Big Brother Watch

Southampton Council, Cameras Fitted In Licensed Taxis and Private Hire Vehicles Consultation

21 May 2013

1. **Whether the condition to have cameras in vehicles licensed by the authority should be mandatory or not?**

Taxi drivers should not be forced to install surveillance equipment in their taxis. Voluntary schemes and panic button systems would offer a solution to those drivers who feel their safety is at risk without forcing every taxi to record their passengers.

We would not object to the council publishing non-binding guidance on best practice and standards of CCTV, but this should absolutely not in the manner of "all systems must adhere to the specifications contained in the Council's guidance" – it should only be advice and non-mandatory.

2. **Should the recording of visual data be permanent or triggered? If triggered what controls the trigger and for how long should a recording be? What would be the benefits or disbenefits?**

We believe if drivers choose to install CCTV, then a panic button system would work to protect them as well as an always-on system, without the associated risks to privacy of law-abiding passengers.

The case for always-on CCTV should be based on a legitimate problem and an impact assessment should require evidence to be provided of what that problem is, how it will be monitored to measure CCTV effectiveness and what the alternatives are, and why they are not suitable.

3. **Should there be any audio recording and if so to what extent?**

Audio surveillance in particular is a gross intrusion on privacy and an entirely disproportionate response to the risk posed. Furthermore, installing such

technology goes entirely against the Information Commissioner's code of practice on CCTV use, which states CCTV should not be used to record conversations except in situations where it is absolutely necessary.

The ICO's code of practice for the use of CCTV is very clear on the issue of audio recording;

"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 comes equipped with a sound recording facility then you should turn this off or disable it in some other way."[1]

So even with a panic button, there is a question as to whether this is still too intrusive.

4. The choice of Data Controller between the Council and the vehicle owner. What would be the benefits and disbenefits?

This is a critical decision. If taxi drivers are the data controllers, then any breach of the Data Protection Act would result in action against the driver. Our concern is that if the Council is the controller, while this has a benefit of existing processes and expertise on DPA compliance being available, the reality of enforcement is that it does not result in individual-level action and any penalty is manifested at a corporate level.

As such, we believe taxi drivers should remain data controllers, particularly as this is far more appropriate to a system where drivers are individually responsible for the decision about installing CCTV in the first place. (We support such a model over any mandatory system)

However, if a mandatory system is introduced, an explicit recognition that through such a system, there is de facto vicarious liability on part of the council should be included. Given a mandatory system may mean drivers who do not wish to install any CCTV equipment would be required to do so, this would arguably be the legal position anyway.

[1] http://www.ico.org.uk/for_organisations/data_protection/topic_guides/cctv

The council's responsibilities to monitoring the policy should include proactive assessment of any DPA infringements, irrespective of who is the data controller.

Further point:

The issue of panic button systems is clearly central to this question. We believe they are a useful way forward to ensure surveillance is not directed at law-abiding people, however there would still be a question over use and

As such, we suggest that if any system is to be installed, the following minimum standards should be adhered to:

- The system must be secured from access by the driver
- Audit processes must be in place to allow an official to see how many times the panic button was pressed and for how long recording took place.
- If there is evidence the system is being over-used, steps taken to investigate why
- License conditions should include that any unauthorised publication or sharing of video or audio would result in immediate revocation of the individual's license

We would also reaffirm our belief that unless there is a criminal offence, punished with a custodial sentence, of abusing or disclosing data collected by CCTV systems, then the risks are still too great. The recent case in Ireland of a person being mis-identified from CCTV footage that ended up on the internet is a salient warning.