Freedom of Information Act 2000 (FOIA)

Decision notice

Date: 20 September 2018

Public Authority: Chief Constable of British Transport Police
Address: Force Headquarters
25 Camden Road
London
NW1 9LN

Decision (including any steps ordered)

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

3. The Commissioner requires British Transport 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. British Transport 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 the lead case being FS50739797[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: FS50739797, FS50739835, FS50739875, FS50741036 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 British Transport 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. British Transport Police responded on 1 September 2017. In respect of question 5, it said that there is no single Digital Media Investigator, and that a number of staff members fulfil that role. It would neither confirm nor deny ("NCND") whether it held the remaining information, citing the NCND exemptions at section 30(3) (investigations and proceedings) and section 31(3) (law enforcement) of the FOIA, with the public interest favouring maintaining the exemptions.

11. On 11 April 2018, the complainant asked British Transport Police to conduct an internal review of its decision to issue a NCND response. British Transport Police responded on 10 May 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 British Transport Police to conduct an internal review of its response,

and so the Commissioner asked her to do so. As noted above, British Transport Police declined to conduct an internal review. The complainant wrote again to the Commissioner on 10 May 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. During the course of the investigation, British Transport Police withdrew its reliance on section 30(3) of the FOIA. The Commissioner has therefore considered British Transport 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 British Transport Police's response in respect of question 5, and so it is not considered in this decision notice.

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 FS50739797. 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 FS50739797 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 British Transport Police was not entitled to rely on section 31(3) of the FOIA 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