Freedom of Information Act 2000 (FOIA)

Decision notice

Date:	**8 February 2024**
Public Authority:	**Commissioner of Police of the Metropolis**
Address:	**New Scotland Yard** **Broadway** **London** **SW1H 0BG**

Decision (including any steps ordered)

1. The complainant has requested various details in connection with 18 invoices listed in its expenditure logs from the Metropolitan Police Service (the "MPS"). The MPS disclosed a small amount of information. Regarding the remainder of the request, it variously cited sections 24(1) (National security), 31(1) (Law enforcement), 40(2) (Personal information) and 43(2) (Commercial interests) of FOIA. It would also neither confirm nor deny ("NCND") holding information by virtue of the provisions in sections 24(2), 31(3), 40(5) and 43(3) of FOIA. The complainant did not contest the citing of section 40.

2. The Commissioner's decision is that sections 31(1) and 31(3) were appropriately cited in respect of the remaining part of the request in its entirety. He does not require any steps.

Request and response

3. On 13 February 2023, the complainant wrote to the MPS and requested the following information:

> "I'm seeking copies of any purchase orders, contracts, and/or memorandums of understanding [MOU] that relate to the following items listed in the Metropolitan Police Service expenditure logs".

4. The request went on to list 18 invoices, giving the following information for each: supplier name, supplier number, invoice number, invoice date and invoice amount.

   (It is here noted that the MPS has advised the Commissioner that most of the invoices had originally been published in error, as they related to goods / services which it considered confidential due to their nature. The MPS advised that this error has since been rectified and the Commissioner understands that information about these invoices is no longer on its website. Whilst unfortunate, the Commissioner will not compound the error by reproducing details of the invoices in this notice and he has accepted the MPS' arguments, having recognised its mistake. The findings are therefore based on the position as it should have been were the error not made.)

5. On 22 June 2023, the MPS responded, apologising for the delay. It partially disclosed two invoices, citing sections 31(1), 40(2) and 43(2) of FOIA for the withheld details. It refused to provide eight invoices, citing sections 24(1), 31(1), 40(2) and 43(2) of FOIA. It would NCND holding information in respect of the other eight invoices by virtue of sections 24(2), 31(3), 40(5) and 43(3) of FOIA.

6. The complainant requested an internal review on 20 July 2023. He said:

   > "I believe it is clear from my initial request that I was seeking copies of **any** and **all** purchase orders, contracts, and memorandums of understanding. The refusal notice suggests that my request has been interpreted as allowing the MPS to consider disclosing only purchase orders. This appears to be a wilful misinterpretation of my request".

7. He raised further arguments in respect of each of the exemptions cited, but accepted that section 40 could be properly cited to withhold any personal information.

8. The MPS provided an internal review on 19 September 2023 in which it maintained its position.

9. During the Commissioner's investigation the MPS again revised its position. It explained that some of the invoices had been published in error and were no longer available online. In light of this, it revised its position and confirmed that it held eight of the 18 invoices. It said that any further information about them was exempt from disclosure, citing sections 31(1), 40(2) and 43(2) of FOIA, as well as section 24(1) for six of these eight. In respect of the remaining ten invoices, it would NCND holding any information, citing sections 24(2), 31(3), 43(3) and 40(5) of FOIA.

Scope of the case

10. The complainant contacted the Commissioner on 20 September 2023 to complain about the way his request for information had been handled. He said:

> "The Metropolitan Police Service has refused to disclose information I have requested. I believe the authority has incorrectly relied upon sections 24, 31 and 43 to support this decision.
>
> In addition, the authority has refused to confirm or deny the existence of other information I have requested - despite the existence of this information already being a matter of public record".

11. No reference was made to the application of section 40 so this has not been further considered.

12. Part of the request refers to Contracts or MOUs. The Commissioner queried this point with the MPS and was advised that the appropriate Director had been consulted who said: "We have no MOU's with any of these suppliers, they are all straight forward contracts". The Commissioner has therefore considered the disclosure of any contracts that may be held in his analysis below.

13. The complainant asked the Commissioner to consider the application of exemptions to the request.

14. The Commissioner has reached his decision in this case taking into account several arguments which were provided 'in confidence' by the MPS. He is unable to reproduce this rationale here.

15. The Commissioner has viewed any relevant information.

Reasons for decision

16. Where the Commissioner refers to 'invoices', he is also taking into consideration any contracts that may or may not be held, as the exemptions have been applied equally to both.

Invoices which the MPS has confirmed holding

17. The Commissioner is first considering any information which has been withheld by the MPS in respect of the eight invoices it has confirmed holding. For the complainant's convenience, these were at positions 1, 3, 4, 5, 8, 9, 11 and 18 in his original request.

18. This information has been withheld in its entirety under sections 31(1), 40(2) and 43(2) of FOIA; section 24(1) has also been relied on for six of these invoices (positions 1, 3, 4, 5, 11 and 18).

19. As the MPS has cited 31(1) to cover all of the information, this is what the Commissioner has considered first.

Section 31- Law enforcement

20. Section 31 of FOIA allows a public authority to withhold information which, if disclosed, could harm its own, or another public authority's, ability to enforce the law.

21. In this case, the MPS is relying on subsections (1)(a) and (b) to refuse disclosure of the information. These apply where disclosure would, or would be likely to, prejudice:

    (a) the prevention or detection of crime; and
    (b) the apprehension or prosecution of offenders.

22. Section 31 is a prejudice-based exemption. This means a public authority can only rely on it where disclosing the information (or confirming or denying that it holds the information) could cause harm. To demonstrate the harm, it must satisfy a prejudice test.

23. In order for the exemption to apply, it must be the case that if the withheld information was disclosed, it would, or would be likely to, cause prejudice (ie harm) to the matters referred to in subsections (a) and (b). Three criteria must be met:

    - the prejudice which the MPS envisages as a result of disclosure, must relate to the prevention or detection of crime and the apprehension or prosecution of offenders;

    - there must be a causal relationship between disclosure and prejudice to those matters. This prejudice must be real, actual or of substance; and

    - the MPS must show that the level of prejudice it envisages is met – ie it must demonstrate why disclosure 'would be likely' to result in prejudice or, alternatively, why disclosure 'would' result in prejudice.

24. The MPS has relied on the same reasoning for the citing of both limbs of the exemption. The Commissioner recognises that there is an overlap within these limbs of section 31(1) so he has considered them jointly here.

25. The MPS explained to the complainant:

"…disclosing detailed information about MPS systems, software, databases and the like leaves the MPS open to cyber-attack by those who perceive that there are vulnerabilities in MPS systems and software. Cyber attackers could build up a picture of what controls the MPS has in place from detailed disclosure of contract information and use this to essentially map out routes of attack on MPS IT systems and services.

Whilst not questioning your motives, we have to be mindful that FOIA disclosures are applicant blind and we have no control over what is done with disclosed information. If we provide detailed information about software and systems which we use for core policing functions, if this information is not in the public domain, this leaves the MPS open for attack as an attacker could look for specific vulnerabilities in that software / hardware in order to try and launch an attack".

26. The MPS explained to the Commissioner:

"The police have a recognised duty to prevent crime and disorder and when it occurs, investigate those committing offences. A fundamental part of that process is the collation of information and the formulation of tactics based upon intelligence obtained to prevent crime and arrest those when crime is committed.

…In today's world it is imperative for the MPS to have the ability to use technology as a significant and evolving tactical option in respect of criminal investigations and intelligence gathering. The pace of development is breath-taking and it is essential that the capability of the police is in no way compromised or undermined. In this fast-moving technical environment is enhanced [sic], without fear that any use of products used as tactics is disclosed under FOI, rendering them less effective.

It is well established that police forces use evolving technologies to counteract criminal behaviour. Disclosing further details in respect of the MPS's operational capabilities would result in law enforcement vulnerability. Criminals / terrorists could gain a greater understanding of the methods and techniques used by the police, enabling them to take steps to counter them. Providing this information across the whole of the UK would allow them to target specific areas. This would be to the detriment of providing an efficient policing service and a failure in providing a duty of care to all members of the public.

Disclosure of the requested information would have the effect of highlighting whether how and where highly sensitive technologies are being utilised. This in itself may reduce the efficacy of these

technological advances and mean that the criminal fraternity might be better placed to avoid i.e. if the criminals know that certain technologies are being utilised, they will take counter-measures and/or operate in an alternative force area.

The information being requested although appearing to be just for the purchase orders, contracts, and/or memorandums of understanding however disclosure could inadvertently disclose a lot more information if it were to be released because of the very specific nature of the held information.

… disclosing the withheld information … would describe to those concerned exactly what type of technologies / techniques / intelligence the MPS hold. This in itself would be likely to prejudice the prevention of crime".

27. When seeking an internal review, the complainant argued:

"The refusal notice states: 'If it is known that a particular piece of software has weaknesses and a force was to disclose they use this then those weaknesses could be exploited. A cyber-attack could negatively affect the infrastructure of policing. By affecting the infrastructure of policing the nation's security will be more vulnerable to terrorism.' The refusal notice also states that the requested information 'would better inform a criminal on how to cyber-attack the police'. I dispute the assertion that the MPS must maintain secrecy over the software it uses in order to maintain cybersecurity. I observe that the MPS does not appear to acknowledge this concern in its cybersecurity advice to other organisations. The Little Leaflet of Cyber Advice[1], published by the MPS, offers 10 cybersecurity tips. None of these state the need for secrecy around the software an organisation uses".

28. In its internal review, the MPS countered this, saying:

"Policing is an information-led activity and information security is fundamental in protecting MPS assets and information (and the ICT infrastructure systems that hold it) from loss or unauthorised access, disclosure or modification. In order to safeguard against malware, viruses and the like, the MPS has measures in place to ensure that our ICT infrastructure is as secure as possible.

[1] https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/fraud/met/little-leaflet-cyber-advice.pdf

> … Criminal groups are increasingly sophisticated, particularly in the area of cyber-crime. The review agrees with our initial response which stated that disclosure of the requested information in full could, over a period of time and a number of disclosures, identify areas of MPS cyber security which criminals consider to be vulnerable to attack. This would prejudice the ability of the MPS to maintain its cyber security which would directly hinder the ability of the MPS to both prevent and detect crime. The release of any information that is likely to prejudice the ability of the MPS to both prevent and detect crime is unlikely to be in the public interest.
>
> … In recent years, large organisations have been the targets of cyber-attacks. For example, in 2017 the NHS was one of many organisations and businesses who were affected by the Wannacry cyber-attack.[2] This and many other attacks has highlighted the need for diligence in respect of information security. The MPS accepts that there is a public interest in transparency and in informing the public about the allocation of public resources in the area of the purchase of technology and security measures to protect these systems. However, there can be no stronger public interest indicator favouring withholding some of the requested information than when tangible harm to the ability of the MPS to both prevent and detect crime would result from the release of information in full".

29. The MPS has confirmed to the Commissioner that it was relying on the lower level of likelihood, ie that prejudice would be likely to occur.

30. The Commissioner is satisfied that the harm the MPS envisages clearly relates to the prevention or detection of crime and the apprehension or prosecution of offenders.

31. As regards a causal relationship between disclosure and prejudice to the above matters, having viewed the withheld information and considered the arguments above, the fuller rationale provided in the internal review and the MPS' response to his investigation enquiries, the Commissioner is satisfied that disclosure would be likely to allow interested parties to build up a detailed picture of the MPS's law enforcement practices, capabilities and tactics. Such knowledge could be used to exploit perceived weaknesses.

---

[2] https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf

32. The Commissioner accepts that the lower level of prejudice (ie that disclosure 'would be likely to' prejudice the matters protected by sections 31(1)(a) and (b) of FOIA) applies. He considers that there is a real and significant risk of disclosure causing harm to the prevention or detection of crime and the apprehension or prosecution of offenders.

33. As the three criteria set out in paragraph 23 are satisfied, the Commissioner has gone on to consider the public interest test.

Public interest test

34. Sections 31(1)(a) and (b) are qualified exemptions and are subject to the public interest test set out in section 2 of FOIA. The Commissioner has considered whether, in all the circumstances of this case, the public interest in maintaining the exemption outweighs the public interest in disclosing the withheld information.

Public interest arguments in favour of disclosure

35. When requesting an internal review, the complainant argued:

> "The refusal notice acknowledges that "the public are entitled to know how public funds are spent and how resources are distributed within an area of policing". In fact, since 2012 it has been a legal requirement[3] that chief officers publish "information on expenditure and contracts" to "ensure that the public has a complete picture of all police spending". The government advises that this information should include both "the recipient" and "the purpose of the expenditure". Releasing the requested information would go some way towards fulfilling this requirement. In addition to transparency as to how public funds are spent, I contend that the public is also entitled to transparency regarding the role that private technology companies play in UK policing. Indeed, the MPS has itself made this argument in a recent submission[4] to a House of Lords inquiry, stating: 'The use of technology including the importance of community engagement and transparency. This is an important part of the ethical use of technology'."

[3] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/143836/publishing-information.pdf

[4] https://committees.parliament.uk/writtenevidence/38736/html/

36. The MPS said that it acknowledged and recognised the value in public transparency and accountability in police activities and accepted that disclosure would ensure the confidence and trust of the public.

37. It also argued:

> "As the information relates to commercially confidential information, namely purchase orders, contracts, and/or memorandums of understanding with named companies used by the MPS it would show the MPS to be open and transparent about how the MPS fulfils its core function of law enforcement. It would also show the MPS to be open in terms of the use of public funds to tackle crime".

Public interest arguments in favour of maintaining the exemption

38. The MPS has explained:

> "Disclosing the requested information could risk prejudicing or undermining the operational integrity of policing that would be likely to adversely affect public safety and have a negative impact on the ability of the MPS to protect the public and uphold the law.
>
> Although the 'public interest' is not defined in the Act, previous case law has formed an understanding of the term. It has been agreed that the public interest is not what interests the public, but what will be of greater good if released to the community as a whole. Therefore, whilst the MPS appreciates an individual may have a genuine interest in this matter, it is not in the public interest to disclose information that may compromise the services [sic] ability to fulfil its core function of law enforcement or jeopardise the safety of the public.
>
> It is important the MPS is not compelled to reveal information which would adversely affect its ability to find new ways to combat crime and gather intelligence or even impact current police operations or investigations. The purchase orders, contracts, and / or memorandums of understanding would idenify [sic] areas of interest as it may also suggest (whether correctly or not) the limitation of police capabilities in a given area, which may further encourage criminal activity by exposing potential vulnerability. Any compromise no matter how minimal it may appear would substantially prejudice the ability to police these areas which would lead to a greater risk to the public.
>
> Disclosure of purchase orders, contracts, and/or memorandums of understanding would technically be releasing sensitive operational information into the public domain which would be far more revealing. It would demonstrate exactly where the MPS look which in turn would enable those with the time, capacity and inclination to

map strategies used by the MPS resulting in it being harder for the MPS to monitor and prevent. Some products may be used for very sensitive operational purposes.

There is no doubt individuals are able to use publicly disclosed intelligence to counter measure the police and use against them. Disclosing any products used could put at risk and highlight to members of the criminal fraternity the considerations, capabilities and tactical options available to the MPS. There is a key link between disclosure and harm (sensitive in nature) by providing those individuals who would wish to cause harm with invaluable intelligence. Once information is disclosed and in the public domain we are not only unable to retract it but it is not known what use that information will have. The mosaic effect can be such that the confirmation of particular information could undermine operational effectiveness. For example, if the MPS disclosed the details of a particular named contract and the description of the purchase order / product, an open source search could identify the type of business the company in question relates to and the product ordered could disclose various sensitives we would not want in the public domain for all to know such as a covert investigation tool which may lead to an individual to ascertain where or how the intelligence was gathered. This would have a seriously detrimental effect to the operational capabilities and could also hinder the possible prevention and detection of crime by revealing capabilities and methodologies.

Consideration has to also be given to the fact that once disclosure is made for all purchase orders, contracts, and/or memorandums of understanding this could potentially therefore set a bad precedent for disclosing operationally commercially sensitive information in the future which would not be of public interest.

Whilst there may be information in the public domain which purports to disclose information on our tactics / technologies used / intelligence platforms / information gathering platforms, much of this is speculative and has not been confirmed by the MPS. Criminals must be kept guessing as to the areas of interest so that they do not change their behaviour and make it more difficult to counter their threat.

Although the argument of transparency will always hold weight, this must be offset against our need to protect the public and uphold our law enforcement functions for the good of the community as a whole. Here it can be argued that we have demonstrated our commitment to transparency thorough [sic] the disclosure already made at the initial request stage and information publically [sic] available on our publication scheme".

39. Further arguments were raised which the Commissioner has taken into account but cannot publish.

Public interest balancing test

40. When balancing the opposing public interests in a case, the Commissioner will decide whether it serves the public interest better to disclose the requested information or to withhold it because of the interests protected by the relevant exemption. If the public interest in maintaining the exemption does not outweigh the public interest in disclosure, the information must be disclosed.

41. The Commissioner considers that there is a presumption running through FOIA that openness is, in itself, to be regarded as something which is in the public interest. He also recognises the need for transparency and accountability on the part of public authorities which are tasked with enforcing the law, particularly with regard to both public expenditure and the methodologies which are being used in modern policing, both of which are of public concern.

42. However, in carrying out this exercise, appropriate weight must be afforded to the public interest inherent in the exemption - that is, the public interest in avoiding prejudice to law enforcement matters. Clearly, it is not in the public interest to disclose information that would compromise the police's ability to accomplish its core function of law enforcement. If police tactics and resources are revealed, the result could impact on the safety of the wider public.

43. The Commissioner considers that the disclosure of the information could reveal strategic intentions, tactical planning information, deployment plans and intelligence. He is satisfied that this information has a considerable value to interested parties wishing to gain an advantage over the police: to ascertain what products it is using and the companies it is dealing with. The Commissioner does not suggest that the complainant intends to use the information in a detrimental way, but disclosure under FOIA is effectively disclosure to 'the world at large', with no onward restrictions on how the information may be used.

44. The Commissioner considers there is a strong public interest in protecting the law enforcement capabilities of the police, and, therefore, that appropriate weight must be given to the public interest inherent in the exemptions. That is, the public interest in avoiding prejudice to the prevention or detection of crime and to the apprehension or prosecution of offenders.

45. On balance, the Commissioner considers that the disclosure of information would undoubtedly aid the strategies of interested parties seeking to resist and disrupt policing. He finds that this outweighs the benefit which would flow from the disclosure of the information. For this

reason, the Commissioner accepts that the public interest favours maintaining the exemptions.

46. His decision is, therefore, that the MPS was entitled to rely on sections 31(1)(a) and (b) of FOIA to refuse to disclose the eight invoices it has confirmed that it holds.

47. In view of this decision, it has not been necessary to also consider the MPS' application of other exemptions to this information.

Invoices which the MPS has neither confirmed nor denied holding

48. The Commissioner is considering the remaining parts of the request.

Neither confirm nor deny ("NCND")

49. Section 1(1)(a) of FOIA requires a public authority to inform a requester whether it holds the information specified in the request.

50. The decision to use a NCND response will not be affected by whether a public authority does, or does not, in fact hold the requested information. The starting point, and main focus for NCND in most cases, will be theoretical considerations about the consequences of confirming or denying whether or not a particular type of information is held.

51. A public authority will need to use the NCND response consistently, over a series of separate requests, regardless of whether or not it holds the requested information. This is to prevent refusing to confirm or deny being taken by requesters as an indication of whether or not information is in fact held.

52. The MPS has taken the position of neither confirming nor denying whether it holds the remaining requested information, citing sections 24(2), 31(3) and 3(3) of FOIA. The issue that the Commissioner has to consider is not that of the disclosure of any of the information that may be held, it is solely the issue of whether or not the MPS is entitled to NCND whether it holds this information.

53. Put simply, in this case the Commissioner must consider whether or not the MPS is entitled to NCND whether it holds any information in respect of ten of the invoices requested.

54. The MPS has said that the invoices in question, if they were held, would be fully exempt from disclosure by virtue of the exemptions cited.

55. The MPS explained to the Commissioner:

> "The police service is charged with enforcing the law, preventing and detecting crime and protecting the communities they serve,

and the MPS will not disclose whether information is or is not held, if it might jeopardise these important functions. Therefore in this instance merely confirming or denying whether or not the MPS holds information might itself reveal something about what is held or not. Therefore we have to adopt a consistent approach when responding to similar requests and a degree of generality is inevitable when we explain why the MPS is exempt from the duty to confirm or deny.

In the Upper Tribunal's Decision in Savic[5] 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.

To highlight the potential risk of the MPS confirming or denying whether the information requested is held, the current threat for potential terrorism actions against the UK interests on the mainland is recorded by MI5[6] as 'Substantial' which means an attack is likely.

In First-tier Tribunal **EA/2018/0164** Privacy International v the ICO & MPS, relating to the purchase and use of mobile phone surveillance equipment by the MPS. Detective Superintendent Nolan's witness statement acknowledged that there is 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 referred 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**

[5] https://assets.publishing.service.gov.uk/media/59db9ac0ed915d493abd4f0a/ 2017 AACR 26ws.pdf

[6] https://www.mi5.gov.uk/threat-levels

of people who work in dedicated teams and are appropriately vetted.'"

Section 31 – Law enforcement

56. Section 31(3) provides that a public authority is not obliged to confirm or deny holding information described in a request if to do so would, or would be likely to, prejudice any of the matters mentioned in section 31(1). The relevant matters in this case are those set out at section 31(1)(a) (the prevention and detection of crime) and 31(1)(b) (the apprehension or prosecution of offenders). This is a qualified exemption, and is therefore subject to a public interest test.

57. The requirements for successfully engaging section 31 are explained above, so the Commissioner has not repeated them here.

58. The MPS explained to the Commissioner:

> "The fact that the exemptions used relate to neither confirming nor denying whether relevant information is held means that any arguments used would primarily relate to the nature of the information requested rather than the actual information that is or is not held. Furthermore, in order for these exemptions to be effective, it is necessary to respond consistently to requests for certain types of information, both when the information is held and when it is not. Therefore, a degree of generality is inevitable when explaining why these exemptions apply to this request.
>
> The MPS are relying on the threshold of 'would be likely'".

59. It also said:

> "To confirm or deny whether the MPS have or had recent contracts with the companies (including whether any details relating to services / equipment / technology etc. is held) would render law enforcement measures less effective.
>
> In consideration of the type of work highlighted on the websites of many of the companies listed (such as sensitive and various security solutions), confirmation or denial of the requested information would be likely to compromise possible ongoing or future operations to prevent or detect crime (regardless of whether information is held or not in respect of theses specific companies).
>
> Law enforcement methodology and tactics are often re-used. A consequence of this that such tactics and methodology (including equipment) can be monitored by criminal groups and activities in the hope of evading detection. To confirm or deny what recent

methods/equipment has or is being used would enable those engaged in criminal activity to identify the focus of policing activity.

Confirmation or denial of whether the MPS has used any of these companies (and to what extent) would therefore increase the risk to operational activity (whether held or not), if the answer is used as intelligence to undermine law enforcement".

60. Relying on the same rationale as applied above, the Commissioner accepts that this exemption is engaged.

Public interest test

61. The exclusion from confirming or denying whether information is held is also subject to a public interest test.

Public interest arguments in favour of confirmation or denial

62. The complainant's arguments are as presented above.

63. He also said: "the authority has refused to confirm or deny the existence of other information I have requested - despite the existence of this information already being a matter of public record", in reference to the invoices which the MPS has advised were previously published in error. On this point, the public does not automatically enjoy the same access rights to information which has previously been published in error, as they do to information which is published correctly. Public authorities are entitled to take corrective action to minimise further harm. The Commissioner has already commented regarding this point, above, and this factor will not be taken into account in his deliberations.

64. The MPS has argued:

"The public will have an interest in being aware of how public funds are spent in terms of services and equipment and which companies the MPS may or may not have contracts with particularly if it relates to law enforcement in any way.

To confirm or deny whether information is held would allow the public to gain a deeper understanding of how public funds are (or are not) spent in respect of law enforcement activity. To confirm or deny whether details of services/equipment is held in relation to these companies would provide the public with a clear awareness of what type of equipment may be used to prevent and detect crime".

65. It also explained to the Commissioner:

"In consideration of the type of work highlighted on the website of many of the companies referred to confirmation or denial of the

requested information would be likely to compromise possible ongoing or future operations to prevent or detect crime (regardless whether information is held or not).

If information were held, it would only be held for the purpose of benefitting policing. It remains the case that law enforcement methodology and tactics are often re-used. A consequence of this is that such tactics and methodology (including equipment) can be monitored by criminal gangs and activities in the hope of evading detection. To confirm or deny what recent methods/equipment has or is being used by certain companies would enable those engaged in criminal activity to identify the focus of policing activity.

Confirmation or denial of whether the MPS have used any of these companies/products (and to what extent) would therefore increase the risk of operational activity (whether held or not), if the answer is used as intelligence to undermine law enforcement. Resources are a valuable too, and it would not be in the public interest to undermine MPS capabilities by confirming or denying what equipment and contracts may or may not exist in respect of these companies.

Just as police collect information for intelligence purposes so too do those intent on committing criminal acts and release of any information relevant to this request places useful information into the public domain and increases the likely 'mosaic' effect. The 'mosaic' effect is in effect the building up of a jigsaw, gradually filling in the pieces to form a complete picture. The potential adverse effect on disclosure is covered in details within the ICO's own guidance[7] in regards to the building blocks of information put together with that already in the public domain, however in this instance it could be that disclosure of the information requested builds the initial blocks of a 'mosaic' pyramid yet to be built.

…It is well established that police forces use publically [sic] available data in order to counter act criminal behaviour. It is has [sic] been previously documented in the media that many terrorist incidents have been thwarted due to intelligence gained by these

[7] https://ico.org.uk/for-organisations/foi-eir-and-access-to-information/freedom-of-information-and-environmental-information-regulations/information-in-the-public-domain/#:~:text=This%20is%20referred%20to%20as,increasing%20the%20likelihood%20of%20prejudice.

means. However, given the sensitive areas in which tools of this type may be used and the Met's role in counter-terror investigations, to disclose if any particular products are used would allow criminal and other adversaries to focus on evaluation the [sic] particular capabilities of a particular product, with this knowledge it would allow criminals and other adversaries to take steps to counteract a specific tool – be it adjusting how they interact and present themselves to take advantage of any weaknesses or gaps in capability they identify. At a simple level, if a policing tool doesn't search 'X' social media site or was unable to identify 'Y' format of images and criminals can establish this, they will exploit this position. The Met's more sophisticated adversaries may be able to go further and take more proactive measures to undermine the products/tools and/or its provider, and a specific confirmation allows efforts to be focused accordingly.

The detrimental effect could also be increased if the request is made to several different law enforcement bodies. In addition to the local criminal fraternity now being better informed, those intent on organised crime throughout the UK will be able to 'map' where the use of certain tools/products are or are not deployed. This can be useful information to those committing crimes. It would have the likelihood of identifying location-specific operations which would ultimately compromise police tactics, operations and future prosecutions as criminals could counteract the measures used against them".

Public interest arguments in favour of maintaining the exclusion to NCND

66. The MPS has argued:

"It is not in the public interest to confirm or deny whether the MPS have or had recent contracts with the listed companies (including whether any details relating to the services/equipment is held), as it would indeed render law enforcement measures less effective.

…Whilst there is a public interest in the transparency of policing operations and in this case providing assurance that the police service is appropriately and effectively engaging with the threat posed by the criminal fraternity, there is a very strong public interest in safeguarding both national security and the integrity of police investigations and operations.

…Any information identifying the focus of policing activity could be used to the advantage of terrorists or criminal organisations. Information that undermines the operational integrity of these

activities will adversely affect public safety and have a negative impact on both National Security and Law Enforcement.

To confirm or deny would lead to an increase harm to our covert investigations and compromise law enforcement".

Public interest balancing test

67. The Commissioner has considered the MPS' submissions and, for the same reasons that he found the public interest in maintaining the exemptions at sections 31(1)(a) and (b) to outweigh the public interest in disclosure, he has reached the same conclusion in respect of the duty to confirm or deny, here.

68. In light of this decision, the Commissioner has not found it necessary to consider the other exemptions cited.

Other matters

---

69. Although they do not form part of this notice the Commissioner wishes to highlight the following matter of concern.

70. Although not referred to by the complainant, the Commissioner has made a record of the delay in the initial response in this case. This may form evidence in future enforcement action against the MPS should evidence from other cases suggest that there are systemic issues within the MPS that are causing delays.

Right of appeal

71. Either party has the right to appeal against this decision notice to the First-tier Tribunal (Information Rights). Information about the appeals process may be obtained from:

    First-tier Tribunal (Information Rights)
    GRC & GRP Tribunals,
    PO Box 9300,
    LEICESTER,
    LE1 8DJ

    Tel: 0203 936 8963
    Fax: 0870 739 5836
    Email: grc@justice.gov.uk
    Website: www.justice.gov.uk/tribunals/general-regulatory-chamber

72. If you wish to appeal against a decision notice, you can obtain information on how to appeal along with the relevant forms from the Information Tribunal website.

73. Any Notice of Appeal should be served on the Tribunal within 28 (calendar) days of the date on which this decision notice is sent.

Signed .....

Carolyn Howes
Senior Case Officer
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF