

Data Sharing Review

Richard Thomas and Dr Mark Walport

Consultation paper on the use and sharing of personal information in the public and private sector

List of questions for response

We would welcome responses to the following questions set out in this consultation paper. Please follow the question order as set out in the consultation paper, leaving a blank response box for any questions not answered.

Please email your completed form to contact@datasharingreview.gsi.gov.uk

Alternatively you can send a hard copy response to:

Data Sharing Review Secretariat
5.26 Steel House
11 Tothill Street
London
SW1H 9LJ

Thank you.

Section 1: Background

Question 1.

Comments: CCTV Compliance with the Data Protection Act. Concentrate in ensuring that individuals and organisations are aware of the issues of CCTV compliance. Any sharing of data must be properly controlled.

Section 2: Scope of personal information sharing, including benefits, barriers and risks of data sharing and data protection

Question 2.

Comments: Crime Prevention and Detection – but must be carried out correctly to retain public confidence.

Question 3.

Comments: The risks are that the public lose confidence in CCTV systems if the data controls are not correct and enforced.

Question 4.

Comments: The risks re CCTV images are the possible misuse of images, tampering of evidence, confidence in procedures. This could lead to evidence being questioned.

Question 5.

Comments: Public authorities' CCTV systems are very often gathering images / data outwith the purposes of the system. Law authorities may also rely on images from systems which are overlooking areas outwith their area for their own purposes – thus raising compliance questions.

Question 6.

Comments: Private sector CCTV systems are very often gathering images / data outwith the purposes of the system. Law authorities may also rely on images from systems which are overlooking areas outwith their area for their own purposes – thus raising compliance questions.

Question 7.

Comments: Passing of images from Shopping Malls to individuals shops to identify potential problem individuals. Also town centre shops could be linked and images passed out to give advance warning of a shoplifter. Full DPA compliance must be enforced for everyone to have confidence in CCTV.

Question 8.

Comments: A large number of CCTV systems inadvertently and incorrectly share data with other systems and individuals against the DPA. Example being airports and police – the police being in charge of the system and airport personnel being allowed access to images. Also CCTV operators allowing third party companies access to images without correct procedures.

Section 3: The legal framework

Question 9.

Comments: For CCTV systems there is a great deal of ignorance among those using the systems. The DPA and it's implications are not publicised enough. Risk Assessments and audits should be mandatory and policed. No CCTV should be used unless operated under the DPA. There should be automatic official feedback from police when requested to view CCTV on the standard of the images and security.

Question 10.

Comments: The second principle is extremely important. Many CCTV systems – especially when they have been upgraded – use the system for much more that the purposes as stated. It is very common to see CCTV being used for much more that as stated to the ICO. It could be that the original system was only used for Crime Prevention and Public Safety but having invested in a very sophisticated modern digital system, the organisation realise how much more it can be used for – stock, staff monitoring, footfall etc

Question 11.

Comments: Issues and repercussions on data captured by CCTV systems not fully explained. No enforcement by experts. No obligatory audits / inspections. Lack of power for the ICO. Lack of expertise in the ICO.

Question 12.

Comments: Issues and repercussions on data captured by CCTV systems should be fully explained. Enforcement by experts. Enforce obligatory audits / inspections. More power for the ICO inline with H&S Executive. More training and expertise within the ICO regarding CCTV systems. Heavier penalties for non-compliance. Police report backs. Compliance certificate required for licences and insurance purposes. The DPA should be rigorously enforced with suitable education and training.

Question 13.

Comments:

Question 14.

Comments: The ICO should have statutory powers to inspect and have audited CCTV systems to ensure the DPA requirements are observed. Organisations are ignoring the DPA requirements for CCTV as the ICO has no proper powers.

Question 15.

Comments: The DPA is relatively straightforward for CCTV systems but should be implemented and enforced thoroughly.

Section 4: Consent and transparency

Question 16.

Comments: Most organisations are not fully aware of the limitations of sharing CCTV images and must be made aware. They are under the impression that they can share images with anyone who requests.

Question 17.

Comments: Gaining consent from individuals to capture them on CCTV is not a barrier but requires CCTV operators / owners to think about what they are doing and why.

Question 18.

Comments: The sharing of CCTV images is restrictive under the DPA and should remain so. A full and accurate audit trail should be enforced for the complete lifecycle of the images / data.

Question 19.

Comments: Regular impact assessments and audits should be mandatory by an independent authority

Section 5: Technology

Question 20.

Comments: More investment is made in more sophisticated CCTV systems and organisations will use their CCTV systems for more purposes outwith their stated purposes. Regulation should be enforced through licencing / certification. New technology has moved CCTV on to new areas which need to be regulated – IP/Internet/wireless/handhelds/entertainment/lapel

cams/"helicopter cams etc

Question 21.

Comments: There needs to be a requirement for regulation and "licensing" of CCTV. It should be fully explained that the onus is on the operators and data controllers of the CCTV system.

Question 22.

Comments:

Section 6: International comparisons

Question 23.

Comments:

Question 24.

Comments:

Question 25.

Comments:

Question 26.

Comments:

Section 7: Additional questions

Question 27.

Comments: The sharing of CCTV images.

Question 28.

Comments:

1. Requirements for police to report CCTV systems where images not fit for purpose. These systems then to be audited and rectified as necessary.
2. Local Authorities to include CCTV DPA compliance audit certificates as a requirement for licence applications – liquor, taxi, public transport, planning, hotels, casinos, shops etc.
3. Regulatory body needs to work closer with CCTV industry and representatives in moving forward to ensure that all CCTV are compliant with the DPA.
4. Home CCTV systems should also be regulated and more sophisticated systems are designed – it is not just a matter of a door entry camera as in the past.
5. CCTV installers should be regulated to ensure that systems are not installed in such a way that they are not compliant from installation.
6. Major issues of technology for sharing data – compatibility of CCTV recordings e.g. organisation - police – criminal justice system – courts.

In conclusion, it must be realised with the steady progress of technology that the capability of CCTV and also the sharing of data captured by CCTV will push surveillance to the limit and therefore it must both be policed and anticipated. Moves must be made to seriously police and enforce the current requirements of the DPA in respect of CCTV systems to a) ensure that systems are used correctly b) ensure that evidence gathered by CCTV will not be challenged due to non-compliance with the DPA and c) ensure that the confidence of the

public in CCTV is not endangered.

The current DPA is adequate for the present time but should be under constant review to anticipate society and new technology. The DPA is not enforced for CCTV systems. For example, the majority of the figure of 80% of CCTV systems (Home Office CCTV Strategy Report 2007) which provide images which are not good enough quality to be used as evidence could be virtually wiped out if the DPA was policed and enforced correctly for CCTV systems. This would result in more confidence in CCTV systems and also the saving of police resources trawling through hours and hours of CCTV images only to find that they are not of the required standard.

All CCTV systems should be fit for purpose(s) as registered with the ICO.