Freedom of Information Act 2000 (FOIA)

Decision notice

Date: **20 September 2018**

Public Authority: **Chief Constable of Bedfordshire Police**
Address: **Bedfordshire Police Headquarters**
Woburn Road
Kempston
Bedford
MK43 9AX

Decision (including any steps ordered)

1. The complainant has requested information about Bedfordshire Police's capabilities with regard to utilising the "Internet of Things" for law enforcement purposes. Bedfordshire Police would neither confirm nor deny whether it holds the requested information, citing the exemption at section 31(3) (law enforcement) of the FOIA.

2. The Commissioner's decision is that Bedfordshire Police was not entitled to rely on section 31(3) to neither confirm nor deny whether it holds the information.

3. The Commissioner requires Bedfordshire Police to take the following steps to ensure compliance with the legislation.

   - Confirm or deny whether information falling within the scope of the request is held, and disclose or refuse any information identified.

4. Bedfordshire Police must take these steps within 35 calendar days of the date of this decision notice. Failure to comply may result in the Commissioner making written certification of this fact to the High Court pursuant to section 54 of the Act and may be dealt with as a contempt of court.

Background

5. The complainant submitted the same request to every UK police force. The Commissioner has initially considered how six police forces handled the request, and is issuing decision notices in respect of those cases, with this being the lead case[1]. The remaining cases will be dealt with separately.

6. The complainant also submitted a further, related request to every UK police force. The Commissioner has considered those cases separately, with the lead case being FS50739828.

The Internet of Things

7. The Internet of Things ("the IoT") refers to the interconnection, via the internet, of computing devices embedded in everyday objects, enabling them to send and receive data. A recent report, "*Policing and the Internet of Things*"[2], assessed both the challenges and the opportunities presented by the IoT, defining it as:

> *"…the notion of devices and sensors – not just laptops or smartphones, but everyday objects – being connected to the Internet and to each other. This includes everything from tablets to washing machines to burglar alarms to car parking sensors. It also applies to components of larger machines, like computer systems in a passenger airliner or the drill of an oil rig. Analysts argue that by 2020 there will be an estimated 50 billion connected devices...By 2020, each person is likely to have an average of 5.1 connected devices on their person. Internet of Things (IoT) sensors and devices are expected to exceed mobile phones as the largest category of connected devices in 2018. By 2020, more than half of major new businesses will be using the Internet of Things in some capacity."*[3]

8. Although still an emerging area of technology, the IoT is expected to present significant opportunities for evidence gathering by law

[1] The other five are dealt with under the following references: FS50739835, FS50739875, FS50741036, FS50748297 and FS50744546

[2] techUK and the Centre of Public Safety, June 2017 https://www.techuk.org/insights/news/item/10985-opportunities-outweigh-the-challenges-posedby-the-internet-of-things-in-policin

[3] *Policing and the Internet of Things*, page 10

enforcement agencies. The extraction of location and other data generated by mobile phones is an increasingly common investigatory tool[4]. And recent criminal cases in the USA demonstrate the wider potential for data generated by, for example, fitness trackers[5] and pacemakers[6] to be used by law enforcement agencies in criminal investigations.

Request and response

9. On 10 August 2017, referring to *Policing and the Internet of Things*, the complainant wrote to Bedfordshire Police and requested information in the following terms:

> *"1. Do you currently have the capability to examine connected devices, also known as internet of things. i.e. what are your digital investigation and intelligence capabilities in respect of the Internet of Things. See the attached report for examples. I note the above comments of Mark Stokes[7].*
>
> *2. If you do have the capability, what software / hardware do you use and/or which companies do you contract with to provide services to examine connected devices for information, such as in the course of police investigations.*
> *- In responding to this question I note the reference to the intention of partnership with industry and academia in the attached report.*
> *- I further note the NCA's call in 2016 that "The speed of criminal capability development is currently outpacing our response as a community and … only by working together across law enforcement can successfully reduce the threat to the UK from cyber crime."*

[4] https://www.telegraph.co.uk/news/2018/03/31/police-rolling-technology-allows-raid-victims-phones-without/

[5] https://www.telegraph.co.uk/news/2017/04/25/man-charged-wifes-murder-fitbit-contradicts-timeline-events/

[6] https://www.journal-news.com/news/judge-pacemaker-data-can-used-middletown-arson-trial/Utxy63jyrwpT2Jmy9ltHQP/

[7] Head of the Metropolitan Police Digital Forensics Lab, quoted in *Policing and the Internet of Things*

3. If you do not have the capability do you have any plans to develop skills and capacity to exploit internet of things as part of criminal investigations;

4. Do you have any internal guidance and/or policies and/or national guidance or policies on the obtaining of evidence from Internet of Things / connected devices.

5. Who is your current Digital Media Investigator.

6. A November 2016 HMIC report warned about the chronic digital skills shortage in policing. Do you currently, or do you have plans, for officers to receive training in relation to extracting / obtaining / retrieving data from or generated by connected devices.

Examples of internet of things:
- Individuals: fridges, health care devices, Amazon Echo, washing machine, burglar alarms, car parking sensors, baby monitors, air conditioners, cars, speaker systems, Smart TVs, energy meters
- Business / govt : traffic light sensors".

10. Bedfordshire Police responded on 8 September 2017. It stated that it held no information in respect of question 5. It would neither confirm nor deny ("NCND") whether it held the remaining information, citing the NCND exemption at section 31(3) (law enforcement) of the FOIA, with the public interest favouring maintaining that exemption.

11. On 11 April 2018, the complainant asked Bedfordshire Police to conduct an internal review of its decision to issue a NCND response under section 31(3). Bedfordshire Police responded on 12 April 2018, declining to conduct an internal review on the grounds that too long a time had passed since the refusal notice had been issued.

Scope of the case

12. The complainant initially contacted the Commissioner on 31 January 2018, explaining that she had submitted the above request to every UK police force. Her complaint to the Commissioner was slightly delayed beyond the usual three month time limit for bringing such complaints, as she had waited to receive the bulk of the responses prior to submitting the complaint to the ICO.

13. At the time of making the complaint, the complainant had not asked Bedfordshire Police to conduct an internal review of its response, and so the Commissioner asked her to do so. As noted above, Bedfordshire Police declined to conduct an internal review. The complainant wrote

again to the Commissioner on 16 April 2018, to complain about the response.

14. In a detailed submission in support of her complaint, the complainant commented as follows:

> "*It is clear that the police have capabilities to extract data even in low level crimes. That they are willing to answer questions about this for computers, laptops and phones but not for connected devices such as those in the home or our vehicles is confusing and inconsistent.*
>
> *We are concerned that without transparency, there cannot be accountability. Just as DNA may have previously appeared to be the silver bullet to solving crime, the difficulties associated with this as a reliable form of evidence are well known. We fear that unless there is transparency around the extraction of data from connected devices, this will undermine access to justice and there is a real possibility of miscarriages of justice…*We *recognise the need not to undermine investigations however, we do not seek detailed information about what the police can and cannot do. These high-level questions and responding to them would provide no real benefit to criminals*".

15. The analysis below considers Bedfordshire Police's application of section 31(3) of the FOIA to NCND whether it holds the information specified in questions 1-4 and 6 of the request. The complainant did not contest Bedfordshire Police's response in respect of question 5, and so it is not considered in this decision notice.

Reasons for decision

Section 31 – law enforcement

16. When a request for information is made under the FOIA, the first duty of a public authority, under section 1(1)(a) of the FOIA, is to inform the requester whether it holds information of the description specified in the request. This is known as the duty to confirm or deny.

17. However, the duty does not always apply and a public authority may refuse to confirm or deny whether it holds information through reliance on certain exemptions under the FOIA.

18. Section 31(3) of the FOIA excludes a public authority from complying with the duty to confirm or deny in relation to information if to do so would, or would be likely to, prejudice any of the functions in sections 31(1); Bedfordshire Police has relied on sections 31(1)(a) (the prevention or detection of crime) and 31(1)(b) (the apprehension or

prosecution of offenders) to NCND whether it holds the information requested in questions 1-4 and 6.

19. When considering a prejudice based exemption such as section 31, the Commissioner will:

    • identify the applicable interests within the relevant exemption;

    • examine the nature of the prejudice, the likelihood of it occurring and that the prejudice claimed is real, actual and of substance; and

    • examine whether there is a causal link between confirming/denying and any prejudice claimed.

20. Addressing the request as a whole, Bedfordshire Police said that by confirming or denying whether it holds the requested information, it would disclose information regarding specific capabilities which the police service may or may not utilise as part of its response to investigating and combatting crime. The Commissioner accepts that this relates to the prevention or detection of crime and to the apprehension or prosecution of offenders, and that it is therefore an applicable interest.

21. The Commissioner then considered the extent to which confirming or denying would result in a real and significant likelihood of prejudice to the prevention or detection of crime, and to the apprehension or prosecution of offenders. In doing so, she has taken account of Bedfordshire Police's assessment that the lower likelihood of prejudice threshold applies (ie that confirmation or denial "*would be likely*" to prejudice the prevention or detection of crime and the apprehension or prosecution of offenders).

22. Bedfordshire Police explained that criminals would be able to gauge its IoT investigative capabilities by it confirming or denying whether it holds the requested information. It said that confirming that it holds the information described in the request would reveal its capabilities with regard to carrying out this type of investigation, whereas to deny that information was held would reveal that the force was unable to conduct this type of investigation. It said that confirming or denying would be likely to *"threaten"* the force's ability to prevent and detect crime and would be likely to reduce the effectiveness of any technological advances in IoT investigative techniques.

23. Bedfordshire Police said it was important that it was able to apply a NCND response to these types of requests in a consistent fashion:

    "If Bedfordshire Police … provided confirmation or denial of each emerging investigation tactic it would limit our operational capabilities. Those intent on committing crime and performing acts of

terrorism could gain a greater understanding of the methods and techniques used by the police, enabling them to take steps to counter them."

24. Furthermore, Bedfordshire Police said that as the request had been submitted to every police force in the UK, it could enable those with criminal intent to build up a nationwide picture of where IoT investigative capabilities appeared to be stronger or weaker, and to target those areas of the UK where they believed they were less likely to be apprehended. It said this would be detrimental to the operation of an efficient policing service and to its duty of care to members of the public.

25. Bedfordshire Police referred the Commissioner to the approach taken in the decision notice issued under FS50459944, in April 2013, which considered information about 'silent' SMS technology. In that case, the Commissioner upheld the application of a NCND response in respect of the protection of national security. Bedfordshire Police believed that the arguments which were accepted in that case were applicable to police forces protecting their law enforcement tactics.

26. Bedfordshire Police's arguments in support of section 31(3) rest on something more being revealed by confirming/denying than whether or not it holds the information described in the request. When determining whether section 31(3) is engaged in this case, it is therefore necessary to consider what would be learned from Bedfordshire Police confirming or denying that the requested information is held, and the extent to which it would be prejudicial to the prevention or detection of crime and to the apprehension or prosecution of offenders.

27. Confirming that the requested information is held would disclose to the public that Bedfordshire Police holds information about its digital investigation and intelligence capabilities. It could be inferred from this that the force has an active interest in the IoT. However, for the reasons set out below, the Commissioner considers that, in the particular circumstances of the case, confirmation (if held) would not reveal something that is not already likely to be obvious to the public. This is significant because the Commissioner's guidance on the duty to confirm or deny[8] states, "*In some cases it may be already known or obvious that information must be held, and in those circumstances confirming that information is held may not cause any harm*...".

[8] https://ico.org.uk/media/for-organisations/documents/1166/when_to_refuse_to_confirm_or_deny_section_1_foia.pdf

28. As noted in paragraph 7, *Policing and the Internet of Things* examines how IoT technology should be exploited for law enforcement purposes. The report comments that in the coming years, the distinction between "cyber-crime" and other crime will deteriorate and that most crimes will involve some use of the internet, or create some form of digital footprint. It observes that the police will need to be equipped with the right skills and tools to respond to the challenges and opportunities this brings[9]. The report also lists, broadly, the types of preparations underway across various national law enforcement-related bodies with regard to the IoT.

29. *Policing and the Internet of Things* contains a foreword by Assistant Chief Constable Richard Berry, Chief Officer Lead, Digital Investigations and Intelligence Programme of the National Police Chiefs' Council ("the NPCC"), encouraging police forces to embrace the potential uses of IoT for law enforcement purposes, and observing that "*Police forces across the country have already adapted locally and there are many pockets of good practice*".

30. Thus, public comments from the NPCC (which itself has a lead officer for Digital Investigations and Intelligence) indicate that this is a strategic area that the police service is actively engaging with.

31. Furthermore, in its submissions to the Commissioner, Bedfordshire Police itself commented that "*It is well established that police forces use covert tactics and surveillance to gain intelligence in order to counteract criminal behaviour*." This lends further credence to the Commissioner's view that the public's expectation is that the police service will be actively addressing the challenges and opportunities presented by the IoT.

32. The Commissioner also notes that by confirming that it holds information about its digital investigatory capabilities, Bedfordshire Police would not be disclosing information about the extent of those capabilities. Such information as it may hold might, in fact, be concerned with identifying relative deficiencies in that area, and the need for them to be addressed. The Commissioner is not satisfied that confirming that information is held necessarily equates with revealing that the force currently has the capability to carry out investigations of IoT devices. She also does not consider that Bedfordshire Police has shown how confirmation would give criminals any meaningful insight into its crime fighting methods and techniques in this area, or how it would undermine the effectiveness of any such techniques. Individual

[9] *Policing and the Internet of Things*, page 17

police forces' capabilities in respect of the IoT may range from the commonplace (obtaining location data generated by mobile phones) to advanced forensic and mapping technology. Confirming that information is held would not reveal which end of the spectrum a force's IoT capabilities lie at.

33. Turning to what denying that information is held would reveal, the Commissioner notes that Bedfordshire Police's concern here is that it would suggest a vulnerability in the area of digital investigatory intelligence, which criminals could seek to exploit. However, as above, the Commissioner does not accept that it can necessarily be inferred from a police force's denial that it holds information about its IoT capabilities, that it has no capabilities in that area.

34. The Commissioner is aware that a number of police forces work together in strategic partnerships, where one force takes responsibility for leading on certain issues in respect of the other forces in the partnership. In light of the existence of these agreements, and particularly where smaller police forces are concerned, a denial that information is held may simply be indicative that a partner force is leading on the development of capabilities or that it utilises the expertise and resources of a partner force, for investigations which touch on this area.

35. The IoT is a fast moving area, and, as *Policing and the Internet of Things* indicates, one which the police service is actively focussed on. The Commissioner notes that when the request in this case was put to the Home Office, it responded that although it did not currently have the capabilities described in the request, it planned to develop them. This suggests that the Home Office, the ministerial department with responsibility for the police service, sees IoT as an important strategic area in which work is being be done. *Policing and the Internet of Things* states that the Home Office's Police Information and Digitisation Unit has been leading the drive in forensics, biometrics and digital transformation with the aim of supporting the police in the challenges and opportunities of digitisation[10]. Any attempt to map the capabilities of individual police forces so as to identify "unprepared" forces would be hampered by the limited lifespan of any information which might be inferred from a denial, which would be likely to be out of date very quickly.

36. The Commissioner notes that Bedfordshire Police did not provide examples of precisely how (an assumed) knowledge of a police force's IoT investigative capabilities would be likely to prejudice its law

[10] *Policing and the Internet of Things*, page 16

enforcement functions, other than to say it would be likely to lead to criminals targeting areas perceived as not having IoT capabilities. It provided no information as to how criminals might take steps to counter a force's perceived law enforcement capabilities and why these might be successful.

37. Rather, although it applied a NCND response, Bedfordshire Police's arguments appear to concentrate on the consequences of disclosing the requested information itself (if held). It referred to the "*greater understanding of the methods and techniques used by the police*" that would result, and implied that knowledge of how the police combat crime would be imparted.

38. The Commissioner does not agree that confirming or denying would be likely to result in the prejudice envisaged. She considers instead that the prejudice envisaged might be likely to occur if the requested information (if held) was to be disclosed. The decision to neither confirm nor deny is separate from a decision not to disclose information and needs to be taken entirely on its own merits. It is only the consequences of confirming or denying whether information is held that may be taken into account when considering whether section 31(3) applies. The Commissioner finds Bedfordshire Police's arguments deficient in that regard.

39. Regarding Bedfordshire Police's citing of the approach taken in the decision notice on 'silent' SMS technology (in which a NCND approach was upheld) the exemptions cited in that case were section 23 (information supplied by or relating to, bodies dealing with security matters) and section 24 (national security). Section 23 is a class-based exemption, meaning that if the information requested is of the type described in the exemption, then it is covered by that exemption. Information will be exempt under section 24 where this is reasonably required for the purpose of safeguarding national security. These exemptions operate differently from the exemption cited in this case, which is a prejudice-based exemption. For section 31(3) to be engaged in this case, it is necessary to establish that prejudice to the prevention or detection of crime and the apprehension or prosecution of offenders would be likely to occur as a result of confirming or denying that the requested information is held. If no such prejudice can be demonstrated, the exemption will not be engaged.

40. The Commissioner also notes that in the decision notice cited by Bedfordshire Police, the request specifically asked to know the number of times the technology referred to had been used. The Commissioner's guidance on confirming or denying whether information is held states that a NCND response is more likely to be needed for very specific requests than for more general or wide ranging requests. The request under consideration here contains no equivalent request to know how

many times any IoT technological capabilities have been deployed. The Commissioner considers the request here to be fairly broad and lacking the level of granularity of the request in the decision notice cited by Bedfordshire Police. The Commissioner therefore does not agree with Bedfordshire Police that the two cases are comparable.

41. For the reasons set out above, the Commissioner is not persuaded that Bedfordshire Police has demonstrated that confirming or denying whether it holds the information described in the request would be likely to prejudice the law enforcement functions at sections 31(1)(a) and 31(1)(b). She disagrees with the inferences which Bedfordshire Police says could be made from confirmation or denial and consequently she is not satisfied that it has shown that the prejudice it envisages would be likely to occur. It is her decision that sections 31(1)(a) and 31(1)(b) of the FOIA were not engaged and therefore that Bedfordshire Police was not entitled to rely on section 31(3) to issue an NCND response.

42. Since her finding is that the exemption was not engaged, it has not been necessary to go on to consider the balance of the public interest.

Right of appeal

43. 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: 0300 1234504
    Fax: 0870 739 5836
    Email: GRC@hmcts.gsi.gov.uk
    Website: www.justice.gov.uk/tribunals/general-regulatory-chamber

44. 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.

45. 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 .....

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