



**IN THE FIRST-TIER TRIBUNAL
GENERAL REGULATORY CHAMBER
(INFORMATION RIGHTS)**

Appeal No: EA/2012/0171

ON APPEAL FROM:

The Information Commissioner's Enforcement Notice dated 23 July 2012

Appellant: Southampton City Council

Respondent: The Information Commissioner

Heard at: Field House, 15 Bream's Buildings, London EC4A 1DZ

Date of Hearing: 30 & 31 January 2013

Before

HH Judge Shanks

Judge

and

Andrew Whetnall and John Randall

Tribunal Members

Date of Decision: 19 February 2013

Attendances:

For the Appellant: Timothy Pitt-Payne QC

For the Respondent: Anya Proops

Subject matter:

Data Protection Act 1998

s.2	Sensitive personal data
s.40	Enforcement notices
s.48	Rights of appeal
s.49	Tribunal's powers
Sched.1	Data Protection Principles: Principles
Sched.2	Data Protection Principles: Processing of Personal data
Sched.3	Data Protection Principles: Processing of sensitive data

Human Rights Act 1998

Article 8	Right to a private and family life
-----------	------------------------------------

DECISION OF THE FIRST-TIER TRIBUNAL

The Tribunal dismisses the appeal.

REASONS FOR DECISION

Introduction

1. This is an appeal by Southampton City Council under section 48 of the Data Protection Act 1998 against an enforcement notice issued by the Information Commissioner on 23 July 2012. The enforcement notice in effect required the Council to drop a policy adopted on 26 August 2009 of requiring all licensed taxis in Southampton to be fitted with a CCTV system which includes an audio-recording facility which is in continuous operation. The Commissioner has no objection to a requirement that there should be continuous video-recording; it is only the continuous *audio*-recording that we are concerned with. We are told that this is the first appeal of its type and it is clear that the issues raised are of national significance.
2. We received very helpful written evidence from John Burke (the Council's licensing manager), Chief Superintendent David Thomas of the Hampshire Constabulary, Deputy Assistant Commissioner Martin Hewitt (who gave evidence in his capacity as an ACPO representative with responsibility for adult sexual offences) and Jonathan Bamford, a senior official in the Commissioner's office. Mr Burke and the police witnesses also attended to give oral evidence. We also received written and oral submissions of characteristically high quality from Mr Pitt-Payne QC for the Council and Ms Proops for the Commissioner.

Factual background

3. The Council is the licensing authority in the Southampton area for taxis (both "hackney carriages" and "private hire vehicles", of which there are about 700 or 800 in all) and taxi drivers (of whom there are about 1,300). As such, it has power to attach reasonable conditions to licences granted in respect of taxis.¹ It is not disputed that in exercising that power the Council must, under section 17 of the Crime and Disorder Act 1998, have due regard to the need to do all it can to prevent crime and disorder in its area but it is also not disputed that the purpose of the power to impose

¹ See sections 47 and 48 of the Local Government (Miscellaneous Provisions) Act 1976.

licence conditions is to promote public safety specifically in connection with the use of taxis.

4. In 2004 the Council received funding to help taxi owners install CCTV in their taxis on a voluntary basis but the take up was limited even though the cost to the owners was minimal. In the light of serious violent and sexual offences taking place in or around taxis and the need to protect vulnerable users of taxis, consideration was given by the Council to the compulsory installation of CCTV as an essential tool to deter and help with the investigation of such incidents.

5. On 6 May 2009 the Council's Licensing Committee was invited to consider the adoption of a number of new standard conditions for taxi licences, including the following:

Digital cameras. As crime and safety are both Government and Council priorities it is proposed that all vehicles are fitted with digital cameras as soon as possible ...

The paper put before the committee also stated:

The Council has for some time been fitting digital cameras to licensed vehicles as part of its strategic approach to reducing crime and disorder and improving driver safety...

The camera currently available has not only digital image technology but also a voice recording facility...

Some proprietors have suggested this is another case of 'Big Brother'. This is simply untrue. What the trade and members can be assured of is that the images will only be downloaded where a crime report has been made to the police involving the relevant vehicle or that a member of the public has a specific and recorded complaint against the driver of a specific vehicle.

Mr Burke told us that the "camera currently available" referred to in the paper was a camera called a VerifEye Mark 4 which had become available in early 2008. Earlier versions of the VerifEye camera (which had been installed up until then) had not included any audio facility. There was considerable confusion in Mr Burke's evidence as to the exact capabilities of the VerifEye Mark 4 but the Tribunal was later provided with some material from the manufacturer which indicated that the system is

triggered by certain events (door opening, meter being turned on or “panic button” being pressed), that the video then works for various periods but with only so many frames per second (one every 15 seconds for most of the time) and that the audio facility works continuously but only for a period of 15 minutes after a triggering event.

6. No conclusion was reached at the meeting on 6 May 2009 and there was further consultation with the trade on the issue. The paper prepared by officers for the next meeting on 26 August 2009 stated:

Digital cameras

Digital cameras are currently fitted to about [110 taxis] and are clearly the cause of some concern ... voiced at a recent consultation meeting:

Data protection issues with cameras. **Cameras are compliant and [the] Council is the data controller ...**

Who will pay for the downloading of photographs? **The licensing team have all the secure equipment and authority to download the encrypted data ...**

Concerns from customers being filmed, both adult and children. **The system is completely secure with the data being held in encrypted format. Data will only be downloaded in the event of a substantive complaint either from a driver or passenger or where a crime is alleged.**

...

Cameras are fitted to fulfil two roles; firstly, to ensure the safety of the public and secondly the safety and integrity of the driver.

There was no mention in the paper of audio-recording as such. The licensing committee resolved at the meeting that (among others) the following condition be added to taxi licences:

In line with Government and Council priorities on crime and disorder, public and driver safety all licensed vehicles to be fitted with Council approved digital cameras as soon as possible and in any case at the time a current licensed vehicle is replaced

...

7. At para 28 of his statement Mr Burke gives more detail about the policy as follows:
- 1 All passengers are made aware of the fact that they are being recorded, by notices strategically placed on the vehicles ... These labels clearly warn that both audio and visual recordings take place in the vehicle ... ²**
 - 2 Data will only ever be downloaded on two occasions:**
 - (1) where a crime report has been made involving a specific vehicle and the Police have formally requested that data or,**
 - (2) when a substantive complaint has been made to the [Council] regarding a specific vehicle/driver and that complaint is evidenced in writing (and cannot be resolved in any other way)**
 - 3 The request form for download must state the approximate time of the event/occurrence and only the timescale relevant to the specific incident will be downloaded, de-crypted and thereafter stored.**
 - 4 After a period of time, typically 14-30 days any data is automatically overwritten dependant upon the specification of the system installed.**
 - 5 Only systems approved by the Licensing Team may be installed by an independent installer – thereby ensuring that any equipment may not be tampered with, encryption is of a sufficient standard and data may not be interfered with or released to a third party/published.**

None of this detail is set out in any official document produced by the Council. Mr Burke amplified certain aspects of the policy in his oral evidence as follows. The only people authorised to de-encrypt and download data are Mr Burke and the three enforcement officers in his team; when they decide they need to take this step, the proprietor or driver of the taxi is obliged to present it to them so that the download can take place. The normal “destruction period” of 14 to 30 days is not a function of any thought-out policy decision but is simply dependent on the fact that the systems used only have so much storage space and the amount of time the data is in fact kept is therefore dependent on the useage of the taxi in question, which obviously varies. As to the “systems approved,” the VerifEye Mark 4 to which we have referred remains approved, but in 2011 two new systems, made by firms called Pageantry and Brigade respectively, were also approved; these two systems are superior to the

² A colour copy of the label is at p210 of bundle.

VerifEye Mark 4 system in that they provide continuous and full video and audio recording of everything that goes on in a taxi. Mr Burke was keen to stress and we fully accept that the Council's primary concern in selecting any system for approval was the security of the system in relation to access so as ensure that no-one was able to get hold of the data improperly. It is not disputed that the desired effect of the policy (notwithstanding the special situation with the still approved VerifEye Mark 4 system) is that every word spoken in a licensed taxi is recorded, whether it is part of a conversation between passengers, between passenger(s) and driver, or between the driver or a passenger and someone on the other end of a phone call; and it covers not only periods when the taxi is being used as a taxi but also periods when it is being used privately by a driver or proprietor, for example to take his family on holiday.

8. We were told that since the licensing condition was introduced the police have asked the Council for access to audio-visual recordings made in taxis on 193 occasions, of which Chief Superintendent Thomas was able to review 164 where it had been possible to get access to a relevant recording. Of these, the majority arose out of incidents taking place in or near taxis and involved criminal allegations against taxi drivers or passengers which included racially aggravated and sexual assaults, though by far the largest group (34 in all) involved allegations of making off without payment. However, there was also a substantial number of requests which involved serious criminal offences (including murder, other serious violence and drug dealing), but which did not directly involve taxis, where the police were simply seeking evidence which may assist their enquiries, for example where suspects had left the scene of a crime by taxi. Mr Burke accepted that in these cases the police were in effect making use of a form of surveillance for which they required no warrant (though it is right to note of course that the surveillance is not covert).
9. There was also a smaller group of downloads made by his team, estimated as 10% of the total by Mr Burke, which did not arise from a police request at all and did not necessarily involve any criminal allegation but which generally arose out of complaints by the public. Mr Burke's evidence was that such downloads would only take place if the allegation in question gave rise to some likelihood of a driver's

licence being withdrawn but he accepted that this may include occasions, for example, where a young female passenger had alleged that a taxi driver had inappropriately invited her out on a date.

10. On 23 July 2012 the Commissioner issued his enforcement notice under section 40 of the Data Protection Act. In the notice he referred to the Council's policy adopted on 26 August 2009, to a report on that policy and correspondence he had had about it with the Council, to his own Code of Practice on CCTV revised in 2008 and to relevant provisions of the Act, in particular the first data protection principle, and Art 8 of the European Convention on Human Rights (ECHR). He stated his view that the Council's policy involved a breach of the first data protection principle in so far as it required an audio-recording facility in permanent operation and that it may result in damage or distress. He therefore required the Council to refrain from recording "any such personal data in future."
11. The Council launched their appeal to the Tribunal on 2 August 2012. By virtue of section 40(7) of the Act, the Council did not have to comply with the enforcement notice pending determination of the appeal, a provision we understand the Council has taken advantage of.

The legal framework and the issues on the appeal

12. There is no issue that words recorded by the equipment installed in taxis under the Council's policy comprise "personal data" for the purposes of the Act; the relevant "data subject" would no doubt include the speaker but may very well also include other parties to any conversation or those being talked about. There is also no dispute that the Council is the "data controller" of that data for the purposes of the Act and that the very act of recording is a form of "processing."
13. It is therefore clear that the Commissioner had power under section 40(1) to issue an enforcement notice against the Council if he was satisfied that the audio-recording involved the contravention of a data protection principle; the primary issue in the case

is whether he was right in his conclusion that this was so. In deciding whether to exercise his power to issue an enforcement notice the Commissioner was also obliged to consider under section 40(2) whether “the contravention has caused or is likely to cause any person damage or distress.” Although it is accepted that a finding to this effect is not a pre-condition to the issue of an enforcement notice, the Council say that in this case the Commissioner approached section 40(2) in a fundamentally flawed way and that, even if he was right to conclude that the Council was contravening the first data protection principle, he ought not, as a matter of discretion, to have issued an enforcement notice. We return to this issue below.

14. The data protection principle relied on by the Commissioner, namely the first, provides as follows:

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

The only potentially relevant conditions in Schedule 2 are these:

3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

...

5. The processing is necessary-

(b) for the exercise of any functions conferred on any person by or under any enactment,

...

(d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

...

6.-(1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed,

except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

And the only potentially relevant condition in Schedule 3 is:

7.-(1) The processing is necessary-

...

(b) for the exercise of any functions conferred on any person by or under an enactment.

15. There is a side issue (to which we return below) as to whether the Council's policy involves the processing of *sensitive* personal data (and therefore whether the Schedule 3 condition needs to be met), but in any event the parties are agreed that the essential question on contravention is whether Art 8 of the ECHR (which guarantees the right of privacy and which we set out below) is infringed by the Council's policy, and in particular whether the policy is justified under Art 8(2) as a proportionate means of achieving a legitimate aim. This is because it is common ground that if Art 8 is infringed by the policy, the audio-recording of conversations will not be "lawful" for the purposes of the first data protection principle by virtue of the Human Rights Act 1998 and, furthermore, that none of the conditions we have identified as potentially relevant will be satisfied, in that the processing will not be "necessary" for any of purposes set out therein any more than it will be "necessary" for the analogous purposes set out in Art 8(2).

16. The Tribunal's powers in relation to an appeal are set out in section 49 of the Act:

(1) If on an appeal under section 48(1) the Tribunal considers-

(a) that the notice against which the appeal is brought is not in accordance with the law, or

(b) to the extent that the notice involved an exercise of discretion by the Commissioner, that he ought to have exercised his discretion differently, the Tribunal shall allow the appeal or substitute such other notice or decision as could have been served or made by the Commissioner, and in any other case the Tribunal shall dismiss the appeal.

- (2) On such an appeal, the Tribunal may review any determination of fact on which the notice in question was based.**

It is common ground based on the wording of section 49 that on an appeal the Tribunal has full power to re-consider the whole matter in the light of all the evidence put before it, including the question whether the discretion ought to have been exercised differently, although due respect must of course be afforded to the views of the Commissioner, who is the person entrusted by statute with the job of enforcing the Data Protection Act.

17. The issues on the appeal can therefore be summarised as follows:

- (1) whether the words recorded under the Council's policy include "sensitive personal data";
- (2) whether the Council's policy infringed Art 8 of ECHR;
- (3) whether the Commissioner was right to exercise his discretion to issue an enforcement notice.

We will deal with them in that order.

Sensitive personal data

18. "Sensitive personal data" is defined by section 2 of the Data Protection Act as personal data consisting of information as to:

- (a) the racial or ethnic origins of the data subject,**
- (b) his political opinions,**
- (c) his religious beliefs or other beliefs of a similar nature,**
- (d) whether he is a member of a trade union,**
- (e) his physical or mental health or condition,**
- (f) his sexual life,**
- (g) the commission or alleged commission by him of any offence ...**

19. Mr Pitt-Payne maintained that in the absence of specific evidence the Tribunal could not find that the Council's policy involved the processing of *sensitive* personal data. We consider that an unrealistic approach. Based on our collective knowledge of the world we are quite satisfied that the inhabitants of (and visitors to) Southampton will from time to time discuss their own and others' sex lives, health, politics, religious beliefs and so on in taxis (notwithstanding the presence of the taxi driver) and, if necessary, we take judicial notice of that fact. It is also worth noting in this context that there must be numerous conversations in taxis of a sensitive nature which do not necessarily come within the strict definition of "sensitive personal data", for example commercial negotiations carried on by a businessman with a client by telephone in the back of a taxi.

20. Mr Pitt-Payne also made the point that it would be open to taxi users, having been informed by the label in the taxi that their conversations were being recorded, not to discuss sensitive matters which they did not want to have recorded. Again, we consider that an unrealistic approach. We do not see why anyone should be forced to modify their normal behaviour in such a way, by being forced to treat what is now (at least) a semi-private space as a public one, not least the taxi driver driving his taxi to a holiday destination with his family. We also note Ms Proops' point that, if the Council's policy resulted in people "self-censoring" their conversations, that would *prima facie* involve a contravention of Art 10 of the ECHR which guarantees freedom of speech.

Art 8 ECHR

21. We set out the familiar terms of Art 8 of the ECHR:

- (1) Everyone has the right to respect for his private and family life, his home and his correspondence.**
- (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of ... public safety ... for the prevention of disorder or crime, ... or for the protection of the rights and freedoms of others.**

22. The Council is prepared to accept that the recording and retention of data under its policy constitutes an interference by a public authority with the right of privacy conferred by Art 8(1). However, it says that such interference is justified (or "... necessary in a democratic society ...") in the interests of public safety, the prevention of crime and the protection of others. It is well established that in order for such an interference to be justified it must serve a "legitimate aim", meet a "pressing social need" and be "proportionate." The Commissioner accepts that the policy serves a "legitimate aim" (which he describes rather narrowly as "assisting in the detection of crime" but which we have no doubt includes all three of the aims relied on in Art 8(2) so far as they relate to the use of taxis) and that there is a "pressing social need" for some surveillance in taxis (though he says there is no "pressing social need" in so far as such surveillance relates only to misconduct by drivers rather than crime). The real issue therefore comes down to the question whether the Council's policy of continuous audio-recording is "proportionate".

23. The question whether the policy is "proportionate" is ultimately one of judgment for us as a Tribunal, balancing the benefits to the legitimate social aims it is likely to achieve against the extent of the interference with the right of privacy likely to be caused. In striking this balance it is important to note two things: (a) the "legitimate aim" of the policy is that of deterring and detecting *taxi-related* crime and other misconduct; the fact, as we mention in para 8 above, that the police have been able to obtain useful evidence about crimes not directly related to taxis cannot therefore come into the balance as a benefit; (b) the relevant benefits and disbenefits are only those marginal ones that come from *audio-recording*; no-one is complaining about the existence of CCTV in taxis as such or about video-recording.

Benefits of the policy

24. As the Council point out forcefully, there are special features of taxis which make those who use them particularly vulnerable to crime. In general, neither drivers nor their passengers have any real choice about making a journey in a taxi, the driver because it represents his living and the passenger because he often has no other

practical means of getting from A to B. Passengers are sometimes vulnerable in themselves, either by nature because they are children or suffer mental or physical disabilities (and the Council itself often contracts with taxi drivers to carry such people) or because they are intoxicated one way or another after a night out. Passengers and drivers are generally strangers to one another, forced to share a confined space in a moving object over which the driver has control. Physical, sexual and verbal assaults (either way) are therefore particularly dangerous when they occur in the context of taxis. Drivers are also particularly vulnerable to the risk of passengers making off without payment. Nevertheless the vast majority of drivers and passengers are of course honest and law abiding and the vast majority of journeys pass off with no incident at all.

25. It must be the case, and we accept, that the existence of CCTV in taxis tends to deter crime and assists in its investigation when it does occur and similarly that it assists the Council in relation to its function of licensing only suitable taxi drivers. The extent of any deterrence, and in particular the extent of any additional deterrence arising from audio-recording, is, we think, unlikely to be susceptible to hard proof and the unsuccessful attempt in Mr Burke's written statement to enlist statistical evidence to demonstrate the success of the policy in deterring crime confirmed our view about this. However, we do accept that there must be some additional deterrent effect from having continuous audio-recording in taxis. For example, it was suggested that a drunken group intent on trouble may get into a taxi and one of their number may persuade the others not to start being abusive by pointing out the audio-recording label, thereby preventing trouble that would otherwise ensue from "kicking off" in the first place. A driver who may be thinking of propositioning a lone female passenger may be deterred from doing so with the consequence that a subsequent sexual assault that might have followed just never happens. A passenger who gets into a dispute with a driver may be constrained in the language he uses and, in particular, not resort to racial abuse.

26. As for assisting the investigation of crime (and lesser matters of complaint) in taxis, which is obviously of great use to the police and the justice system and to the Council

in its licensing function, it was clear that in *some* of the cases we refer to at paras 8 and 9 the existence of audio-recording in addition to video-recording had made a real difference. The clearest were a few cases where drivers had alleged that passengers were guilty of racially aggravated assaults or racial abuse where, obviously, the existence of audio-recording was crucial. There was also reference to one or two allegations of sexual assault where the video-recording did not show exactly what was going on out of view of the camera but an audio-recording would help, and one can imagine that the recording of the conversation before an alleged sexual assault might assist in establishing whether sex had been consensual. There may also be cases where the existence of an audio-recording would assist in establishing an offence of making off without payment or whether a driver had behaved inappropriately (but not criminally) in a way that would affect his entitlement to a licence. It is right to note also that benefit comes from the ability not only to prove true allegations but also to disprove false allegations. And it is right to recognise that while few of the examples raised involved really serious crime, it *may* be that one day there is a rape or a murder associated with a taxi which would have been successfully prosecuted if there was audio-recording but not if there was only video-recording.

27. The Commissioner raised the possibility of a more targeted and less intrusive alternative to continuous audio-recording, and in particular a “panic button” system whereby the driver or passenger could activate audio-recording if a need arose at the press of a button. As we understand it, there is no technical bar to such a device and the Commissioner would regard it as an acceptable alternative. We agree with the Council that the Commissioner did not fully meet its criticisms of a panic button system. We accept that such a system would clearly not be as effective as continuous audio-recording, since it would obviously not be as full a deterrent, it would require often vulnerable or incapacitated passengers to make use of it and it would by definition miss the initial and perhaps most important part of an incident. However, a panic button system would have some (albeit limited) additional benefits in relation to the legitimate aims being pursued over a pure video-recording system. For what it is worth, therefore, the relevant benefits of the Council’s policy for us to consider are only the additional marginal benefits associated with a *continuous* audio-recording system over those that could be achieved with a panic button system.

Extent of interference

28. We have already alluded to the extent of the interference with privacy rights involved in the Council's policy in paras 7, 19 and 20 above. In short, every single conversation, however private and however sensitive the subject matter, taking place during every single taxi ride in Southampton (of which there may well be a million a year) will be recorded and accessible to a public authority.
29. Mr Pitt-Payne emphasises aspects of the policy which he says mean that it involves only a slight interference with privacy rights: first, the data is only retained for a short time (14 to 30 days) unless it is accessed for good reason; second, access to the data is confined to a few individuals (Mr Burke and his team); and, third, their access is strictly controlled: there must be a request relating to a specific incident or allegation from the police or which Mr Burke and his team judge worthy of further investigation. The evidence is that the data has been accessed on only about 200 occasions in three years. It is not in any sense continuously monitored. We accept that these are highly relevant considerations but there are a number of points which go to weaken them in our view.
30. First, as we have mentioned, the policy has never been written down as such and we are concerned that, at least in so far as it relates to audio-recording, it was not very fully consulted on or well thought through. Rather it appears to have been driven by technological developments. The 14 to 30 day retention period in particular is simply a function of the capability of the systems and, if a new approved system came along which could retain data for much longer, there is nothing in the policy to stop data being so retained. Second, there is already evidence of what was called at the hearing "function creep": for example, the use of the system by the police to gather evidence about crimes not directly related to taxis, however beneficial in itself, was not (or should not have been) part of any policy devised by the Council arising from its taxi licensing function. Third, it has to be accepted that however robust the systems in place and however well-intentioned and conscientious Mr Burke is (and he made a generally good impression on us) there must always be a danger that a taxi driver or a

Council official or someone else will access and make improper use of this data. As it is, we were told that there were possibly four to five “data access requests” per year (generally made by taxi drivers) which had been acceded to: we do not have details of these but we wonder whether full consideration was given to the interests of data subjects other than the requester and we note that, once in the hands of the requester, notwithstanding the Council’s standard letter warning him that to publish will involve a breach of the Council’s copyright, there is little that anyone can do in practice to control the use of such data (and these days they can be instantly broadcast to the whole world through sites like *YouTube*).

31. Both sides sought to demonstrate in different ways that there was public support for their respective positions. The Council relied on the outcome of their consultation and certain opinion polls in Southampton. Although we were open to the possibility that firm evidence of local support or opposition could be relevant on the proportionality issue, we did not consider that the exercises relied on were sufficiently focussed on audio-recording to have any influence on our decision. The Commissioner relied on various complaints about the policy, in particular by taxi owners and drivers; without knowing more about motivation we do not think that any weight can be attached to these either.

32. We do, however, give some weight to the views expressed by the Commissioner in his 2008 Code of Practice on CCTV where he states:

CCTV must not be used to record conversations between members of the public as this is highly intrusive and unlikely to be justified. You should choose a system without this facility if possible. If your system come equipped with a sound recording facility then you should turn this off or disable it in some other way.

There are limited circumstances in which audio recording may be justified, subject to sufficient safeguards. These could include:

...

- where recording is triggered due to a specific threat, e.g. a panic button in a taxi cab.

We also formed the view that (notwithstanding the possible benefits to them of the Council's policy) the police witnesses took a somewhat neutral stance on the question of the proportionality of continuous audio-recording.

Conclusion on proportionality

33. Having regard to the considerations set out at paras 24 to 32 above, and paying due respect to the Commissioner's views, in our judgment the Council's policy, in so far as it requires continuous blanket audio-recording of everything said in taxis, is disproportionate when the extent of the interference with the right of privacy is weighed against the marginal benefits to the legitimate social aims of increasing public safety and reducing crime in relation to taxis which are likely to result from it. It follows from that conclusion that the policy is not justified under Art 8(2) and accordingly that it contravenes the first data protection principle.

34. Having reached that conclusion we wish to record that we were impressed by the police evidence in this case and that we appreciate the nature of the problem and the special vulnerability of some taxi passengers, in particular children, those with disabilities and those travelling at night, especially when they are "the worse for wear" as is so often the case. It may be that, bearing these points in mind, there is scope for a more targeted scheme involving audio-recording based on times of day, types of customer (for example, children or vulnerable adults carried under contract between a taxi firm and the Council), the use of panic buttons or a combination thereof, which strikes a better balance between the competing considerations and does not contravene the Data Protection and Human Rights Acts. Any such scheme would be a matter for the parties to work out and not for this Tribunal to put forward.

The exercise of the discretion by the Commissioner

35. Mr Pitt-Payne submitted that the Commissioner's approach to section 40(2) was flawed and that, in any event, he ought not to have exercised his discretion to serve an enforcement notice. Looking at para 8 of the enforcement notice we are inclined to agree with him that the Commissioner did not apply a sufficiently stringent test of

likelihood of damage or distress. However, we do not think that we need to consider that matter further for the simple reason that, having concluded that the Council were acting in breach of the Data Protection Act and having regard to the high level of public importance of the case, we think it must have been right in this case to decide to issue an enforcement notice, regardless of the likelihood of any actual damage or distress resulting from the policy.

Conclusion

36. We therefore dismiss the appeal. Our decision is unanimous.

Signed:

HH Judge Shanks

Date: 19 February 2013