Freedom of Information Act 2000 (Section 50)

Decision Notice

Date: 6 September 2011

Public Authority: **The Chief Constable**
Address: **Kent Police Headquarters**
Sutton Road
Maidstone
Kent
ME15 9BZ

Summary

The complainant asked Kent Police (the "public authority") to provide information relating to whether its ANPR equipment had checked either of two vehicles between specific dates. The public authority initially neither confirmed nor denied holding information using the exemption at section 31(3) of the Freedom of Information Act (the "Act"), but later substituted the section 12 costs exclusion instead. The Commissioner has concluded that, under section 40(5)(b)(i), the public authority should in fact have neither confirmed nor denied having information.

The public authority is not required to take any steps.

The Commissioner's role

1. The Commissioner's duty is to decide whether a request for information made to a public authority has been dealt with in accordance with the requirements of Part 1 of the Freedom of Information Act 2000 (the "Act"). This Notice sets out his decision.

Background

2. The request refers to ANPR, i.e. automatic number plate recognition. Further information about ANPR can be found in the following online publication:

http://www.acpo.police.uk/documents/crime/2009/200907CRIANP01.pdf

The following extracts may be useful:

"ANPR is a technology that automatically reads vehicle registration marks (VRMs), allowing these details to be compared against database records. ANPR systems are used by the police, government agencies, eg, the Highways Agency, and commercial companies including garages, shopping centres and car parks."

"ANPR data comprises 'read' data and 'hit' data. A read is the capture of the VRM and image of a vehicle as it passes through the camera; read data is the term used to describe all the data collected as vehicles pass through the ANPR reader. A hit is a match to a VRM held within the database being searched."

"In addition to the VRM, ANPR data includes:

- *A digitalised picture of the VRM (or patch plate image);*
- *The time the data was captured;*
- *The date the data was captured;*
- *The location (and GPS coordinate) of the camera;*
- *The force identification;*
- *The camera name (such as description of where it is and the exact location)."*

"Each force has a centralised computer database for storing and analysing ANPR data, commonly known as the Back Office Facility (BOF). Stored data may be accessed for analysis. The BOF can be searched on a case-by-case basis in support of an investigation for matches in both read and hit data. Any searches must be authorised in accordance with the National ACPO ANPR Standards 2008 (NAAS)."

"An ANPR database is a list of vehicles of interest to a particular force or specialist area against which ANPR data is checked. These are sometimes referred to as 'hot lists'. There are a number of databases loaded onto the ANPR system".

"An ANPR hit will only identify a vehicle of interest which, when matched to relevant databases, will identify the registered keeper and, if the image shows the occupants of the vehicle, may assist with enquiries to identify them."

"Personal data gathered (by the police) using ANPR technology should only be obtained for a specified purpose which has been registered and it shall not be used for any other purpose".

The request

3. On 11 April 2011 the complainant made the following information request:

> *"I wish to know if the following vehicles have been checked on the Kent police ANPR system since 8th Dec, 2010, the purpose of the check and by whom.*
> *Ssangyong Musso – [VRM removed]*
> *Vauxhall Astra – [VRM removed]".*

4. On 15 April 2011 the public authority responded. It refused to confirm or deny holding information by virtue of section 31(1) (law enforcement). It stated:

> *"… confirmation or denial of whether information is held would be likely to lead to the identification of the location of ANPR cameras based on knowledge of where the vehicles had travelled. This information is not released to the public since it would result in the cameras being targeted by terrorists or criminals to the detriment of law enforcement generally and of the prevention and detection of crime specifically"*.

5. On 16 April 2011 the complainant sought an internal review. She stated:

> *"I am a current employee of the organisation and have been for over 30 years. I have access to the ANPR system so am well aware of where the cameras are located".*

6. On 25 May 2011 the public authority provided its internal review. It changed its position stating:

> *"… you pointed out that you are employed by Kent Police, have access to the ANPR system and have knowledge of where the cameras are located.*
>
> *…Your knowledge of the camera locations is not relevant to our response [because] all FOIA responses are deemed to enter the public domain. Any information released is deemed to be disclosed to the wider world. In exercising your rights to information as a private citizen, no consideration can be given to your specific access to information by virtue of your employment".*

7. In went on to change its previous position saying:

> *"Transactions on the ANPR system for audit purposes can only be checked against users. There is no way of easily ascertaining whether specific vehicle registration marks have been checked. This has been confirmed with the auditors and ANPR support team at Kent Police. Therefore, in order to confirm or deny whether your vehicles have been checked on the system, a manual review of all ANPR users' searches for the period specified would be required. This would involve an expenditure of resources that would exceed the amount that a public authority is required to invest in responding to a request, i.e. the cost of locating and retrieving the information exceeds the 'appropriate level' (currently 18 hours) as stated in the Freedom of Information and Data Protection (Appropriate Limit and fees) Regulations 2004".*

The investigation

Scope of the case

8. On 13 June 2011 the complainant contacted the Commissioner. She asked him to consider whether compliance would exceed the appropriate limit.

Chronology

9. On 26 July 2011 the Commissioner commenced his investigation. He wrote to the public authority and raised some initial queries.

10. On the same day the public authority provided a response.

11. On 27 July 2011 the Commissioner advised the complainant that he was considering her case.

Analysis

Exemption

12. The Commissioner will not proactively seek to consider exemptions in all cases before him, but in cases where personal data is involved the Commissioner believes he has a duty to consider the rights of data subjects. These rights, set out in the Data Protection Act (the "DPA"),

are closely linked to article 8 of the Human Rights Act and the Commissioner would be in breach of his obligations under the Human Rights Act if he ordered disclosure of information or confirmation/denial without having considered these rights, even where the exemption has not been cited.

Section 40 – personal information

13. The full text of the relevant provisions of the Act referred to in this section is contained within the Legal Annex.

14. Section 40(5)(b)(i) provides that a public authority is not obliged to confirm or deny whether requested information is held if to do so would:

- constitute a disclosure of personal data, and
- this disclosure would breach any of the data protection principles or section 10 of the Data Protection Act (DPA).

15. The Commissioner's analysis of whether the above criteria would be satisfied follows.

Would confirming or denying that the requested information is held constitute a disclosure of personal data?

16. The DPA defines personal information as:

> *"…data which relate to a living individual who can be identified*
> *(a) from those data, or*
> *(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the data controller or any person in respect of the individual."*

17. In his guidance on the section 40 exemption[1], the Commissioner expanded on what constituted personal data:

> *"The two main elements of personal data are that information must 'relate to' a living person, and that person must be identifiable. Information will 'relate to' a person if it is about them, linked to them, has some biographical significance for them, is used to inform decisions affecting them, has them as its main focus or impacts on them in any way."*

[1]http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/personal_information.pdf

18. The Commissioner considers that the way in which the request is worded clearly indicates that the complainant is seeking information which can be linked with named individuals, i.e. the driver/s and or owner/s or the two identified vehicles. He considers that to comply with section 1(1)(a) of the Act (i.e. to either confirm or deny holding the information) would inevitably put into the public domain information about whether either vehicles has been captured by ANPR equipment. This would constitute the disclosure of information that would relate to the owners / drivers of those two vehicles, be it either a 'read' or a 'hit' event (see *Background* section above).

19. Therefore, the Commissioner considers that to confirm or deny whether the requested information is held would in itself constitute a disclosure of personal data.

Would disclosure of this personal data breach a data protection principle?

20. The first data protection principle requires that personal data is processed fairly and lawfully and that:

> *"at least one of the conditions in Schedule 2 is met, and in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met".*

21. The Commissioner's considerations here focus on the general issue of whether disclosure would be fair to the relevant individuals.

Fairness

22. In establishing whether disclosure is fair, the Commissioner will look to balance the consequences of any release of personal data and the reasonable expectation of the data subjects, with general principles of accountability and transparency.

23. The personal data that would potentially be disclosed here would relate to the individuals in a private capacity. This is significant in that previous decisions issued by the Commissioner have been guided by the principle that information about an individual's private life will deserve more protection than information about someone acting in an official or work capacity.

24. The Commissioner would therefore consider that in the circumstances of this case, the individuals would have a legitimate expectation that information would not be disclosed which may or may not confirm whether they had been caught on any ANPR camera (either by virtue of

passing one or by virtue of being a targeted vehicle). To disclose this information would be an unwarranted intrusion into the rights and freedoms of the data subjects, given the distress that the release of the information could potentially cause.

25. In considering whether the exemption contained within section 40(5)(b)(i) should have been applied to the request the Commissioner has taken into account that the Act is designed to be applicant blind and that disclosure should be considered in its widest sense – which is to the public at large. If information were to be disclosed it would, in principle, be available to any member of the public. A confirmation or denial in the circumstances of this case could reveal to the public information which is not already in the public domain and is not reasonably accessible to the general public, about the whereabouts of those parties and the possibility that they have been under some level of police surveillance.

Conclusion

26. Leading on from these considerations, the Commissioner has determined that to confirm or deny whether the requested information is held would be unfair to the data subjects. As disclosure would therefore breach the first data protection principle, section 40(5)(b)(i) is engaged and the correct approach would have been for the public authority to have neither confirmed nor denied holding the requested information.

The decision

27. The Commissioner's decision is that the public authority did not have a duty to comply with section 1(1)(a) of the Act on the basis of the exemption contained within section 40(5)(b)(i).

Steps required

28. The Commissioner requires no steps to be taken.

Other matters

---

29. Although they do not form part of this Decision Notice the Commissioner wishes to highlight the following matters of concern.

Internal review

30. Part VI of the section 45 Code of Practice makes it desirable practice that a public authority should have a procedure in place for dealing with complaints about its handling of requests for information, and that the procedure should encourage a prompt determination of the complaint. As he has made clear in his *'Good Practice Guidance No 5'*, the Commissioner considers that these internal reviews should be completed as promptly as possible. While no explicit timescale is laid down by the Act, the Commissioner has decided that a reasonable time for completing an internal review is 20 working days from the date of the request for review. In exceptional circumstances it may be reasonable to take longer but in no case should the time taken exceed 40 working days.

31. The Commissioner does not consider this case to be 'exceptional', so is concerned that it took over 20 working days for an internal review to be completed.

Subject access

32. The Commissioner notes that, in her letter of complaint, the complainant refers to '*my vehicles*'. As such any data, if held, may be her 'personal data'. He would therefore like to suggest that it may be appropriate for her to make a request to the public authority under the 'subject access provisions' of the DPA.

Right of appeal

33. 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,
Arnhem House,
31, Waterloo Way,
LEICESTER,
LE1 8DJ

Tel: 0300 1234504
Fax: 0116 249 4253
Email: informationtribunal@tribunals.gsi.gov.uk.
Website: www.informationtribunal.gov.uk

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.

Any Notice of Appeal should be served on the Tribunal within 28 calendar days of the date on which this Decision Notice is sent.

Dated the 6th day of September 2011

Signed ……

Jon Manners
Group Manager

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF