Freedom of Information Act 2000 (FOIA)

Decision notice

Date: **20 September 2018**

Public Authority: **Chief Constable of Staffordshire Police**
Address: **Police Headquarters**
PO Box 3167
Stafford
ST16 9JZ

Decision (including any steps ordered)

1. The complainant has requested information about Staffordshire Police's capabilities with regard to utilising the "Internet of Things" for law enforcement purposes. Staffordshire 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 Staffordshire Police was not entitled to rely on section 31(3) to neither confirm nor deny whether it holds the information.

3. The Commissioner requires Staffordshire 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. Staffordshire 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 seven police forces handled the request, and is issuing decision notices in respect of those cases, with the lead case being reference FS50739828[1]. The other cases will be dealt with separately.

The Internet of Things

6. 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]

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

---

[1] The other six cases are dealt with under the following references: FS50739828, FS50739852, FS50741045, FS50748303, FS50744518 and FS50751700

[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

8. Prior to the request under consideration here, on 10 August 2017, the complainant submitted a request for information to every UK police force, and to the Home Office, asking about their capabilities with regard to utilising the IoT for law enforcement purposes. While the Home Office largely answered the questions contained in the request, the police forces would neither confirm nor deny holding the requested information, citing various exemptions[7].

9. Dissatisfied by this response, on 6 October 2017 the complainant then made the following request for information to every UK police force:

> "*I write further to my previous request. I note your response*. *In light of the attached response from the Home Office please can you provide information / documentation / policies/ guidance / meeting notes in relation to whether:*
> *1. Your force is or anticipates they will be involved in the development of capabilities, skills and capabilities to exploit the internet of things as part of criminal investigations.*

[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] The Commissioner has considered this response in decision notice FS50739797

2. Your force is or anticipates they will receive training in relation to extracting / obtaining / retrieving data from or generated by connected devices.
3. Documentation in relation to communications to / from / with the Home Office in relation to exploiting the internet of things / connected devices in criminal / civil / immigration or other investigations.

10. Staffordshire Police responded on 26 October 2017. It would neither confirm nor deny ("NCND") whether it held the information, citing the NCND exemption at section 31(3) (law enforcement), with the public interest favouring maintaining that exemption.

11. On 11 April 2018, the complainant asked Staffordshire Police to conduct an internal review of its decision to issue a NCND response under section 31(3). Staffordshire 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 Staffordshire Police to conduct an internal review of its response, and so the Commissioner asked her to do so. As noted above, Staffordshire Police declined to conduct an internal review. The complainant wrote again to the Commissioner on 20 April 2018, to complain about the response.

14. In 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 Commissioner has considered Staffordshire Police's application of section 31(3) of the FOIA to NCND whether it holds the information specified in the request.

Reasons for decision

16. The request in this case is identical to a request for information which the Commissioner has considered alongside this case, under reference FS50739828. The decision notice in that case is also being issued at the same time as this case.

17. Having considered all the factors applicable to this case, the Commissioner is satisfied that the similarity between the arguments submitted in this case and the request in case reference FS50739828 is such that she is able to reach the same decision about the citing of section 31(3).

18. For brevity, the Commissioner will not reproduce the content of that decision notice here but she has adopted the same analysis and concluded that Staffordshire Police was not entitled to rely on section 31(3) to issue a NCND response.

Right of appeal

19. 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

20. 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.

21. 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