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

Case Number EA/2018/0170

PRIVACY INTERNATIONAL

Appellant

and

THE INFORMATION COMMISSIONER

First Respondent

POLICE AND CRIME COMMISIONER FOR WARWICKSHIRE

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: Alex Ustych, counsel, instructed by Warwickshire County Council Legal Services

DECISION ON EA/2018/0170

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 Police and Crime Commissioner for Warwickshire ("PCCW") to that request. PCCW took the view that the requested information was exempt from disclosure under sections 24(1) and 31 (1) FOIA and that the public interest favoured maintaining those exemptions. Privacy International complained to the Information Commissioner.

3. The Information Commissioner issued Decision Notice FS50728057 on 10 July 2018, in which she decided that PCCW was entitled to rely on s. 24 (1) FOIA to refuse to provide the requested information and that the public interest favoured maintaining the exemption. She did not determine the engagement of s. 31 (1) 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 extant appeals arising from the original series of information requests. These have been stayed pending the outcome 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 material as it constituted the withheld information or was revelatory of it. 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 material and our conclusions about it. This will not be disclosed to Privacy International.

6. This is the Tribunal's decision in relation to PCCW only. Our Decision in the other case we heard, EA/2018/0164, 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 PCCW:

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

I refer, in particular, to the recent article written by the journalist collective The Bristol Cable titled "Revealed: Bristol's police and mass mobile surveillance". The article makes reference to the minutes of an Alliance Governance Group meeting in May 2016 between Warwickshire and West Mercia Police in which the topic of ... CCDC equipment was discussed.

Specifically, the minutes record that three options relating to "CCDC replacement" were discussed:
'Option one -upgrading the existing equipment with the current supplier.
Option two -replacing the existing equipment with the current supplier's new product.
Option three -Replacing the existing equipment with a new supplier'.

The minutes go on to observe that: "Within the West Midlands region both West Midlands and Staffordshire Police have recently purchased and operated 4G compatible CCDC equipment. Both have purchased the same equipment from the company referred to in option 3". The minutes indicate that the following decision was made: 'Both PCCs [West Mercia and Warwickshire Police and Crime Commissioners] agreed to replacing the existing equipment with a new supplier'.

[Name]... requests the following records:

1. *Records relating to the purchase of "existing" CCDC equipment, referred to in the...minutes above including purchase orders, invoices, contracts, loan agreements, solicitation letters, correspondence with companies and other similar records.*
2. *Records relating to the purchase of replacement CCDC equipment referred to in the...minutes above, including purchase orders, invoices, contracts, loan agreements, solicitation letters, correspondence with companies and other similar records.*
3. *Records relating to the decision 'to replace the existing [CCDC] equipment equipment with a new supplier referred to in the...minutes above, including any records referred to or consulted in reaching that decision'.*

4. "

8. The fourth paragraph of the request is not relevant to this appeal, as it should have been addressed to a different public authority. The Information Commissioner commented in her Decision Notice that PCCW should have assisted Privacy International with making that request to the appropriate public authority.

9. In its initial response to the request in December 2016, PCCW stated that it held some information within the scope of parts 1-3 of the request but the information was exempt from disclosure under FOIA sections 24 (1) (national security) and 31 (1) (a) and (b) (prevention or detection of crime/apprehension or prosecution of offenders). It maintained that position following an internal review in May 2017.

The Decision Notice

10. Privacy International complained to the Information Commissioner, whose office conducted an investigation. The Decision Notice dated 10 July 2018 records that PCCW had described the information it held as "the business case regarding the replacement of existing CCDC equipment", which was provided to the Information Commissioner in confidence.

11. The Decision Notice concluded that PCCW was entitled to rely on s.24 (1) FOIA in response to parts 1-3 of the information request and that the public interest did not favour disclosure. It did not therefore determine the engagement of s. 31 (1) FOIA.

12. The Decision Notice considered at paragraphs 21 to 34 the proper interpretation of s. 24 (1) FOIA and the meaning of the term *"required for the purpose of safeguarding national security"* with reference to case law. At paragraphs 35 to 39 of the Decision Notice, the arguments in favour of, and against, disclosure with reference to the public interest test under s.2 (2) (b) FOIA were considered. At paragraph 40, the Decision Notice concluded that there was *"some valid public interest in disclosure"* as it would increase public knowledge, but at paragraph 42 it was concluded that:

> *"The Commissioner considers it clearly to be the case that the public interest in disclosure does not match the weight of the public interest in safeguarding national security. This means that her conclusion is that the public interest in the maintenance of the exemption provided by s. 24 (1) outweighs the public interest in disclosure of the requested information".*

Appeal to the Tribunal

13. Privacy International's Grounds of Appeal in respect of the PCCW Decision Notice may be summarised as follows. The Decision Notice is said to be wrong and/or unlawful because s. 24 (1) was not engaged by the particular information in dispute and, if it was, then the balance of public interest favoured disclosure.

14. The Information Commissioner's Response to the appeal may be summarised as follows. It was submitted that the Decision Notice was correct in its application of s. 24 (1) FOIA. However, the Commissioner also indicated that she anticipated supporting additional reliance by PCCW on s. 31 (1) FOIA.

15. PCCW's Response to the appeal may be summarised as follows. The Decision Notice was correct in relation to s. 24 (1) FOIA but PCCW also wished to rely on s. 31 (1) FOIA, which it had raised at an earlier stage but had not been determined by the Decision Notice.

The Law

16. 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 al/ the circumstances of the case, the public interest in maintaining the exemption outweighs the public interest in disclosing the information.

S. 24(1) provides that:
Information which does not fall within s. 23 (1) is exempt information if exemption from section 1 (1) (b) is required for the purpose of safeguarding national security.

S. 31 (1) provides that:
Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice
(a) The prevention or detection of crime,
(b) The apprehension or prosecution of offenders".

17. Both sections 24 (1) and 31 (1) are qualified exemptions and so engage the public interest balancing exercise under s. 2(2)(b) FOIA.

18. 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

19. 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.

20. Privacy International relied on four witness statements, one of which was 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'.*

21. Privacy International also relied on a witness statement from Silke Holtmans, 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. "*

22. Privacy International also 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 such responses have put a considerable amount of information into the public domain, for use in litigation and to inform public debate.

23. Privacy International also 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.

24. PCCW 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.

25. 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. "*

26. Turning to the particular withheld information in this case, DSU Nolan commented that:

> *“...if the business case were to be disclosed, it would allow terrorists and criminal networks to build up a picture of different forces' abilities to respond to the activities of these groups and thus increase the threat to the public.*
>
> *...it would seriously damage our fight against crime and terrorism should the information be made public."*

27. 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.

28. 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.

29. Cross-examined by Mr Knight on behalf of the Information Commissioner, he explained that the business case which has been withheld has more information in it than either the un-redacted minutes which had been published in error or the financial data contained within the redacted minutes. His witness statement had expressed the view that PCCW's relationship with other law enforcement agencies had been adversely affected by the inadvertent disclosure but in answer to Mr Knight he confirmed that this has not stopped anyone from doing their job.

30. PCCW also 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.*
>
> *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. "*

Submissions

31. 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.

32. Mr Bunting's skeleton argument dealt with the PCCW appeal briefly in submitting that neither the exemption at s. 24 (1) FOIA nor that at s. 31 (1) FOIA were engaged and that in either case, the public interest in maintaining the exemptions is "obviously outweighed" by the public interest in disclosing it.

33. In his oral submissions, Mr Bunting cautioned the Tribunal against automatic acceptance of the evidence of police officers and urged us to seek an objective evidential basis in support of their professional opinions. He submitted that PCCW had not demonstrated sufficiently in its open evidence that national security considerations would be impacted by the disclosure of the business case. He urged the Tribunal to ask itself what the business case tells us that is different to the information already in the public domain. In his submission it was unlikely that the business case would tell us the "how, when and why" of current usage or how the equipment might be used in the future.

34. In respect of the public interest balancing exercise, Mr Bunting submitted that Privacy International had made a strong case for disclosure. He referred us to Privacy International's witness evidence which, in his submission, demonstrated that there is already significant information in the public domain and that greater transparency, as demonstrated in the USA and Germany, had not been shown to impact negatively on national security or police operations.

35. 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.

36. As to Privacy International's role, Mr Bunting submitted that the role of the 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).

37. Mr Knight's skeleton argument on behalf of the Information Commissioner, acknowledged that PCCW was entitled to rely on s. 31 (1) FOIA before the Tribunal. He submitted that the "would be likely to" limb of s. 31 (1) was engaged by the open evidence before the Tribunal because it provided the Tribunal with a basis for concluding that disclosure of the information in the business case would inform serious criminals about a significant potential investigative technique and thus enable them to seek to avoid the application of it.

38. In relation to s. 24 (1) FOIA, Mr Knight submitted that the term "national security" has been interpreted broadly by the Tribunal and higher courts. Even where the likelihood of a particular harm to national security occurring may be assessed as low, the serious nature of the risk means that the public interest in avoiding it is strong.

39. Mr Knight submitted that, whilst not all crime would fall within the ambit of s. 24 (1), national security considerations should be understood to be engaged by serious organised crime. He submitted that the Tribunal should afford the 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 disclosure. He described their evidence in this appeal as "clear, cogent and common-sensical".

40. 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 disclosure 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 referred the Tribunal to the Decision of the Upper Tribunal in *Keane* v *Information Commissioner, Home Office and Metropolitan Police Service* [2016] UKUT 461 (AAC), which concluded at [58] that:

> *"Whilst it may well be wise to avoid characterising particular exemptions as carrying 'inherent weight' ... the reality is that the public interest in maintaining the qualified national security exemption in section 24 (1) is likely to be substantial to require a compelling competing public interest to equal or outweigh it" ...*

41. 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 this must be weighed against the public's right to live in peace and security and to be protected from harm by the state.

42. 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.

43. Mr Ustych, on behalf of PCCW, supported Mr Knight's submissions. In relation to s. 24 (1) FOIA, he drew the Tribunal's attention to DSU Nolan's evidence that the term "national security" encompassed risks not only from terrorism but also from serious organised crime. In respect of s. 31 (1) FOIA, he drew the Tribunal's attention to DSU Nolan's evidence as to the increasingly 'tech-savvy' nature of offenders.

44. Commenting on Privacy International's submissions about the information already in the public domain, Mr Ustych submitted that the issue is more nuanced than Mr Bunting had suggested, because the degree of specificity, certainty and correctness of that information was relevant. The evidence from DSU Nolan was that Privacy International's evidence was speculative. This, in Mr Usych's submission, undermined Privacy International's argument that a meaningful public debate could not take place without disclosure.

45. As to the public interest test, Mr Ustych submitted that in respect of both s. 24 (1) and 31 (1) FOIA, the Tribunal must consider how serious the potential harm from disclosing the business case is. Even if the risk of harm were small, the severity of the consequence was, on the evidence, high. Mr Ustych submitted that Privacy International's evidence about transparency in America and Germany (a) did not purport to be a study of all jurisdictions where such technology was used and (b) was not given by witnesses with experience of law enforcement in this country. As to the domestic oversight regime, he referred the Tribunal to the recent judgment of the Divisional Court in R *(National Council for Civil Liberties) v Secretary* of *State for the Home Department* [2019] EWHC 2057 (Admin) in which a Human Rights Act challenge to Part V of the Investigatory Powers Act 2016 had been dismissed.

46. In his submissions in reply, Mr Bunting suggested for the first time that a redacted version of the business case might be disclosed. Neither Mr Knight nor Mr Ustych was able to support that proposal.

Conclusion

47. Our conclusion in relation to s. 24(1) 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.

48. 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.

49. We have adopted Mr Bunting's sensible approach of asking ourselves what the business case tells us that is different to the information already in the public domain. In undertaking this exercise, 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 Homans' evidence (see paragraph 21 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. We have assessed the information in the business case itself in the light of this conclusion and find that it does tell us things that are different to what is in the public domain via both the minutes disclosed in error and generally.

50. We accept the evidence of both police witnesses that the business case should be regarded as exempt from disclosure for the purpose of safeguarding national security. We do not accept their evidence uncritically, but have done so having considered 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 have also had regard to the evidence given in closed session which supports the views they have expressed in their open witness statements.

51. We are accordingly satisfied that the information contained in the business case, which is different to the information in the public domain, engages the exemption for the purpose of safeguarding national security. We consider the public interest balancing exercise in relation to the engagement of s. 24 (1) FOIA below.

52. Our conclusion in relation to s. 31 (1) (a) and (b) is that the exemption is engaged by the information withheld 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 the business case were disclosed. For the reasons given above, we find their evidence on this point reliable with reference to their experience of policing serious organised crime and their evidence about the use to which information of the sort contained in the business case would 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.

53. In assessing the public interest balancing exercise in relation to both of the exemptions which we have found to be engaged by the withheld material, 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* 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 detecting crime and bringing offenders to justice.

54. 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.

55. Having balanced those considerations with reference to the open and closed evidence, we conclude that the public interest favours maintaining both the exemptions in this case. We accept the open evidence of DSU Williams and Nolan that lives would be put in danger by the disclosure (including via a 'mosaic effect') of the information contained in the business case because if criminals or terrorists knew about the capabilities of covert technology, they would adjust their behaviour accordingly. We conclude that the acknowledged public interest in disclosure does not outweigh such a weighty case for non-disclosure.

56. We do not consider that a redacted business case could be disclosed because the extent of the redactions necessary to give effect to our Decision would render the information disclosed useless.

57. 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