Freedom of Information Act 2000 (FOIA)

Decision notice

Date:	**4 September 2023**
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 details of the applications which are provided on mobile phones that are issued to its officers from the Metropolitan Police Service (the "MPS"). The MPS refused to provide this information citing sections 31(1)(a) and (b) (Law enforcement) of FOIA.

2. The Commissioner's decision is that the MPS was entitled to rely on sections 31(1)(a) and (b) to withhold the requested information. He does not require any steps.

Request and response

3. On 30 March 2023, the complainant wrote to the MPS and requested the following information:

> "Please accept this request under the Freedom of Information Act. I'm seeking:
>
> - A list of off-the-shelf apps provided on Android smartphone devices issued to MPS officers".

4. On 6 May 2023, the MPS responded. It refused to provide the requested information citing section 31(1)(a) FOIA.

5. The complainant requested an internal review on 16 May 2023. He said:

> "While I acknowledge your assertion that to reveal a list of off-the-shelf apps available to MPS officers "would reveal tactical capability", I disagree that this would place the MPS at a "tactical disadvantage". The refusal notice fails to illustrate how the requested information could assist criminals. It also fails to take into account the possibility that greater awareness of officers' tactical capabilities could serve as a deterrent to criminals, or cause them to adjust their behaviour in ways that make them more visible to law enforcement, enhancing the police's ability to prevent and detect crime".

6. The MPS provided an internal review on 12 June 2023 in which it maintained its position, adding reliance on section 31(1)(b).

Scope of the case

7. The complainant contacted the Commissioner on 15 June 2023 to complain about the way his request for information had been handled. His grounds of complaint were:

> "The MPS is seeking to rely on Section 31 of the FOI Act, arguing that "disclosing detailed information about applications used by the MPS leaves us open to cyber-attack by those who perceive that there are vulnerabilities in applications and products used by the MPS". However, the MPS Little Leaflet of Cyber Advice offers 10 tips to help businesses avoid cyber attacks, none of which relate to the need for secrecy over software or applications being used.
>
> https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/fraud/met/little-leaflet-cyber-advice.pdf
>
> To further illustrate this point: The MPS has cited the Wannacry ransomware attack against the NHS to highlight "the need for diligence in respect of the security of software, hardware and databases used". However, the Lessons Learned review of the Wannacry attack noted that it was possible because NHS organisations had failed to apply a software update patch — not because the attackers had gained intelligence regarding NHS software or applications".

8. The Commissioner will consider the application of section 31 to the request below. He has viewed the withheld information.

Reasons for decision

Section 31 – Law enforcement

9. Section 31 of FOIA creates an exemption from the right to know if disclosing the information would, or would be likely to, prejudice one or more of a range of law enforcement activities.

10. In this case, the MPS is relying on sections 31(1)(a) and (b) of FOIA in relation to all the withheld information. These subsections state that information is exempt if its disclosure would, or would be likely to, prejudice:

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

11. In order to engage a prejudice-based exemption such as section 31 there must be likelihood that disclosure would, or would be likely to, cause prejudice to the interest that the exemption protects. In the Commissioner's view, three criteria must be met in order to engage a prejudice-based exemption:

    - Firstly, the actual harm which the public authority alleges would, or would be likely to, occur if the withheld information was disclosed has to relate to the applicable interests within the relevant exemption;

    - Secondly, the public authority must be able to demonstrate that some causal relationship exists between the potential disclosure of the information being withheld and the prejudice which the exemption is designed to protect. Furthermore, the resultant prejudice which is alleged must be real, actual or of substance; and,

    - Thirdly, it is necessary to establish whether the level of likelihood of prejudice being relied upon by the public authority is met – ie disclosure 'would be likely' to result in prejudice or disclosure 'would' result in prejudice.

12. Consideration of the exemption at section 31 is a two-stage process: even if the exemption is engaged, the information should be disclosed unless the public interest in maintaining the exemption outweighs the public interest in disclosure.

13. Rather than differentiate between the subsections of the exemption, the MPS has presented one set of arguments. The Commissioner recognises that there is clearly some overlap between subsections 31(1)(a) and 31(1)(b) and he has therefore considered these together.

The applicable interests

14. The first step in considering whether this exemption is engaged is to address whether the prejudice predicted by the public authority is relevant to the law enforcement activities mentioned in sections 31(1)(a) and (b) – the prevention or detection or crime and the apprehension or prosecution of offenders.

15. With respect to law enforcement activities, the Commissioner recognises in his published guidance[1] that section 31(1)(a) will cover all aspects of the prevention and detection of crime. With respect to section 31(1)(b), he recognises that this subsection: "… could potentially cover information on general procedures relating to the apprehension of offenders or the process for prosecuting offenders".

16. The Commissioner acknowledges that the arguments presented by the MPS refer to prejudice to the prevention or detection of crime and to the apprehension or prosecution of offenders and that the appropriate applicable interests have therefore been considered.

The nature of the prejudice

17. The Commissioner next considered whether the MPS has demonstrated a causal relationship between the disclosure of the information at issue and the prejudice that sections 31(1)(a) and (b) are designed to protect. In his view, disclosure must at least be capable of harming the interest in some way, ie have a damaging or detrimental effect on it.

20. The MPS advised the complainant that:

> "The MPS is charged with enforcing the law and preventing and detecting crime. Any information released under the Act which reveals detailed information concerning technology we employ could prejudice the prevention and detection of crime and the apprehension or prosecution of offenders. Disclosure could potentially provide any individuals with malicious intent to target information about the products we use which could in turn aid individuals to commit attacks on applications and technology used by the MPS.
>
> To elaborate further, you have asked for information which if disclosed could be used to the detriment of the MPS as disclosing

[1] https://ico.org.uk/media/for-organisations/documents/1207/law-enforcement-foi-section-31.pdf

> detailed information about applications used by the MPS leaves us open to cyber-attack by those who perceive that there are vulnerabilities in applications and products used by the MPS. Cyber attackers could build up a picture of what security controls the MPS has in place from detailed disclosure about the software it uses and essentially map out routes of attack on applications and services MPS IT systems and services".

And:

> "If we provide information about applications used on MPS mobile phones, which is not in the public domain, this leaves the MPS open for attack. For example, if it is said that we are using a named application, then an attacker could look for specific vulnerabilities in that software in order to try and launch an attack".

18. On the evidence provided, the Commissioner is satisfied that the MPS has demonstrated a causal link between the requested information and the applicable interests relied on, and that disclosure would be likely to have a detrimental impact on law enforcement.

Likelihood of prejudice

19. With regard to the likelihood of prejudice in this case, the MPS did not specify the likelihood. Therefore, the Commissioner has considered its position at the lower level of 'would be likely to' prejudice.

Is the exemption engaged?

20. In a case such as this, it is not enough for the information to relate to an interest protected by sections 31(1)(a) and (b); its disclosure must also at least be likely to prejudice those interests. The onus is on the public authority to explain how that prejudice would arise and why it would occur.

21. The Commissioner recognises the importance of protecting information which, if disclosed, would be likely to undermine law enforcement activity.

22. Having considered the arguments put forward by the MPS, the Commissioner accepts that disclosure would be useful to someone intent on establishing any vulnerabilities which the MPS may have with the applications that its officers have access to on their mobile phones. Consequently, the Commissioner is satisfied that disclosure would be likely to represent a real and significant risk to law enforcement matters.

23. As the Commissioner accepts that the outcome of disclosure predicted by the MPS would be likely to occur, he is satisfied that the exemptions provided by sections 31(1)(a) and (b) are engaged.

Public interest test

24. Section 31 is a qualified exemption. The Commissioner must now consider whether, in all the circumstances of the case, the public interest in maintaining the exemption at sections 31(1)(a) and (b) of FOIA outweighs the public interest in disclosing the information requested by the complainant.

Arguments in favour of disclosure

25. Some of the complainant's views are included above. He has also argued:

> "The public interest arguments in favour of disclosure are clear and have been outlined by policing bodies including the Metropolitan Police Service.
>
> The National Policing Digital Strategy[2] states: "For policing to maintain its mandate to 'police by consent', the ethical questions of the application of technologies need to be carefully explored and governed." This is only possible if police forces are transparent about what technology they use and how it is deployed. In a submission[3] to a House of Lords inquiry, the Met Police made this very point, stating that "community engagement and transparency … is an important part of the ethical use of technology".
>
> It is a long established principle that when police officers are granted new capabilities, through the adoption of technology or otherwise, that these are the subject of public scrutiny and debate. For example, when Tasers were introduced to the UK in 2003, this took place after a well-publicised trial at five police forces. Disclosing a list of the off-the shelf apps available to MPS officers is essential to uphold the principle of 'policing by consent', while there is little evidence to suggest it would compromise law enforcement activities".

26. The MPS has recognised the public interest in transparency. It argued:

> "When any request for information is made to the police, it is important that the MPS are transparent, where possible, in

[2] https://pds.police.uk/wp-content/uploads/2020/01/National-Policing-Digital-Strategy-2020-2030.pdf

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

responding to that request for information. Disclosing the information held would reinforce the Met's commitment to transparency with the public.

…The public release of the list off-the-shelf [sic] apps provided on Android smartphone devices issued to MPS officers would accordingly, reinforce the MPS commitment to be an open and transparent organisation. Furthermore, it would show that the MPS have allocated their resources appropriately. As transparency is intrinsically linked to public confidence, release of the requested information would be likely to improve public confidence in the MPS".

Arguments in favour of maintaining the exemption

27. In its refusal notice the MPS argued:

"To disclose the list of off-the-shelf apps provided on Android smartphone devices issued to MPS officers would reveal tactical capability and would place the MPS at a tactical disadvantage as outlined in the harm above. It cannot be in the public interest to disclose information which would undermine our ability to detect crime. As detailed within the harm, this would be a valuable asset to individuals and/or organisations wishing to commit crimes. Those with criminal intentions would enable offenders to evade apprehension.

The release of the list would provide, persons intent on disrupting the peace and cause harm, with information that would assist them to do so. In this regard, a person with this intent would be likely to use this information to possibly commit crimes in those areas that the apps are not being used. The MPS has a duty to protect the public from harm and that duty of care to all involved must be the overriding consideration. It cannot be in the public interest to disclose information which would undermine our ability to detect crime and bring offenders to justice".

28. Further arguments were also submitted which the Commissioner has taken into account.

Balance of the public interest arguments

29. In carrying out the statutory balancing exercise in this case, the Commissioner considers that appropriate weight must be afforded to the public interest inherent in the exemption - that is, the public interest in avoiding likely prejudice to law enforcement matters. Clearly, it is not in the public interest to disclose information that may compromise the police's ability to accomplish its core function of law enforcement.

30. In that respect, he recognises that there is a very strong public interest in protecting the law enforcement capabilities of a police force and he considers that appropriate weight must be afforded to the public interest inherent in the exemption – that is, the public interest in avoiding prejudice to the prevention or detection of crime.

31. The Commissioner recognises the need to ensure transparency and accountability on the part of the police. However, whilst the complainant refers to arguments such as ethical concerns and the principle of 'policing by consent', the Commissioner can only envisage limited tangible benefit in letting the public know exactly which applications the MPS' officers use on their mobile phones.

32. The complainant himself has recognised that disclosure "would reveal tactical capability", but his view is that this would not be disadvantageous, him believing that greater awareness could act as a deterrent. However, the Commissioner recognises that there are wider concerns with this view. The world of phone applications is ever changing, and those who perpetrate crimes are likely to be in a position to be both technically advanced and knowledgeable of the latest products. Disclosure would enable them to maximise their opportunity to make use of any foreseeable shortfalls in the police's use of technology in this area of policing.

33. The Commissioner accepts that providing criminals with a list of the applications that the MPS has available to use places MPS officers at a disadvantage. He considers it highly likely that, rather than it acting as a deterrent, it would encourage those with bad intent to find ways to circumvent these products in an effort to either go undetected or cause disruption.

34. In the Commissioner's view, policing techniques can only be properly effective when full policing capabilities are not publicly known; disclosure of the data requested would be to the detriment of the wider public, as those seeking to evade the law may be able to ascertain how best to do so.

35. Having carefully balanced the opposing factors involved in this case, the Commissioner finds that the public interest in maintaining the section 31(1) (a) and (b) exemptions outweighs the public interest in disclosure.

Right of appeal

36. 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

37. 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.

38. 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