IN THE FIRST-TIER TRIBUNAL **Appeal No: EA/2010/0174**
GENERAL REGULATORY CHAMBER
(INFORMATION RIGHTS)

ON APPEAL FROM:

The Information Commissioner's Decision Notice No: FS50270424
Dated: 23 December 2010

Appellant:	**Steven Mathieson**
Respondent:	**The Information Commissioner**
2nd Respondent:	**Chief Constable of Devon and Cornwall**
Heard at:	**Competition Tribunal**
Date of Hearing:	**7 June 2012**

Before

HH Judge Shanks

Judge

and

Henry Fitzhugh and **Pieter de Waal**

Tribunal Members

Date of Decision: **18 June 2012**

Attendances:

For the Appellant: Guy Vassall-Adams

For the Respondent: Anya Proops

For the 2nd Respondent: Jeremy Johnson QC

Subject matter:

Freedom of Information Act 2000

s.24 National security

s.31 Qualified exemption: Law enforcement

DECISION OF THE FIRST-TIER TRIBUNAL

For the reasons set out below the Tribunal dismisses the appeal.

REASONS FOR DECISION

Introduction

1. On 20 July 2009 Mr Mathieson, a journalist with Guardian News & Media who has a close interest in the public sector use of information technology, requested the following information from the Devon and Cornwall Police:

    - **the locations of fixed, operating automatic numberplate recognition (ANPR) cameras operated by Devon and Cornwall Police and its agencies**
    - **the locations of CCTV cameras with ANPR functionality used by Devon and Cornwall Police.**

    On 21 September 2009, following a review, the Devon and Cornwall Police (who we will refer to as the Respondent) refused to supply the requested information, relying on a number of exemptions in the Freedom of Information Act 2000, namely sections 31(1)(a)

(prejudice to the prevention and detection of crime), 31(1)(b) (prejudice to the apprehension and prosecution of offenders) and 31(1)(c) (prejudice to the administration of justice) and section 24(1) (national security).

2. Mr Mathieson complained to the Information Commissioner, who upheld the Respondent's position in a decision notice dated 23 September 2010. He appealed against the decision notice to the First-tier Tribunal. On 11 April 2011 the Tribunal allowed his appeal and ordered the Respondent to disclose the requested information. The Respondent appealed successfully against that decision to the Upper Tribunal which on 1 February 2012 set aside the decision and remitted the appeal for rehearing to this differently constituted First-tier Tribunal.

3. The issue we have to resolve is whether in September 2009 the Respondent was indeed entitled to withhold the information requested by Mr Mathieson on the basis of sections 24 and/or 31 of the 2000 Act. Section 24(1) provides:

> **… information … is exempt … if exemption … is required for the purpose of safeguarding national security.**

Section 31(1) provides:

> **Information … is exempt … if its disclosure under this Act would, or would be likely to, prejudice-**
>
> **(a) the prevention or detection of crime,**
>
> **(b) the apprehension and prosecution of offenders, [or]**
>
> **(c) the administration of justice …**

If either or both these exemptions was established, the Respondent was entitled to withhold the information if, in all the circumstances, the public interest in maintaining the relevant exemption or exemptions outweighed that in disclosing the information.

The evidence and hearing

4. We have received a mass of written evidence, most of it not put before the Commissioner or the earlier constitution of the First-tier Tribunal. In particular, we have been provided with statements exhibiting numerous relevant documents from the following witnesses:

   - Louise Fenwick, Freedom of Information Officer with the Respondent;
   - Russell Middleton, Respondent's Assistant Chief Constable;
   - Mark Hannaford, police sergeant with the Respondent;
   - Neil Winterbourne, detective superintendant who runs the ANPR unit Counter Terrorism Command for the Metropolitan Police;
   - Jeremy Harris, assistant Chief Constable in the Police Service of Northern Ireland;
   - Michael Shaw, a barrister who prosecuted an armed robbery called R v Speed;
   - John Charles Dean, ANPR co-ordinator for the Association of Chief Police Officers;
   - Mr Mathieson himself.

   The statements of Mr Hannaford, Mr Winterbourne and Mr Harris were served on Mr Mathieson in redacted form but, following the intervention of the Tribunal, many of the redactions were removed from the statements of Mr Hannaford and Mr Winterbourne and their statements were re-served. It was agreed at the outset of the hearing that the appeal would be decided on the basis of the material as served on Mr Mathieson and that the Tribunal would take no account of the content of any redactions which remained in place. There was therefore no need for a closed session.

5. At the hearing we also received oral evidence from Mr Middleton and oral submissions from all parties supplementing the detailed and helpful skeleton arguments that had already been lodged.

Findings on applicability of sections 24 and 31

6. On the basis of all the evidence, we are satisfied of the following:

(1) ANPR cameras are able to scan the vehicle registration numbers (VRNs) of vehicles passing them and the VRN can then automatically be checked against information stored in other electronic databases, in particular the police national computer: thus they enable the police to be notified immediately if a vehicle they are interested in (because it is stolen or uninsured or is being tracked, for example) passes a ANPR camera; these are known as "hits". Furthermore, all the data captured by an ANPR camera (ie the VRN of every vehicle passing an APNR camera and the date and time it passes, known as "reads") are also stored for two years and can be used subsequently, by means of a simple electronic search, to help to establish the movements of a particular vehicle or to establish which vehicles passed a particular ANPR camera at a particular time.

(2) The Respondent had about 45 fixed and 25 mobile ANPR cameras; there were also an unknown number of ANPR cameras owned by others (some attached to local authority CCTV cameras) but the Respondent did not have direct access to data obtained by those cameras; the Respondent's own ANPR cameras were a small part of a national network of about 5,000 such cameras used by the police throughout the UK which captured around 16 million "reads" per day.

(3) The ANPR network of cameras is, as Mr Middleton puts it in his statement and as Mr Vassall-Adams in effect accepted, a "highly effective crime fighting tool": clearly, it has the potential to help the police to prevent, to investigate and to prosecute crime, including (significantly for this case) serious organised crime and terrorism, and it has indeed done so on a number of occasions referred to in the evidence.

(4) If the location of a fixed ANPR camera site is known detection by the camera can be avoided by the simple expedient of taking a route which goes round it or by "adopting counter-detection driving techniques" (as Mr Winterbourne

put it)[1] or by damaging the camera. These are all steps that those involved in serious organised crime or terrorism might well take if they thought it would help them not to be detected in carrying out their plans.

(5) Although the location of individual fixed ANPR cameras is not hidden and a well informed member of the public would be able to identify one, if the locations of all the fixed ANPR cameras in the Respondent's area (or in any other police area) were disclosed publicly it would be very likely that they would be mapped and it would be easier for terrorists and those involved in serious organised crime to take the steps identified above to avoid detection by them.

(6) Disclosure of the requested information would thus be likely to undermine the effectiveness of a tool which helps the police to prevent, to investigate and/or to prosecute terrorist incidents or serious crimes.

7. It is therefore clear in our view that exemption of the requested information from disclosure is required for the purpose of safeguarding national security (ie to assist in combatting terrorism) and that its disclosure would involve a real and significant risk of harming the interests set out in sections 31(1)(a), (b) and (c) of the 2000 Act. It follows (and Mr Vassall-Adams in the end accepted) that both sections 24 and 31 of the Act are engaged in this case. The real issue is therefore whether the public interest in maintaining those two exemptions outweighed that in disclosure. We therefore turn to consider the weight of the respective public interests.

Public interest in maintaining the exemptions

8. Clearly there is always likely to be a substantial public interest in maintaining the exemptions we are concerned with, in particular that provided by section 24 which relates to national security.

[1] The Tribunal asked for further details of these techniques but the Respondent did not wish to reveal them for obvious reasons and no objection was taken to this.

9. However, Mr Vassall-Adams made a number of points in support of the proposition that the negative impact of disclosure of the requested information had been greatly overstated. He pointed out that most criminals were unlikely to take the avoidance steps that terrorists and serious organised criminals would and that, to that extent, disclosure would not undermine the utility of the ANPR system. He reminded us that the location of current APNR cameras can be discovered "on the ground" (though we also remind ourselves that there are thousands of such cameras around the country and to identify the position of all of them or even those within the Respondent's area would be a very substantial undertaking). He pointed out that there are other forms of surveillance which would remain as effective as before (eg mobile ANPR cameras, those owned by local authorities or other bodies, CCTV) and that terrorists and serious organised criminals have other means of trying to undermine the effectiveness of APNR surveillance, in particular by manipulating VRNs in various ways.

10. All these points have some validity and we accept that disclosure of the requested information may only have tipped the scales in favour of terrorists and serious organised criminals slightly. But we are bound also to take account of the fact that, although the risk may have been small, if disclosure of the information requested meant, for example, that a terrorist incident took place which might otherwise have been avoided, the results could be catastrophic. We have considerable sympathy with Mr Middleton's plea that the police "…need to stay one step ahead" and with his rhetorical question: "Why would we want to give one of our tools back to the criminals?"

Public interest in disclosure

11. There was an issue about the applicability of the Data Protection Act 1998 and Art 8 of ECHR to the operation of the APNR system. Mr Vassall-Adams and Ms Proops maintained that "read" data was always the personal data of the owner (or keeper) of the relevant vehicle and that Art 8 was inevitably engaged. Mr Johnson accepted that the Data Protection Act and Art 8 may be relevant in particular cases depending on the circumstances but he did not accept that they inevitably applied. We do not think it is necessary or appropriate to resolve this issue in the context of this case and are content

simply to note that it is an arguable issue and that, as we say, Mr Johnson accepted that in particular cases "read" data may contain personal data and Art 8 may apply.

12. It was common ground among all parties, however, that there were (and are) issues of enormous and legitimate public interest arising out of the ANPR system which were (and have remained) highly topical. The use of ANPR by the police has grown massively since 2002 but at the time of Mr Mathieson's request there was no statutory framework in place governing its operation.[2] The system enables the police easily to discover the movements of millions of ordinary drivers going about their daily business, keeping details of the time, date and location of something like 16 million vehicles per day, which obviously has very serious implications in relation to the power of the state over the citizen and his privacy rights. There is also a clear public interest in citizens being able to judge whether the police are using this technology in the most effective way. Thus, there were (and are) legitimate and important issues for public debate (a) as to whether the APNR system should be used at all; (b) if so, as to where cameras should be located and whether (in general) their location should be public knowledge or not; and (c) as to whether "read" data should be retained at all or, if so, for as long as two years and as to what use should be made of them.

13. The main point made by Mr Vassall-Adams (supported to a great extent in this respect by Ms Proops) was that a proper public debate on these issues required the disclosure of the requested information. We accept that if the public were made aware of the location of ANPR cameras the debate would in a sense be more "meaningful" because the public would be able to see and comment on the actual use being made by the police of ANPR (eg whether they were focussing on particular crime "hot spots" or whether they were wrongly focussing on a particular community) and that it would be more "engaging" because it is human nature to take more interest in something which people know has a direct effect on them. But we do not think the lack of the requested information in any way prevents the debate taking place or prevents those who, like Mr Mathieson, have strong views on the issues from making their arguments, as shown by experience since

[2] Section 29 of the Protection of Freedoms Act 2012 now provides for a code of practice to be issued in relation to surveillance camera systems.

2009. In particular, the general debate about whether it is better for the location of fixed ANPR cameras to be completely open and provide a so-called "ring of steel" or scattered (and relatively covert) is still one that can be pursued without the public knowing the precise location of the cameras; and there is no evidence that the Respondent was in fact using the ANPR system improperly, for example to focus wrongly on a particular community.

14. Mr Vassall-Adams also maintained that knowing the location of ANPR cameras would assist members of the public in making focussed "subject access requests" under the Data Protection Act to find out what data the police held about them obtained by such cameras. We accept this point to a limited degree but the fact remains that not knowing their location is no bar to anyone making a subject access request and that knowing their location will not tell the citizen what data has been obtained about him, or whether it has been kept too long or misused.

15. A related point which was discussed at the hearing was whether knowledge of the position of the cameras might assist those accused of criminal offences to establish a legitimate alibi; in relation to this we accept Mr Johnson's points (a) that it would be open to a defendant in such circumstances to make a suitable subject access request or to caste the onus onto the police through his defence case statement to make disclosure of relevant "read" data without him knowing where the cameras were and (b) that knowing where they were might help criminals to manufacture false alibis (eg by getting someone else to drive past a camera in their car at the time they were going to commit an offence).

The balancing exercise

16. We acknowledge that there are important considerations pointing in both directions in this case and that balancing two such strong but different public interests has to involve some measure of instinctive judgment. But taking account of all the circumstances (and in particular the considerations in paras 8 to 15 above) we have reached the unanimous view that the public interest in maintaining the exemptions outweighed that in disclosure. We are reassured that the Commissioner, having also seen the written evidence presented to

us, remains of that view notwithstanding the strong public interest he sees in disclosure in this case.

17. We have therefore decided unanimously to dismiss Mr Mathieson's appeal.

[Signed on the original]

HH Judge Shanks

18 June 2012