bodies covered by* s. 23 *FOIA. ...*

5. The fact that police use covert tactics to target criminality and terrorism is widely known. The exact detail and extent of law enforcement capabilities are not widely known ....

6. ...Disclosure of our capabilities or tactics (or lack thereof) would seriously undermine future operations and place people's lives at risk.

9. Criminal networks and terrorists are actively trying to find out which covert tactics and their capabilities law enforcement utilise. The internet is scattered with pages and forums dedicated to people speculating on police tactics and the capabilities of law enforcement. Much of this information is guesswork, incorrect or based around what is seen in the 'movies'. Even when specific tactics are discussed, people are not aware of their capabilities, limitations, or true nature of how they are used.

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

11. If we were to disclose the ownership or use of specific tactics or equipment, or that the same are not owned or used, it would allow criminal networks and terrorists to build up an accurate picture of our ability to respond to the most serious criminality ....

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

48. Accordingly, the deployment of any covert technique or technology is subject to multiple checks and balances to ensure that the rights of the citizenry are protected. MPS, and generally, UK Policing takes the rights of individuals seriously. The importance of the work undertaken by covert units nationwide cannot be overstated. It is of utmost importance that the capabilities of these units remain secret in the face of concerted efforts by criminal networks and terrorists to piece together their methodology in order to adapt their behaviours and stay ahead of law enforcement. For this reason, the MPS and UK law enforcement correctly asserts their right to reply "NCND" to requests which would demonstrate either the capabilities available, or their lack thereof (as the case may be)."

28. MPS also relied on open and closed witness statements made by Detective Superintendent Andrew Nolan of Warwickshire Police, who has been seconded into the West Midlands Regional Organised Crime Unit. In his open witness statement, DSU Nolan explained that the minutes of the meeting referred to by Privacy International in its information request had been inadvertently published in un-redacted form as a result of human error. When the error was realised, the minutes were removed from the website and a redacted version was later published.

29. DSU Nolan's witness statement described Ailidh Callander's witness statement as containing much speculation. He acknowledged that there is a certain amount of

information about covert policing tactics available in the public domain, but expressed the view that further disclosure about equipment or tactics would have a significantly detrimental impact on policing and therefore the safety of the public within the UK. He also expressed the view, in line with national guidance on the subject, that some elements of organised crime directly impact national security. He refers to the National Crime Agency's annual threat assessment containing a finding that organised crime groups are increasingly run by younger, tech-savvy offenders, which he says underlines the importance of restricting public knowledge of any covert tactics or technologies which law enforcement agencies may use. He comments that:

> *"Within law enforcement across the country, the use* of *certain types of covert capabilities are only known about by* a *small number of people who work in dedicated teams and are appropriately vetted. "*

30. DSU Nolan described the oversight regime for the use of Targeted Interception and Targeted Equipment Interference, noting that at the time of the information request in this case it was governed by part 3 of the Police Act 1997 but that since September 2018 the relevant regime has been under part 5 of the Investigatory Powers Act 2016, which involves judicial oversight.

31. In his oral evidence during the open session, DSU Nolan up-dated his witness statement to say that he has recently taken up post as Head of Intelligence for Warwickshire Police.

Submissions

32. The Tribunal is grateful to all counsel for their helpful written and oral submissions. We record here the open submissions only, as the closed arguments are detailed in the closed annexe to this Decision.

33. Mr Bunting's skeleton argument submitted that, from the evidence of Ulf Buermeyer and Nathan Freed Wessler, there was no suggestion that the high degree of transparency adopted in Germany and the USA regarding the use of IMSI catchers had had any negative impact on national security or police operations. He submitted that it was 'difficult to understand' MPS's case that confirming or denying whether it holds the information requested would undermine future operations and put people's lives at risk because there is information already in the public domain domestically and internationally and no evidence that the availability of this information has impacted on policing or national security in any way. In oral submissions, he suggested that MPS, having been put on notice of this submission, bore the burden of refuting it through evidence.

34. In respect of s. 23 (5), Mr Bunting submitted that an absolute exemption must be construed narrowly because the 'default' position under FOIA was one in favour of disclosure. He submitted that the Decision Notice had taken too broad a view of the test for engagement of this exemption and that the evidence did not show a connection sufficient to bring the requested information within it.

35. As to s. 24 (2), Mr Bunting submitted that the Decision Notice had taken too broad an approach to determining its engagement. He submitted that a police force which revealed that it did not use IMSI catchers would not thereby be confirming that it could not obtain operationally-sensitive information by other means. Further, he submitted that knowing which police forces possess IMSI catchers would not allow an individual to map or be aware of how much information is obtained, or identify more vulnerable areas to commit crime.

36. Turning to s. 31(3), Mr Bunting submitted that MPS had not made an adequate case for the Tribunal to consider its engagement.

37. Mr Bunting's submissions on the public interest test were that confirming or denying whether the requested information was held would be an important contribution to a public debate about surveillance and privacy rights; that there is significant information about the use of IMSI catchers by UK police already in the public domain; that there is a clear public interest in holding an informed debate; and in the public being informed whether public money is being spent on something which is or is not regulated.

38. Mr Bunting confirmed that he did not ask the Tribunal to rule on the adequacy of the legal safeguards as to the use of CCDC or IMSI catchers, but referred us to the public clamour for information about the technology, as shown by the press reports, questions asked in Parliament and the involvement of Privacy International as a privacy watchdog. He submitted that the greater the potential for arbitrary use of the technology, the greater the need for an informed public debate.

39. As to Privacy International's role, Mr Bunting submitted that the role of the information requester is not irrelevant where it has a watchdog function and requests information in order to exercise its rights under Article 10 ECHR, referring us to the ECtHR judgment in *Magyar Helsinki Bizottsag v Hungary* (18030/11).

40. Mr Knight's skeleton argument on behalf of the Information Commissioner referred to the Upper Tribunal's Decision in *Savic* v *Information Commissioner, Attorney General's Office and Cabinet Office* [2016] UKUT 535 (AAC) at paragraph 60, in which a NCND response was described as a protective concept to stop inferences being drawn about the existence of types of information and enables an equivalent position to be taken on other occasions. He submitted that a NCND approach was permissible in MPS's case because the evidence showed there had been no direct public confirmation by it (or other forces) that any of them use IMSI catchers, still less which of them use IMSI catchers. Whilst the Appellant had drawn together a range of materials, it had not produced confirmatory proof. He drew the Tribunal's attention to the evidence of risk that confirmation or denial of the position by any force would allow a map to be created of where such equipment was available for use and thus allow terrorists or criminals to locate themselves in other areas. He submitted that the avoidance of this risk plainly engaged the exemptions at s. 24(2) and s 31 (3) FOIA.

41. Mr Knight acknowledged that MPS was entitled to rely on s. 31 (3) FOIA before the Tribunal. He submitted that the *"would be likely to"* limb of s. 31 (3) was engaged by the open evidence before the Tribunal which was to the effect that confirmation or denial would be likely to prejudice law enforcement by informing serious criminals of a significant potential investigative technique and thus enable them to seek to avoid the application of it.

42. In relation to s. 24 (2) FOIA, Mr Knight submitted that the term "national security" has been interpreted broadly by the Tribunal and higher courts. He reminded the Tribunal that two policing bodies responsible for policing organised crime were within the list of bodies at s.23 (3) FOIA: the National Crime Agency ("NCA") and its predecessor body, the Serious Organised Crime Agency. Also, that the NCA has statutory power (see section 5 (5) Crime and Courts Act 2013) to direct any other force to carry out a task on its behalf. He also drew our attention to the Security Services Act 1989 and the Intelligence Services Act 1994 which each confer on the security agencies a statutory power to support other law enforcement agencies in the prevention and detection of serious crime.

43. Mr Knight submitted that, whilst not all crime would fall within the ambit of s. 24 (2), national security considerations should be understood to be engaged by serious organised crime. He submitted that the Tribunal should afford the open evidence given by DSU Nolan and DSU Williams in this appeal respect, as their professional experience, understanding and judgement qualified them to make a predictive assessment as to the likely effect of

confirmation or denial. He described their evidence in this appeal as "clear, cogent and common-sensical".

44. Turning to the public interest balance, Mr Knight submitted that the Commissioner had accepted the weighty public interests in transparency, accountability and advancing public understanding in relation to the issues raised in this appeal and to the public interest in debating the issues, but had correctly favoured the public interest in avoiding a confirmation or denial which was likely to undermine national security. In his submission, similar public interest considerations should be applied to the detection and prosecution of offenders. He submitted that, even where the likelihood of a particular harm to national security occurring may be assessed as low, the serious nature of that risk meant that the public interest in avoiding it is strong.

45. As to s.23 (5), Mr Knight submitted that it may be unnecessary, in the light of the other exemptions, for the Tribunal to determine its application. If we were minded so to do, his submission was that s. 23 afforded the widest protection of any of the FOIA exemptions - see *Home Office v Information Commissioner and Cobain* [2015] UKUT 27 (AAC). He submitted that a plain reading of *"relates to"* should be adopted. Meaning *'connected with'* or *'arising out of'.* He reminded the Tribunal that in *APPGER v Information Commissioner and FCO* [2015] 377 (AAC), the Upper Tribunal had interpreted the phrase to mean' *some connection'* and/or *'that it touches or stands in some relation to' ...*

46. Mr Knight submitted that the Upper Tribunal's approach in *Corderoy & Ahmed v Information Commissioner, Attorney General's Office and Cabinet Office* [2017] UKUT 495 (AAC) should be followed in this case, noting the 'revelatory problem' and the risk of disclosing information about security bodies 'by the back door' via a 'yes or no' answer to this information request. He submitted that confirmation of the possession of IMSI catchers by MPS would be more likely than not to be combined with an inference of operational activity alongside s. 23 bodies and that denial would give rise to an inference that any use of IMSI catchers was carried out only by s 23 bodies themselves.

47. In his oral submissions, Mr Knight accepted that there needed to be a public debate about CCDC and its potential to interfere with privacy rights, but submitted that in the context of this appeal, this must be weighed against the public's right to live in peace and security and to be protected from harm by the state.

48. As to the position of Privacy International as a watchdog, Mr Knight's submission was that as a matter of precedent the Tribunal was bound to prefer the judgment of the Supreme Court in *Kennedy v Charity Commission* [2014] UKSC 20, that Article 10 ECHR did not encompass a right of access to state information. He noted that the Upper Tribunal is expected to rule shortly on this point.

49. Mr Talalay, on behalf of MPS, submitted that for MPS to confirm or deny whether it has the information requested (purchase orders, contracts etc.) would effectively confirm or deny whether it possesses and uses IMSI Catchers. The Tribunal should consider the impact of informing the world whether this information is held in considering the correctness of MPS's NCND stance.

50. As to s. 23 (5) FOIA, Mr Talalay submitted that the correct interpretation of *'relates to'* was *'some connection'* and that the Tribunal should resist any attempt to narrow the plain meaning of the statutory provision. He submitted that the purpose of NCND in s. 23 (5) was to keep the involvement or non-involvement of s. 23 bodies a secret, so that requiring a direct relationship to be established would undermine the purpose of the provision.

51. Turning to s. 24 (2) and s. 31 (3) FOIA, Mr Talalay submitted that the term 'national security' had been interpreted broadly and that the open evidence showed that covert policing is a central plank of policing serious crime and terrorism so that disclosing specific

capabilities would have a deleterious impact on MPS's ability to prevent crime and safeguard the nation.

52. As to the public interest, Mr Talalay submitted that significant weight should be afforded to the Police Officers' evidence as to the impact on crime and national security of confirming or denying whether the requested information is held. He suggested that public debate on these matters has been over-stated by the Appellant and that there exists a robust oversight regime to protect individual privacy rights, including judicial oversight.

53. Mr Talalay submitted that the Tribunal should place minimal weight on the information 'in the public domain' relied on by Privacy International, because it lacks specificity and contains information which is unproven and speculative. Similarly, the information made available in other jurisdictions should be viewed as having minimal relevance to this case. He noted that the Appellant had provided no evidence to support its assertion that the disclosure of information had not impacted on crime or national security.

Conclusion

54. We comment first on the terms in which the information request in this case was made. We note that it is phrased so as to include implicit assumptions about MPS's acquisition, possession and use of CCDC technology. Given the terms of the request, MPS was put in a position from where it would be difficult to confirm or deny whether it held the requested information without revealing whether these underlying assumptions were correct. It seems to us that a request made in such terms is more likely to elicit a NCND response than one which is phrased more neutrally.

55. We accept MPS's evidence that it has never made a public statement about its use or otherwise of IMSI Catchers. We note that the MPS's published budgetary information refers to "CCDC" only, and not to IMSI Catchers in particular. In contrast, we have found it difficult to assess the reliability of the considerable body of evidence relied on by Privacy International as being 'information in the public domain'. We are unable to go so far as DSU Nolan who described it as speculative, but we do note that the press reports cite either un-named police sources or quotes from former officers alongside official responses which clearly neither confirm nor deny the use of IMSI catchers (exhibits AC1/1, AC1/2 and AC1/3). We also note that the Sky News report referred to by Ailidh Callander at paragraph 9 of her witness statement apparently relied on the use of technology to detect IMSI catchers, whilst Silke Holtmanns' evidence (see paragraph 24 above) was that such methods of detection were unreliable. We conclude, as DSU Williams stated, that even when specific tactics are discussed, people are not aware of their capabilities, limitations, or the true nature of how they are used. This evidence supports, in our view, the adoption of a NCND stance in relation to the detailed information requested in this appeal.

56. Our conclusion in relation to s. 24(2) FOIA is that the exemption is engaged by the information requested in this case. We note that s. 24 is not a "prejudice-based" exemption and that the word "required" has been interpreted as meaning "reasonably necessary" in other First-tier Tribunal Decisions. While these do not bind us, we also adopt this formulation, which seems to us to accord with a plain reading of the statutory provision.

57. We accept Mr Knight's submission that the term "national security" should be understood to encompass threats from terrorism and also from serious organised crime. The open evidence from DSU Williams and DSU Nolan supported such an approach, and their closed evidence gave us greater detail. They explained in their open evidence that "safeguarding" national security involved protecting the public from all such threats and saving lives.

58. As to s. 31 (3) FOIA, our conclusion is that it is engaged by the information requested in this case. Both DSU Williams and DSU Nolan gave open evidence about the likely

prejudice to the prevention or detection of crime and the apprehension and prosecution of offenders if MPS were required to confirm or deny the matters raised in the information request. We found their evidence on this point cogent and compelling, with reference to their experience of policing serious organised crime and their evidence about the use to which information of the sort requested could be put by offenders. We rely also on the evidence given in their closed witness statements and testimony. We conclude, on the basis of their evidence, that the "would be likely to" prejudice test is met.

59. In assessing the public interest balancing exercise in relation to both of the exemptions to which it applies, we remind ourselves that there is no inherent weight in a qualified exemption under FOIA. We also remind ourselves of the Upper Tribunal's analysis in *Keane v Information Commissioner, Home Office and Metropolitan Police Service* [2016] UKUT 461 (AAC) and its approach in relation to s. 24 (1) FOIA of looking for a compelling public interest in disclosure to equal or displace the compelling public interest in the safeguarding of national security. We apply the same approach to the public interest in maintaining a NCND stance.

60. We acknowledge, as did the Information Commissioner in the Decision Notice, the weighty public interest in transparency about how public funds are spent, and in promoting informed public discourse about the potential for CCDC equipment, particularly IMSI catchers, to infringe individual privacy rights. We also acknowledge the leading role that third sector bodies such as Privacy International play in such discourse. However, we do not accept that the public interest in disclosure is enhanced by the status of the requester under FOIA. We regard the "applicant blind" approach taken by this Tribunal over many years as fundamentally important to the protection of the right to information requested by ordinary citizens. We are not persuaded that the ECtHR's judgment in *Magyar* disturbs that approach as we are bound as a matter of precedent to rely on the domestic authority of *Kennedy,* cited above.

61. Those conclusions are sufficient to dispose of this appeal and we agree with Mr Knight that we do not need to go on to determine the application of s. 23 (5) FOIA. However, we are conscious of the seven cases stayed behind this appeal and we hope that it will be helpful for us to set out our conclusions on this issue also. We accept that the engagement of this provision is more problematic than the others and make clear that, if we are wrong in our analysis, we would dismiss the appeal in any event.

62. We are satisfied that the phrase *"relates to"* in s. 23 FOIA should be given its plain meaning, as the Upper Tribunal has decided. We find no support in the authorities for Mr Bunting's principle of narrower construction or for his submission that s. 23 should be construed in the context of a presumption in favour of disclosure under FOIA. On the contrary, we are mindful of the absolute nature of the s. 23 exemption (described by Mr Knight at paragraph 45 above as affording 'the widest protection of any of the FOIA exemptions') and the clear intention of Parliament in enacting such a rigid provision. We adopt the Upper Tribunal's approach of being conscious of the 'revelatory problem' particularly, as in this case, where similar requests have been made to a number of public authorities.

63. We accept Mr Knight's submissions as to the statutory nexus between the MPS and the s. 23 bodies, including the NCA. We also accept DSU Williams' open evidence about joint covert operations between MPS and NCA. Having also considered the closed evidence, we conclude that the information requested should be regarded as *'relating to'* the s. 23 bodies. We are mindful of the Upper Tribunal's guidance in *Savic* that a NCND response is to be understood as a protective concept to stop inferences being drawn about the existence of types of information. Given the terms in which the information request was made, it seems to us that the risk of inference being drawn about the existence of the information requested is significant.

64. We have accepted the evidence of both police witnesses in this appeal. We have not done so uncritically, but having regard to their long experience of policing and the specialist roles they both now hold, which gives them knowledge of matters known to very few people. We also do so having heard their oral evidence and responses to cross examination. We have also had regard to the evidence given in closed session which supports the views they have expressed in their open witness statements.

65. We do not rely on the Appellant's un-evidenced assertion that greater transparency in other jurisdictions has not impacted negatively on policing or national security. We do not accept that the Respondents had a duty to rebut an un-evidenced assertion. It does not seem to us that this particular assertion is, in any event, likely to be capable of proof either way.

66. Having balanced all these considerations with reference to the open and closed evidence, we conclude that the public interest favours maintaining the NCND responses under s. 24(2) and s. 31(3) FOIA in this case. We accept the open evidence of DSU Williams and DSU Nolan that lives would be put in danger by the confirmation or denial of holding the information requested because if criminals or terrorists knew about the capabilities and location of covert technology, they would be likely to adjust their behaviour accordingly. We conclude that the acknowledged public interest in transparency does not outweigh such a weighty case for a NCND stance in these circumstances.

67. For the reasons given above, we now uphold the Decision Notice and dismiss this appeal.

Signed

Judge Alison McKenna
Chamber President

Date: 28 October 2019
Promulgation Date: 20 December 2019

Corrected Decision

Date: 18 February 2020