RTIG

The use of cameras on bus networks

A guide to good practice

RTIG Library Reference: ***RTIGPR006-D002-1.0***

Note: in February 2008 DfT published technical requirements for CCTV devices used in civil traffic enforcement. This document has not yet been updated to take these into account.

16 March 2007

Price:

Foundation Members:	Free
Full Members:	Free
Associate Members:	Free
Non-members:	£250

Introduction

Closed circuit television (CCTV) and related video technologies have been used in security management for many years. Cameras have become a familiar sight, first on site perimeters, then in supermarkets, and in town centres. Since about 2000 they have increasingly been fitted to buses

Cameras and video technology have developed significantly in recent years. The advent of cost effective, reliable, digital imaging technology has allowed cameras to be deployed more widely than before, while the development of video analysis software have allowed much greater automation in their use and management.

In parallel with this there have been a series of legislative developments that have a material impact on the operation and utility of cameras.

An RTIG scoping study in Autumn 2005 found that local authorities and bus operators would value good-practice guidance for the use of technology systems in support of transport security. To help meet this need, RTIG has compiled the present document as a good-practice guide to the use of CCTV in the bus industry.

The purpose of this document is to collate as far as possible good practice guidance regarding the functional, technical and operational requirements for CCTV systems for all stakeholders in the bus industry. This document is not a prescriptive standard and the specifics of any particular system must be determined on the bases of a risk assessment. This document may be updated from time to time as changes in legislation, technology or good practice require. A Short Glossary of Terms is included for information in Annex A.

A few of the statements made in this document are statutory requirements. Those statements are presented in a text box like this. These are rules with which you **must** comply. Other statements are 'dos' and 'don'ts' based on good practice, either taken from previously developed guidelines or collected during the current project.

Some regulations only apply in certain circumstances. The guidance attempts to apply a uniform standard to all

circumstances and contexts, but the legal force of statements may vary because of this.

This document itself has no formal status. It is a guideline document and has not been formally approved. Specifically the inclusion or exclusion of any statement from this document should not be taken as proof of its relevance or irrelevance.

RTIG welcomes feedback on this document and will endeavour to keep the guidance current. Please contact the RTIG secretariat at secretariat@rtig.org.uk, or by post to RTIG Secretariat, c/o Centaur Consulting Limited, Surrey Technology Centre, Surrey Research Park, Guildford, Surrey GU2 7YG.

The editors wish to thank all those who gave their time to the Working Group that produced this document – Neil Cohen (HOSDB), Neal Skelton (ITS UK), Keith Waghorn (TfL), Dick Wallis (Position Systems Ltd), Adrian Waters (Infocell Solutions) and Raymond Webb (WayOut Associates Ltd).

For those looking for more detailed advice, a list of references is provided at the end of the document. This includes the full text of regulations which are cited in guidelines.

List of contents

1. The function of video systems

Introduction

Camera technology – still or video – is uniquely useful in recording recognisable, visual representations of the world. It may be in colour, black and white or combination of both including audio In a transport context this can be useful in a number of ways:

- To increase the levels of personal security for the driver and his/her passengers
- To provide additional information to a driver about his/her vehicle's immediate travel environment, enhancing road safety
- To provide information to a control room or driver about traffic conditions
- To provide information to a driver or control room about non-transport activities, including anti-social and criminal activities: vandalism, robbery/theft, disorder, and counter -terrorism

In each case there is a spectrum of usage, from pure information (monitoring), through information used to prompt further action (intelligence) and data (information) that can be used in a Court of Law or used for proof of a claim (evidence).

These variations impose different requirements on the cameras, and the systems of which they are part. Some of these requirements are underpinned by legislation, some are best practice, others simply by utility and effectiveness.

Camera based systems can be expensive to buy, integrate and operate. Although camera technology itself is getting cheaper and more capable, it may require considerable supporting civil engineering and IT, and the operation of a system may require a significant element of human activity. If the system is to be effective, it is crucial that before implementation, an assessment is carried out to determine, whether CCTV addresses the issues, the purpose of the CCTV, and what information is required from the system.

Do:	be clear on which functions you want your camera system to perform – it will affect both the technical specification and operations. Complete parts 01 and 02 of an Operational Requirements

	explore the potential for a camera to be used in multiple roles
	consider carefully where the key costs lie before embarking on a camera project
	advertise the fact that you are using cameras, as a deterrent

Do not:	try to force each camera into multiple jobs – this may result in over-specification and excessive cost

Security needs

Security is important for both passengers and operators. The DfT guidance note "Get on Board" cites the following:

We know from research…into the transport needs of different social groups, that the personal security issues for passengers are as follows:

- *the time spent waiting for the bus is generally more fearful than the time spent on-vehicle*
- *women consistently express higher levels of fear than men*
- *fear is greater after dark for both men and women*
- *black and minority ethnic groups are more fearful for their security than their white counterparts*
- *the presence of young people and people who have been drinking tends to make other passengers more uneasy*
- *young people have similar fears to adults, with similar gender differences*
- *young people are more likely to be bullied or intimidated by other young people than by adults*
- *people with learning disabilities are particularly subject to harassment and bullying*
- *the presence of graffiti and vandalism contributes to perceptions of unease/fear for adult passengers, although this is less so for young people*
- *the majority of incidents of harassment or intimidation on bus travel – as elsewhere – goes unreported either to operators or the police*

For operators:

- *graffiti and vandalism to buses and bus infrastructure is often a serious and costly problem, warranting significant financial investment in preventative measures such as CCTV*
- *Transport for London estimates the annual cost of vehicle damage to be around £10m*
- *44% assaults on drivers are serious enough to result in some days being taken off work, and a further 13% result in the victim being off work for the remainder of their shift*
- *assaults against staff are most likely to be associated with traffic or fare disputes and regulating passenger boarding numbers*
- *many operators report an increase in the problem of both staff assaults and damage*
- *the school bus journey at the end of the day is often particularly problematic*
- *bus stations tend to become magnets for people looking for relative warmth and shelter, such as those who are homeless, and young people*
- *travel without a valid ticket is often associated with other crime and other nuisance behaviour*

Cameras and the law

Camera use is hedged about with legal constraints and implications. These fall essentially into two categories.

The most difficult area is, perhaps, the Data Protection Acts, which provide limitations on how "personal information" can lawfully be recorded and stored, and who has access to those images. Fortunately the Information Commissioner has issued substantial guidance on this area. However, a CCTV system and its owner must be registered with the Information Commissioner's Office under the Data Protection Act.

Regulation

…personal data must not be processed unless an entry in respect of the data controller is included in the register maintained by the Commissioner…

Source: Data Protection Act 1998, section 17(1)

The second type of legal constraint arises where the camera data is to be used for evidence or prosecution. Any CCTV image is admissible in court as evidence. Its weight as evidence, however, will be enhanced if the technical quality is high, the operational procedures are open, transparent and robust and the audit trail is clear and well maintained.

This document sets pointers to some legal instruments but cannot be regarded as definitive. We recommend that whenever a CCTV system is installed, legal advice is sought as well as advice from all stakeholders in the project: including operators, drivers, police, and the local authority etc.

Annex B lists a number of sources of information on legal constraints, though it does not claim to be comprehensive. Note also that some of these do not apply across the whole UK: readers in Scotland, Wales and NI may be subject to additional or alternative legal constraints.

Do:	get legal advice prior to implementing any camera-based project
	Register the CCTV system with the Information Commissioners office and detail what the systems are being specifically used for. There is an annual fee of £35 payable. Also ensure that this registration is kept up to date.

Cameras for driver security

Bus drivers operate their vehicles in a wide range of geographical locations and at most hours of the day. They are usually alone and often are entrusted with considerable quantities of money which may present a robbery incentive.

Much has been done to protect against this, including though the deployment of smart cards and street side payment, as well as driver protection screens, sealed cashboxes, etc. Nevertheless, operators are keen to minimise still further the risk of abuse and attack.

Operators have a duty under the Health and Safety at Work Act ("HSWA") to manage this risk, and 'cab TV' has for a while been taking its place as part of this protection.

Regulation

It shall be the duty of every employer to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all his employees.

Source: Health and Safety at Work etc Act 1974, section 2

Cab cameras have a multiple potential benefit – as deterrent, alarm and evidence. There is little hard analysis, but anecdote from areas such as London and Tyneside suggests that:

- the most important function is that of evidence, i.e. the ability to trace and prosecute a driver's attacker;
- the deterrent benefit is important too.

Do:	undertake a risk analysis to determine whether the implementation of cab cameras would be materially beneficial to drivers
	discuss the benefit and functional of cab cameras with drivers and their unions in advance
	expect to design the cab camera system with evidential quality imagery in mind, as described elsewhere in this document
	locate cab cameras where they have a clear view of passengers standing by the driver, even if they are wearing headgear
	locate cab cameras out of reach of passengers standing by the driver
	make sure that the processes are in place to capture, store and use the camera images as evidence
	ensure that signage indicating that CCTV cameras are in operation is clearly visible

Do not:	locate the camera in a way which obstructs other driver activity or view of the road

Cameras for security outside the cab

Passengers too have a right to expect their journey to be safe. They also have a very strong desire to feel safe; passengers regularly cite personal safety as one of the most significant requirements if they are to use public transport more. A DfT survey in 2004 found[1] that "11.5% more journeys would be made on public transport if passengers felt they were more secure". The same survey concluded that "people waiting for or travelling by bus…felt that locally monitored CCTV surveillance was the most reassuring form of security".

This safety requirement applies both on and off the vehicle; the off-vehicle environment includes stops, shelters and stations and the physical approach to and from these.

1 See http://www.dft.gov.uk/pgr/crime/tacklingcrimeonpublictransport.

Street-based service controllers and revenue protection officers are also entitled to the duty of care from their employers imposed by HSWA. Because they deal with the public, they are also at risk of attack – they do not handle cash, but they also do not have the opportunity of a protected cab.

Both operators and local authorities have a duty under HSWA to manage these risks. Again, cameras can provide a component of this protection.

> ## Regulation
>
> It shall be the duty of every employer to conduct his undertaking in such a way as to ensure, so far as is reasonably practicable, that persons not in his employment who may be affected thereby are not thereby exposed to risks to their health or safety.
>
> *Source: Health and Safety at Work etc Act 1974, section 3*

> ## Regulation
>
> It shall be the duty of every employee while at work to take reasonable care for the health and safety of himself and of other persons who may be affected by his acts or omissions at work.
>
> *Source: Health and Safety at Work etc Act 1974, section 7*

Cameras within the bus cabin form a relatively straightforward control environment, and the same is generally true of stations. However shelters and stops are a different case, where the physical security environment merges into the wider public space. There is also a role for outward-facing vehicle-mounted cameras to monitor street areas, particularly where stone-throwing is common.

Do:	consider whether the baseline levels of criminality on a service or route justify the use of vehicle-mounted cameras
	ensure that the distant parts of the vehicle are covered: at the back and, particularly, on the top deck (if any)
	consider installing playback screens in the driver's cab – it makes the point that someone is watching the cameras

	make sure that the processes are in place to capture, store and use the camera images as evidence
	ensure drivers know what they should do in the event of an incident – this may include, for example, triggering the permanent recording of camera data
	consider the siting and environment of shelters on a case by case basis to determine the potential value of shelter-mounted cameras
	consider the use of covert cameras if shelter is signed
	where shelter cameras are deployed partly for passenger comfort, use other mechanisms too – particularly improved lighting

Do not:	install cameras on only a small proportion of vehicles – the deterrent effect is largely lost unless the impact is widely wisible
	distract drivers with in-cab monitors while the bus is in motion

Use of bus cameras for traffic monitoring

The presence of security cameras in the bus environment has direct potential benefits to bus services and passengers. However it can also help with other aspects of enforcement and security.

Bus lane enforcement is the one natural step in this. London has had camera-based bus lane enforcement for several years, and is actively developing this area; a number of other UK authorities are taking up this idea too, particularly now that this has been decriminalised.

Regulation

A device is an approved device for the purposes of regulations under section 144 of the Transport Act 2000 (civil penalties for bus lane contraventions) if it is of a type which falls within any of the following descriptions:...

Source: Bus Lanes (Approved Devices) (England), SI2756/2005

The London experience has been that while this takes considerable resource, there is a clear and substantial cost-benefit case for camera-based bus lane enforcement based on the demonstrable success in improving bus vehicle journey times[2]. The move to more intelligent digital systems is expected to significantly improve this case, particularly by making the camera analyst more efficient.

Once cameras are available and a process in place for bus lane enforcement, it is straightforward to use them for other traffic violations. The easiest step is to other decriminalised (civil law) areas, notably parking contraventions.

In TfL's experience, bus-based (moving) cameras can be good at providing a security "sweep" for fixed offences, such as illegal parking; static cameras can be good at capturing moving targets such as a vehicle driving in a bus lane. Combining the management of moving and fixed camera operations can be helpful.

Pursuing offenders who challenge a Penalty Charge Notice (PCN) can be labour intensive, but most will back down in the face of photographic evidence. Interestingly, the TfL experience is that while only 1% of bus lane infringements are challenged, the figure is more like 20% for parking violations. (The figures for both were much higher when the PCN was sent out without a photo.)

Do:	recognise that bus and shelter cameras may have a use for other enforcement and security areas
	work closely with other potential users to ensure that the most is made of a camera deployment; this includes, in particular, traffic managers and the police

Other uses of cameras

Two other uses of cameras deserve a mention.

2 TfL, personal communication.

The first is a rather specific use: the protection of an operator against vexatious or fraudulent claims. From time to time passengers or other road users may claim that they have suffered injury from a vehicle, and sue. Without evidence it is almost always more costly to contest than simply to settle out of court. A number of operators have cited anecdotal evidence of this being used as a scam, i.e. to gain money from fraudulent claims. Cameras can assist by providing evidence, not just in court but by deterring potential scammers from making fraudulent claims in the first place.

The second is a much more traditional use. Bus Garages depots, and stations, as industrial premises, can benefit from CCTV security, to protect against risks such as burglary and the theft of valuables, equipment, or vehicles. While it is possible that vehicle-mounted systems could contribute to this during the working day, these site security systems are likely to be separate from those directly related to service security. In any case, CCTV should be seen as one of a basket of measures which contribute to premises security. It is always worth ensuring that premises are adequately secured before installing an expensive CCTV system.

Do:	consider whether these other risks would benefit from the deployment and use of camera systems

2. General security systems – design

Introduction

A CCTV system, like any other system, must be designed adequately to perform its functions. There are a number of aspects to this.

Some – the placement of cameras, lighting, and camera control – are part of the environment and essentially independent of technology. Others – image quality, recording and retrieval systems – are very much technology linked.

Most new CCTV systems are digital. However, many analogue systems are still in operation. The two recording technologies do not always behave in the same way; some of the advice given below is therefore specific to neither one nor the other.

Placement

> Regulation
>
> Private and Family life should not be exposed by CCTV systems in the public domain.
>
> *Source: The Human Rights Act 1998*

Cameras may be static (permanently sited) or mobile (may be moved from one location to another, or may be vehicle mounted). Cameras may be digital or analogue and may be hardwired, networked or wireless networked.

On street, it is often advisable to have at least two cameras for each location: one of these will provide the context and the other will provide close up information and identification. Together these provide the evidence necessary for a prosecution.

On buses, cameras should be positioned such that they provide the information they need. For instance, if a camera will be used by the driver to ensure all passengers are clear of the rear door, then a camera needs to be positioned such that a clear view of the rear door is afforded.

Although a camera need not be visible, the First Data Protection Principle dictates that a sign should be mounted in clear sight indicating that CCTV recording is taking place.

Cameras should be positioned to avoid accessibility by vandals as far as possible. The camera should have a protective housing to protect the camera from the damp, heat, light and physical damage.

Do:	position cameras so they monitor only intended areas
	consult owners of other properties if your cameras will cover properties which are not your own.
	screen out electronically all private areas owned by third parties in the case of systems used at Stations and Depots. Adequate screen may not be possible on vehicles, but will be used to reduce intrusion as much as possible.
	consider changes in light according to time of day and season when placing a camera, to avoid glare and silhouetting
	consider how you will get power to the camera and data from the camera when placing it
	place CCTV cameras to create the required field of view
	place CCTV cameras specifically on problem services and in problem shelters to identify perpetrators of vandalism
	locate cameras in stations or services which are not easily supervised by staff or are a target for offences
	have two cameras for each street location, a wide angle camera for context and a close up camera for identification
	avoid reflections from safety screens etc
	review camera locations annually and move them in response to changing crime problems

Do not:	position cameras such that they intrude into the private, domestic or family life
	position cameras where they may be inadvertently knocked by passengers or pedestrians
	position cameras where they are easily accessible to vandals
	position cameras where their line of sight may be obstructed by seasonal foliage growth

	mount cameras where vibration, wind and structural bending may cause excessive picture movement

Image quality

It is critical to determine the purpose of the CCTV camera in order to ensure that the appropriate resolution is achieved. What will the observer of the image need to see? Generally, the more detail obtained in the image, the smaller the area covered by the camera. Therefore, if it is necessary to be able to see a license plate or identify a person, some of the context around the license plate or person will be lost.

The requirements for each of the different categories of observer task – monitoring and control, detection, recognition, or identification – have been standardised by the Home Office using the Rotakin® system (see Annex C).

Do:	ensure that the resolution of the image produced is adequate for the use to which the image will be put
	ensure that the observer can resolve the image in sufficient detail for both live monitoring and recorded review
	ensure that “reasonable” system checks are made in line with the recommendations laid down in the Data Protection Act 1998 to ensure that equipment is maintained, cleaned and performing correctly
	keep a record of any servicing from the date of purchase
	view recorded pictures or printouts, not the live screen, to assess system performance

Do not:	reduce picture quality to fit the available storage capacity of the system; it is better to have a little useful imagery than lots of useless imagery

Lighting

Cameras should be placed in a position which will provide adequate light for good picture quality and contrast. There should be plenty of light and as few shadows as possible. Night-time recordings require either sufficient lighting to enable a visible light camera to capture clear images, or cameras with infrared capabilities.

Do:	ensure lighting is adequate for a clear image as far as possible
	Avoid placing cameras where backlighting and glare will compromise the quality of the image.
	design lighting in shelters and stations to minimise shadows which would affect the quality of a CCTV image
Do:	use cameras capable of night vision and backlight correction where surveillance will occur 24 hours a day and sufficient lighting has not been installed
	add a lens hood to the camera where strong light on the lens may be a problem

Do not:	place cameras such that strong direct light falls on the lens, causing flare and loss of detail
	expect cameras which operate in very low light levels to compensate for poor lighting

Camera control

Some cameras show a fixed field of view; others can be controlled, for example using Pan-Tilt-Zoom (PTZ) controls. The recording process may also be controlled.

Recording may in some circumstances benefit from automatic triggers. For example, TfL's bus lane enforcement cameras are triggered to record only when the vehicle is in an enforcement zone. Driver safety cameras may be triggered by the panic button, so that the driver initiates recording if he is threatened or attacked. This cuts down significantly on storage requirements, but risks missing incidents while the camera is off.

No camera should rely on the bus driver to operate or control in any way which may act as a distraction while driving.

Where cameras are manned by an operator, the operator should only give evidence on the process of how the CCTV data was gathered and appropriate logs and audit trail

Do:	consider whether PTZ control is required, and if so who will control the camera
	ensure that where cameras are connected to a monitoring station, there is a secure link
	ensure help points at shelters or stations have CCTV which is automatically activated when the help button is pressed.

Recording

Images may be transmitted over wireless or wired networks to a recording medium. Wired networks use coaxial cable, Cat 5 cable or optical fibre. They are relatively cheap, are largely unaffected by the environment and permit large amounts of data to be transmitted. Wireless cameras can be beneficial where the use of wires is not practical. These often operate on the 2.4GHz frequency band which is used by numerous other systems, making the likelihood of interference high. This may also mean that data is less secure or may become corrupted.

As CCTV moves towards fully digital systems, cameras communicating via the Internet Protocol (IP) are expected to become increasingly popular. It allows information to be transmitted across a data network and can be wired or wireless as necessary or practical.

Video contains a large amount of information and storage, particularly for extended use systems, can be expensive. There is often, therefore, a trade-off to be made between image quality, frame rate and length of recording between media reuse. The actual quality selected will depend on the purpose of the recording:

- Digital recording systems store video on a hard drive like that found in a standard computer. The hard drive has a finite storage capacity and so a digital

CCTV system can only retain video on the system for a finite time before it is overwritten. If an incident occurs, it therefore needs to be copied to a permanent storage medium such as a DVD.

- For recognition of individuals within a relatively slow-moving context, the minimum frame rate (image rate if digital) should be no less than of one frame per 2 seconds. For after-the-fact analysis of an incident the frame rate should be much higher: around 5 frames per second.
- For immediate use within a managed environment – e.g. where on-bus recordings are reviewed at the end of a working run and the operator takes a decision on whether the recording contains any useful content – an overwrite interval of 5-7 days may be acceptable. For police use, where it may take an investigating officer some while to establish that a particular recording is of evidential value, the overwrite time should be much longer – ideally at least a month.
- Bear in mind that you should not compromise image quality to try to fit more data onto a hard drive. The more data is compressed, the poorer the image quality will be.

To be usable as evidence, the imagery needs not only to be good quality but tied closely to the real world. Location is likely to be established adequately by the visuals, but it is also important to know the date and time the recording was made. Each frame, therefore, needs to be "timestamped" with an accurate recording time at the point the recording is made.

Do:	ensure recording equipment is kept clean, dry and secure
	ensure that the frame rate is adequate for the purpose of the system
	ensure that the recording capacity is adequate for the purpose of the system
	ensure that the recording facility is rated for use in its operating environment – temperature, vibration etc
	keep a record of the make, model, format and reference of any equipment used as part of the Audit Trail
	ensure a record is kept of the camera location and number and the vehicle's fleet number.
	ensure that the camera records accurate current time on each frame
	synchronise the camera clock to a suitable reference source (e.g. Rugby), taking into account summer time changes

	ensure that the internal camera clock is accurate within +/-10 seconds over a 14 day period and is re-synchronised at least once in that period

Analogue

With analogue systems the main factors affecting the recording quality are physical or magnetic damage to the tape. Tape has a finite lifetime: it cannot be indefinitely reused.

Do:	ensure that the recording head is kept clean to avoid damaging video tape
	allow video tapes and recording equipment to reach local ambient temperature before use to prevent condensation damage
	test tapes before use to ensure that they are still capable of taking a high quality recording
	keep a record of the number of times which a tape is used – it will probably be necessary to destroy the tape after 10-12 uses
	Degauss the video tape before reusing or destroying

Digital

Digital recording generally suffers less from physical problems but has other challenges.

Do:	ensure that hard drives are tested regularly
	encrypt digital images which are transmitted from the roadside to a central facility where possible

Do not:	allow electronic access controls, passwords or encryption devices to prevent access by authorised personnel

Retrieval, replay and export mechanisms

Where recordings are to be used for evidence, a master recording needs to be retained and carefully controlled. This impacts both analogue and digital systems – though differently.

Regulation

The investigator must retain material obtained in a criminal investigation which may be relevant to the investigation.

All material which may be relevant to an investigation must be retained until a decision is taken whether to institute proceedings against a person for an offence.

If a criminal investigation results in proceedings being instituted, all material which may be relevant must be retained at least until the accused is acquitted or convicted or the prosecutor decides not to proceed with the case.

Source: The Criminal Procedure and Investigations Act 1996 Code of Practice (5.1, 5.7, and 5.8)

Regulation

The constable may require any information which is contained in a computer and is accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible if he has reasonable grounds for believing it is evidence in relation to an offence which he is investigating or any other offence.

Source: Police and Criminal Evidence Act 1984

Do:	ensure that for any recording (digital or analogue) a master or evidence copy is kept for reference; this should be stored securely, with access controlled
	ensure that for any recording, a working copy is available from which stills and sections of video can be made by investigators
	ensure the time and date associated with each picture is legible
	ensure a system operator is always available at short notice to replay and export recordings
	ensure that a simple system operator's manual is available locally to assist with replay and export
	ensure that system operators know the retention period of the system and export time for various amounts of data

Analogue

Tape is very delicate and can easily be damaged by improper handling, storage or replay.

Some analogue CCTV recording systems are capable of simultaneous twin recordings. One of these will be the evidence tape must be kept, secure and unedited for use by the police, if necessary. A working tape is used from which an operator can work or stills can be made. If the system is not capable of simultaneous twin recordings, a copy of the first recording should be made and the original sealed for use as the evidence tape.

Do:	Avoid replaying original video recordings except (i) to make a copy (ii) in the context of a court when suitably instructed

Digital

Digital recordings suffer much less from degradation. They are also much less bound to their medium. A recording file can be copied, bit for bit, to a backup file so that a working copy is always available. Nevertheless, using digital CCTV represents a significant issue in the retrieval, replay and export of those images as evidence.

It is always preferable to extract video data in the native format to avoid reduction in picture quality and maintain the evidential integrity of the data. Methods that involve format conversion, such as scan conversion or recording to videotape, should only be used if there is no method available to transfer the data in its native format.

There may be instances where the police require not just the recording of an incident, but the hard drive itself because of a major crime or terrorist incident. Generally this will happen because the volume of data is so large that it is the only practical method available or there are no export options. Because of this possibility, CCTV systems should have removable – and spare – hard drives to take the place of any which are currently in police possession. It must be stressed that this is the exception and not the rule, and that in most instances bit for bit cloned copies of the CCTV data can be exported to another medium such as a CD or DVD.

Do:	Give the police both the master/primary evidence and working copy along with any stills if the CCTV data is in relation to a crime.
	ensure that the CCTV system has a suitable export facility: connector socket (e.g. USB), network port or removable hard drive, DVD writer.
	make provision for a stock of say 10% of spare removable hard drives
	transfer images recorded onto a hard drive or any reusable recording medium onto a “write once read many” (WORM) recordable medium. This should happen as early as practical in the recording chain, so as to simplify the audit chain management
	if file compression is used to store data, ensure that the algorithm is appropriate for the reconstruction of data for replay. Test the quality of playback video under different conditions of lighting etc
	ensure that the system is able to quickly export video and stills to a removable storage-medium, including timestamps
	export video in the native file format wherever possible and at the same quality that they were stored on the system

To simplify and speed the use by investigators of the recorded video, it is highly desirable that any digital camera system comes with playback software which provides some specific functions.

Do:	ensure that the manufacturer provides any software required to view or replay the exported pictures
	ensure that files can be replayed immediately once exported to removable media
	ensure playback software: • has variable speed control including frame by frame, forward and reverse viewing; • displays a single camera at full resolution; • enables the synchronised display of single and multiple cameras and maintains the aspect ratio; • permits the recording from each camera to be searched by time and date; • allows printing and/or saving of pictures in faithful format (e.g. bitmap) including time and date.

3. General security systems – operations

Introduction

The operational aspects of any CCTV system will be crucial to its success and to its usefulness to the Police in any prosecutions that result. The CCTV operator who sits in the office watching the output of the CCTV camera will add the necessary human element which will ultimately decide whether a transgression has taken place. Therefore it is vital that secure, robust and consistent operational practices are in place. This section details both the recommended and required operational practices for a successful CCTV system.

CCTV recordings will have greater evidential weight if it can be shown that a robust Audit Trail has been maintained throughout their life, from event to court room. This includes ensuring that appropriate logs are kept, indicating who has had access to recordings and when. In the event that a recording is used as evidence, it can help show that the security of the data has not been compromised.

Operators have a duty under the Data Protection Act 1998 to ensure that the data which they hold is accurate, relevant, and not excessive. The Information Commissioner's Office has written a Data Protection Manual which provides checklists for those who hold data to evaluate whether they are compliant with Data Protection Act requirements. Wherever possible, regular self-evaluation for compliance should be undertaken to show that internal procedures are well-defined, robust and regularly reviewed.

Finally, unless the equipment used to capture and process the images is working properly there can be no confidence in the recordings which are extracted from it. As part of the operation of the system a routine maintenance programme should be in place. This will include regular cleaning/clearing, repair and replacement, and ensuring that the date and time is accurate.

Regulation
The Public has a right of access to data including video images.

Source: The Data Protection Act 1998

Regulation

Private and Family life should not be exposed by CCTV systems in the public domain.

Source: The Human Rights Act 1998

Regulation

Where public CCTV is used, any directed surveillance must be authorised.

Source: The Regulation of Investigatory Powers Act 2000

Do:	register your CCTV operation with the Office of the Data Protection Commissioner detailing the exact nature of the use of the CCTV camera systems. Ensure that any audio recording systems in place are also detailed.
	ensure that Operational Manuals are available to all staff involved in CCTV operations, and that appropriate training is conducted
	carry out regular self-audits and self-assessments to ensure that procedures are robust and well-defined
	keep logs detailing who has had access to CCTV footage and when; more than one log may be necessary
	display camera enforcements signs in areas where a system operates including references to any audio recording systems
	Carry out regular safety checks of the system and its operators

Retention and storage

Regulation

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Source: Data Protection Act 1998, Schedule I, Part I

Regulation

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Source: Data Protection Act 1998 Schedule 1, Part 1

All video recordings (working and evidence) remain the property of the data controller which made the recording. It is his responsibility to ensure that they are suitably managed in accordance with both data protection legislation, and the legitimate requirements of the criminal justice system.

Do:	keep a catalogue of stored recordings (working and evidence) for accessibility
	keep all recordings (working and evidence) made during a monitoring period in secure storage and in an unaltered state until destruction
	give each video recording an individual reference number for unique identification regardless of format
	keep an audit log of the movement and viewing of all working and evidence video recordings. The log begins when the monitoring period begins and ends when the media is released from secure storage to be degaussed or destroyed
	keep all recordings (working and evidence) for a period of at least a month regardless of whether there are any contraventions on the tape
	control access to the system and recorded images to prevent tampering and unauthorised viewing
	keep a record of who accessed the system and when
	ensure that the system is capable of securing relevant pictures for review or export at a later date

Do not:	remove an evidence recording from storage unless it is required for adjudication evidence or it is no longer required for evidential purposes

	remove a working recording from storage unless it is required to: • generate stills or on screen prints or photographs • view by authorised personnel or staff when considering representations or appeals • for viewing under strictly controlled conditions. • for copying or release to third parties • for monitoring purposes to obtain statistics on the performance of the scheme • for additional monitoring purposes
	prevent authorised access (e.g. by police or CSI) with electronic access controls using proprietary software or hardware

Analogue

As with operation, analogue tape storage is principally constrained by the need to prevent physical or magnetic damage to the tapes.

Do:	store video tapes short-term (3 months or under) vertically, in their cases, in a constant environment which will not suffer from extremes and away from any electric or magnetic field. This will normally mean: • dust-free • maintained between 15°C and 24°C • maintained at a relative humidity of 35% - 55%
	remember that long-term storage of video tapes can compromise the quality of images – there is no clear guidance available on lifetime
	store tapes on or in steel furniture with steel shelving which is fire resistant
	cut small holes if polythene bags if these are used for storage, e.g. of evidence videos, to prevent condensation damage
	ensure that tapes are rewound before they are stored
	ensure that all tapes are degaussed before reuse or disposal
	ensure that the evidential video is stored with the record protect device activated to avoid accidental erasure.

Do not:	reuse a tape until all contraventions recorded on it have been fully and finally settled

	reuse tapes containing classified or important information (e.g. tapes which have recorded video of a serious crime)
	degauss a tape more than 12 times
	release a working video for reuse until all contraventions on it have been fully and finally settled
	store video tapes in airtight containers because of the risk of condensation damage
	store tapes in direct sunlight
	store paper in video cassette boxes: paper dust is abrasive and may damage the tape
	store video tapes in the recorder

Digital

Digital evidence can be fragile is different ways. It can be altered, damaged or destroyed by improper handling or storage. Therefore special precautions must be in place to collect, document and preserve this type of evidence.

See also the Code of Practice of Legal Admissibility of Information Stored Electronically (BIP 0008-1:2004), available from BSI.

Do:	store digital recordings in a away from sunlight and heat sources
	ensure that special sequences or individual pictures can be protected to prevent overwriting before they can be viewed in an investigation
	store digital material away from magnetic sources
	store digital material away from extremes of humidity
	store discs in individual cases
	ensure that discs are labelled on the upper side of the disc only and not on the data side
	store hard drives in individual boxes with foam inserts
	securely delete or physically destroy (e.g. shred) digital images once they are no longer required

Do not:	Convert digital CCTV data back to analogue as this causes deterioration of the data and can also lead to data corruption.

Control room security

Access to the control room should be strictly controlled with regard to British Standard (BS7499). It should be both secure and lockable. All monitoring, recording and control equipment should be located in this room and any working or evidence tapes and other relevant records must be kept in secure locked cabinets either in this room or similar secure environment. The control room must never be left unattended and unlocked for any period, however short.

Do:	ensure that the control room Operating Procedure is well documented in a user manual which is accessible to all operators
	design and operate the control room in accordance with the technical requirements for analogue/digital recordings and retrieval above
	keep all recordings in a secure location for seven years, where applicable in criminal cases
Do:	release copies of sections of working video recordings only to legitimate enforcement and investigative authorities
	keep a detailed record of the release of any recording including the information to whom it was released and the reason for release
	provide the police with a statement verifying the integrity of the recording upon release
	ensure that all monitoring operations take place in a secure and lockable room
	permit visitors access to the Control Room only when authorised by the named Senior Officer
	Adhere to the recommendations laid down with regard to British Standard (BS) 7499

Do not:	release working video recordings without proof of identity and authority
	release any recordings to members of the public, notwithstanding the Freedom of Information Act and the Data Protection Act.

Staff

Regulation

Category of licensable activity [under the Private Security Industry Act 2001] …involves the use of CCTV equipment to monitor the monitor the activities of a member of the public in a public or private place; or identify a particular person including the use of CCTV in these cases to record images that are viewed on non-CCTV equipment, for purposes other than identifying a trespasser and protecting property

Source: The Private Security Industry (Licences) (Amendment) (No. 2) Regulations 2005

The Private Security Industry Act 2001 requires contracted operatives involved in public space surveillance to be licensed under the Security Industry Authority (SIA). Licensing must be preceded by training at an accredited CCTV training course (see Annex D). All applications are submitted to a Criminal Record Bureau (CRB) check to ensure that the person is both qualified and fit to hold the SIA license. The license is issued in the form of a wearable, credit card sized badge.

Employers may also find it prudent to undertake relevant staff checks as laid down in British Standard (BS) 7858.

It is essential that when recruiting operators for CCTV operation and monitoring that those tasks which will fall to the operator are analysed and well understood. HOSDB research has indicated that operators need to show a range of competencies to undertake CCTV monitoring. These include: good interpersonal skills, good stress tolerance, good self control, excellent manual dexterity, and an excellent ability to apply specialist knowledge (including current legislation, operational procedures and systems, knowledge of the area covered by the cameras, and police systems and procedures).

Do:	ensure staff are properly trained and qualified in the use of CCTV
	ensure that a senior officer has responsibility for access to the Control Room and for the release of video tapes and still images.
	ensure that staff who are to monitor CCTV have undergone a sight test since it is a visually demanding job
	ensure that system operators know the retention period of the system and export time for various amounts of data

	ensure that a Code of Practice and a Control Room Procedures Manual are made available to staff who will be monitoring CCTV cameras
	ensure that all staff employed for the monitoring of CCTV cameras are made aware of their obligation to work to the rules of confidentiality
	ensure that all staff who undertake enforcement of traffic regulations using CCTV has successfully completed an approved CCTV training course
	ensure that details pertaining to British Standard (BS) 7858 are considered

Audit log

An audit log must be kept to track the movement of all evidential media. In all cases the audit log must begin when monitoring begins and ends when the evidential recording is released from secure storage to be degaussed, deleted or destroyed. A detailed record must be kept of any recording which is released. This should include the reason for release.

A recording should only be released to an authorised representative from

- the parking and traffic appeals service (copies to the appellant)
- the Police
- lawyers acting on the behalf of appellants
- lawyers acting on the behalf of defendants or victims
- third party prosecuting authority such as HM Customs and Revenue or the Health and Safety Executive
- this may also apply to Data Subject Access requests

Proof of identity and a signature must be required before release.

Do remember that the Audit Log or Logs may form part of the evidence which is submitted and its consistency, accuracy and clarity will add weight to any video evidence which is submitted. The Audit Log should be kept safe and secure and should only be completed by those authorised to do so.

4. Bus lane enforcement: a special case

Introduction

In addition to the general provisions discussed in section 2, there are additional requirements that must be adopted in specific circumstances. One particular context is the use of CCTV for bus lane enforcement.

Originally limited to London, bus lane enforcement is (subject to Government approval) now available to all English local authorities, under Statutory Instrument 2005 no 2757, The Bus Lane Contraventions (Penalty Charges, Adjudication and Enforcement) (England) Regulations 2005. CCTV may be used subject to SI2005 no 2756, The Bus Lanes (Approved Devices) (England) Order 2005.

Transport for London and the London Boroughs have been using CCTV cameras to enforce traffic regulations since 1999. CCTV is monitored by a trained operator keeps a contemporaneous record of any contraventions witnessed during the CCTV recording. If, on review, the contravention is deemed to be clear and indisputable, the registered keeper of the vehicle and the circumstances of the contravention are noted. A Penalty Charge Notice (PCN) is then sent to the keeper of the vehicle within 14 days of the contravention.

Note that the requirements and guidance presented in this section is in addition to Section 2, which should still be followed even if the only CCTV application used is traffic enforcement.

Placement

> Regulation (extract)
>
> 2.(c) The equipment includes a camera which is capable of producing (i) a close-up legible image of the registration plate of any vehicle in the bus lane or, as the case may be, the selected area; and (ii) a wider angle image of the carriageway such as will enable information to be provided about any

circumstances which may have caused the vehicle to be in the bus lane or the selected area.

Source: Statutory Instrument 2005 No. 2756 – The Bus Lanes (Approved Devices) (England) Order 2005

Placement of enforcement cameras is worth considering carefully. During the passage of the Road Traffic Act 1991 considerable debate surrounded the positioning of traffic enforcement cameras. At the time, it was advised that cameras be placed to capture the rear view of the offending vehicle, in part to allay the public perception that these cameras would be used for surveillance of the individual.

However, since then it has become evident that although the offending vehicle has been identified, the offending individual has not. Therefore, it may be preferable to have two cameras which provide both a rear and a frontal view (Code of Practice for Operational Use of Enforcement Equipment – ACPO, 2004).

For enforcement use, cameras must be paired, in such a way as to ensure that both contextual and identifying video is shot.

Many situations will need a combination of permanent and temporary cameras. Permanent cameras are best for situations where repeated offences are likely to occur such as bus lanes, junctions or a congestion charge zone. A temporary or mobile camera may be best if it needs to respond to changing crime patterns or if the area which the camera will need to cover is large. It may also be more cost effective to use mobile CCTV units to cover a variety of ad hoc situations, than to have multiple fixed cameras in multiple locations.

Image quality

Regulation (extract)

3. The equipment includes a recording system in which…

(b) recordings are made at a minimum rate of 5 frames per second.

(c) each frame is timed (in hours, minutes and seconds), dated and sequentially numbered automatically…;

(d) the location of the bus lane or selected area being surveyed is shown;

Source: Statutory Instrument 2005 No. 2756 – The Bus Lanes (Approved Devices) (England) Order 2005

Slow scan video is not acceptable for bus lane enforcement.

Camera control

Regulation (extract)

3. (e) Where any part of the equipment is controlled manually, two simultaneous recordings [must be] made of the camera output viewed by the operator.

Source: Statutory Instrument 2005 No. 2756 – The Bus Lanes (Approved Devices) (England) Order 2005

There are specific provisions for recording manually-controlled cameras.

Where cameras are manned by an operator for the purpose of confirming data for road traffic violations, the operator is the primary witness of any infraction and the video recording is the record of what the operator witnesses. Appropriate logs should be kept of infractions witnessed, and witness statements produced.

Recording

Regulation (extract)

2.(d) [The camera must be] connected by secure data links to a recording system.

4. The equipment is [must be] (a) synchronised with the "Rugby" atomic clock or another independent national standard clock; and (b) accurate within plus or minus 10 seconds over a 14-day period and [be] re-synchronised at least once during that period.

6. Where the equipment includes a facility for simultaneous voice-over recording, it incorporates a time mark from the clock

with which the recording system is synchronised, denoting contemporaneous recording with the vision track.

Source: Statutory Instrument 2005 No. 2756 – The Bus Lanes (Approved Devices) (England) Order 2005

Analogue CCTV recording systems should be capable of simultaneous twin recordings. A digital CCTV recording will be made to a hard drive from which an evidence copy and a working copy can be made. A working tape is needed from which an operator can work or stills can be made. An evidence tape must be kept, secure and unedited for use by the police, if necessary.

Monitoring

Regulation (extract)

5. Where the equipment includes a facility to print a still image—

(a) of any frame recorded on the videotape; or

(b) from a digital record,

any printed image is endorsed with the time and date when the frame was captured and its unique number.

6. Where the equipment includes a facility for simultaneous voice-over recording, it incorporates a time mark from the clock with which the recording system is synchronised, denoting contemporaneous recording with the vision track.

Source: Statutory Instrument 2005 No. 2756 – The Bus Lanes (Approved Devices) (England) Order 2005

Contraventions of traffic regulations must be identified in real time and at the time when they are committed. No pre-recorded video images may be studied to identify contraventions committed at a previous time. The operator's view of the traffic contravention is the primary evidence that a traffic contravention occurred (Code of Practice for Operation of CCTV Enforcement Cameras, 2006).

The operator must identify the time and sufficient vehicle identification information at the time of the contravention using a logbook or approved audio voice-over equipment. The working copy of the video is the physical copy of the operator's view. The operator will then be able to return to the working video at a later date to produce still images which can be used to issue Penalty Charge Notices (PCNs).

The enforcement log

Operators are required to keep logs of incidents as they see them in real time. this log should contain information on:

- date and time;
- operator, camera ID, date, etc;
- the incident and vehicles involved: location, VRN(s), vehicle description – make/model/colour, actions witnessed, etc

A separate Control Room Log should also be kept which records the monitoring that has been undertaken: date, camera operator, camera ID, location, start and finish time, equipment problems, etc. This Log should be signed by the Control Room Supervisor.

Where a contravention has been observed, the authorised officer will be required to make a witness statement which declares that at the time that the contravention was observed the equipment was approved by the Secretary for State and was in full working order. Reference should be made to the Control Room Log. The Statement should also enumerate what evidence (e.g. stills) is being produced in support of this statement and under what circumstances the evidence was produce (e.g. what camera). See Code of Practice for Operation of CCTV Enforcement Cameras in London Boroughs (Template, ALG 2006) for sample witness statements.

Still images

Someone who has received a PCN is entitled to view the section of video recording the contravention. Still images are often supplied with the Penalty Charge Notice (PCN) as an alternative to viewing the video evidence. A still image is a single frame of a video recording printed onto paper. This single image then becomes the property of the recipient. Still images should only be supplied at the discretion of the Senior Officer.

Glossary of terms and acronyms

ACPO – Association of Chief Police Officers

BSI – British Standards Institution

Cat 5 – Category 5 cabling standard – up to 100Mbit/s

CCD – Charge-coupled device – electronic component for capturing digital imagery

CCIR – Comité Consultatif International de Radio – now part of the International Telecommunications Union, the global telecoms standards organisation

CCTV – Closed Circuit Television

GHz – Gigahertz (measure of frequency)

HOSDB – Home Offices Scientific Development Branch

IP – Internet Protocol (communications standard)

JPEG – Joint Pictures Expert Group (digital still image standard, involving compression)

MPEG – Motion Pictures Expert Group (digital video standard, involving compression)

PCN – Penalty Charge Notice

Rotakin – HOSDB standard test for CCTV technology

RTIG – Real Time Information Group

SIA – Security Industry Association

SIO – Senior Investigating Officer a Term normally given to the police officer in overall charge of an investigation

TfL – Transport for London

VRN – Vehicle Registration Number

WORM – Write Once Read Many (characteristic of storage device)

Further reading

Sources with legal force

Bus Lanes (Approved Devices) (England) Order 2005: Statutory Instrument 2005 number 2756. Available at: ***http://www.tiresias.org/*** ***http://www.opsi.gov.uk/si/si2005/20052756.htm***

Bus Lane Contraventions (Penalty Charges, Adjudication and Enforcement) (England) Regulations 2005: Statutory Instrument 2005 number 2757. Available at: ***http://www.tiresias.org/*** ***http://www.opsi.gov.uk/si/si2005/20052757.htm***

Criminal Procedure and Investigations Act 1996 Code of Practice. Available at: ***http://www.tiresias.org/*** ***http://www.tsoshop.co.uk/bookstore.asp?FO=1159966&Action=Book&ProductID=0113413033***

Data Protection Act 1998. Available at: ***http://www.tiresias.org/*** ***http://www.opsi.gov.uk/acts/acts1998/19980029.htm***

Data Protection Act 1998 Code of Practice (2000). Available at: ***http://www.tiresias.org/*** ***http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/cctv_code_of_practice.pdf***

Freedom of Information Act 2000. Available at: ***http://www.tiresias.org/*** ***http://www.opsi.gov.uk/acts/acts2000/20000036.htm***

Health and Safety at Work etc Act 1974. Available at: ***http://www.tiresias.org/*** ***http://www.healthandsafety.co.uk/haswa.htm***

Human Rights Act 1998. Available at: ***http://www.tiresias.org/*** ***http://www.opsi.gov.uk/acts/acts1998/19980042.htm***

Code of Practice of Legal Admissibility of Information Stored Electronically (BIP 0008-1:2004, 2:2005, 3:2005). May be ordered from BSI: ***http://www.tiresias.org/*** ***http://www.bsi-global.com/ICT/Legal/bip0008.xalter***

London Local Authorities Act 1996. Available at: ***http://www.tiresias.org/***
http://www.opsi.gov.uk/acts/locact96/Ukla_19960009_en_1.htm

London Local Authorities Act 2000. Available at: ***http://www.tiresias.org/***
http://www.opsi.gov.uk/acts/locact00/20000007.htm

Police and Criminal Evidence Act 1984. May be ordered from The Stationary Office ***http://www.tiresias.org/*** *:* ***http://www.tiresias.org/***
http://www.tsoshop.co.uk/bookstore.asp?FO=1159966&Action=Book&ProductID=0105460842

Private Security Industry Act 2001
http://www.opsi.gov.uk/acts/acts2001/20010012.htm

The Private Security Industry (Licences) Regulations 2004 (Statutory Instrument 2004 No. 255) ***http://www.opsi.gov.uk/si/si2004/20040255.htm***

The Private Security Industry (Licences) (Amendment) (No. 2) Regulations 2005 (Statutory Instrument 2005 No. 2118)
http://www.opsi.gov.uk/si/si2005/20052118.htm

Railways and Transport Safety Act 2003. Available at: ***http://www.tiresias.org/***
http://www.opsi.gov.uk/acts/acts2003/20030020.htm

Regulation of Investigatory Powers Act 2000. Available at: ***http://www.tiresias.org/***
http://www.opsi.gov.uk/acts/acts2000/20000023.htm

Road Traffic Regulation Act 1984. May be ordered from The Stationary Office ***http://www.tiresias.org/*** *:* ***http://www.tiresias.org/***
http://www.tsoshop.co.uk/bookstore.asp?FO=1159966&Action=Book&ProductID=0105427845

Road Traffic Act 1991. Available at: ***http://www.tiresias.org/***
http://www.opsi.gov.uk/acts/acts1991/Ukpga_19910040_en_1.htm

Statutory Instrument 2001 No 690: Transport for London (Bus Lanes) Order 2001. Available at:http://www.tiresias.org/
http://www.opsi.gov.uk/si/si2001/20010690.htm

BS 8418 Installation and remote monitoring of detector activator CCTV systems – Code of Practice

BS 10008 Evidential Weight and legal admissibility of electronic information – Specification (2008)

Guideline sources

UK Police Requirements for Digital CCTV Systems (Home Office Scientific Development Branch, 2005)

Neil Cohen, Simon Walker, Ken MacLennan-Brown, Retrieval of Video Evidence and Production of Working copies from Digital CCTV Systems (Home Office Scientific Development Branch, 2006).

Neil Cohen, J Gattuso, Ken MacLennan-Brown, CCTV Operation Requirements Manual (Home Office Scientific Development Branch, Publication Number 55/06, 2006)

Code of Practice for Operational Use of Enforcement Equipment (ACPO, 2004)

Digital Imaging Procedure, (Police Scientific Development Branch, 2002)

Diffley C and Wallis E, CCTV: Making it Work, Recruitment and Selection of CCTV Operators (Police Scientific Development Branch, 1998)

Neil, DC, Mather P and Brown EC, Guidelines for Handling Video Tape (Police Scientific Development Branch, publication no. 21/98 ,1999)

Get on Board: an Agenda for Improving Personal Security – Guidance (Department for Transport, April 2002)

Good Practice Guide for Computer Based Electronic Evidence (ACPO)

Skelton, Neal and Raymond Webb Protocol for the handling of digital images on public transport vehicles

CCTV Code of Practice (Information Commissioner's Office, 2000)

Data Protection Audit Manual (Information Commissioner's Office, 2001)

Code of Practice for Operation of CCTV Enforcement Cameras in London Boroughs (Template, ALG 2006)

Webb, Raymond (Metropolitan Police) and Neal Skelton (Police Scientific Development Branch). Protocol for the handling of digital images on public transport vehicles (Private Communication)

Useful websites

www.the-sia.org.uk Website of the Security Industry Authority

www.sito.co.uk Website of the Security Industry Training Organisation

http://www.cctvusergroup.com/ Website of the CCTV User Group

http://www.cctvimage.com/ Official publication of the CCTV User Group

http://www.informationcommissioner.gov.uk/ Website of the Information Commissioner's office – dealing with organisations that hold information

http://www.informationcommissioner.gov.uk/cms/DocumentUploads/cctvcop1.pdf Link to the Information Commissioner's Office CCTV code of practice

http://www.homeoffice.gov.uk Website of the Home Office

http://www.crimereduction.gov.uk/cctvminisite4.htm Website of the Home Office CCTV initiative

http://www.hmso.gov.uk/ Main HMSO website link to publications

http://www.hmso.gov.uk/acts/acts1998/19980029.htm HMSO website link to the Data Protection Act 1998

http://www.hmso.gov.uk/acts/acts2000/200000369.htm HMSO website link to the Freedom of Information Act 2000

http://www.hse.gov.uk Website of the Health and Safety Executive

http://www.dca.gov.uk/hract/hramenu.htm Department of Constitutional Affairs

http://www.yourrights.org.uk/your-rights/chapters/privace/other-types-of-surveillance/cctv.shtml Liberty's website - Details of the Human rights Acts and Privacy issues

Extract from HOSDB guidance

Prosecution requires clear, accurate and high quality surveillance images, which monitor, detect, recognise and identify any intruder or criminal activity. To assist developers, the Home Office Scientific Development Branch (HOSDB) developed the Rotakin® system to test and measure the image quality of analogue CCTV systems. The Rotakin® system and is now a recommendation of the British and European standard BS EN 50132-7:1996.

These guidelines are related to the image height of a standing man defined using the Rotakin® standard test target 1.6 metres high. When the image of Rotakin® fills the screen vertically the image height is said to be 100%R.

The figures are based on a 625 line CCIR standard system and assume all equipment is correctly adjusted and operated within its design range.

There are at present no comparable set of video standards for digital systems, where the problems of picture quality are quite different. Developing digital system guidance is currently the subject of work within HOSDB.

Observer Task	**Definition**	**Rotakin® Value**	**Notes**
Monitor and Control	An observer can determine the number, direction and speed of movement of people whose presence is known to him	Not less than 5%R	Assuming that the image contrast of the target is sufficiently above the threshold of human sensitivity and that the picture is not unduly cluttered with non targets
Detection	Following an alert an observer can, after a search, ascertain with a high degree of certainty whether or not a person is visible in the pictures displayed to him	Not less than 10%R	Assuming that the image contrast of the target is sufficiently above the threshold of human sensitivity and that the picture is not unduly cluttered with non targets

Observer Task	Definition	Rotakin® Value	Notes
Recognition	Viewers can say with a high degree of certainty whether or not the individual shown in the same as someone they have seen before	Not less than 50%R	Assuming that the angle of view and lighting is suitable and no significant degrading effects such as image blur due to motion or out of focus are evident
Identification	Picture quality and detail should be sufficient to enable the identity of a subject to be established beyond reasonable doubt	Not less that 120%R	Assuming that the angle of view and lighting is suitable and no significant degrading effects such as image blur due to motion or out of focus are evident
Reading a car licence plate		Saloon car not less than 50% picture height	Assuming that the angle of view and lighting is suitable and no significant degrading effects such as image blur due to motion or out of focus are evident

CCTV approved training courses

(as at Jan 2007)

Training Course	Training Provider	Date of Approval
Level 2 Certificate for CCTV Operatives (Public Space Surveillance) ASET Level 2- Operating CCTV for Public Space Surveillance	ASET www.aset.ac.uk	
Level 2 Award for CCTV Operators (Public Space Surveillance)	City and Guilds	
BTEC Level 2 Intermediate Award in CCTV Camera Enforcement	London Borough of Croydon, London Borough of Camden	December 2003
CCTV Traffic Enforcement BTEC Unit (Anyone taking this training course will have to have already successfully completed TAVCOM's CRO1 and CRO2 modules which provide them with control room operators training.)	TAVCOM	August 2004
Tavcom CRO8 – CCTV for Transport Analysts – BTEC Level 3 Award. This 3 day residential course covers best practice around the retrieval, production and despatch of on-vehicle CCTV images	TAVCOM	May 2005
Level 2 Award in CCTV Operations (Public Space Surveillance) NOCN Award in CCTV Operations (Public Space Surveillance) (Scotland)	NOCN	
VINCI Park CCTV Enforcement Training Programme	VINCI Park	January 2006

The future of CCTV

CCTV is a rapidly developing technology, particularly now that it can be achieved by digital cameras. Each component of the system is benefiting from continuous improvements and downward cost trends – image detectors, image compression algorithms, encryption software, storage solutions, communications (fixed and radio), image analysis, etc.

This makes it difficult to be definitive about what kind of system should be employed in the future: the economics of CCTV may have change dramatically. For instance, large hard discs are available but still expensive – hence the trade-off discussed in Section 2 between image quality, frame rate and overwrite interval. This is quite likely to be resolved as prices fall.

CCTV is also surrounded by legislation and regulation, and this may also change. Relatively small changes (for example, in where liability for security lies) could change the willingness of organisations to invest. Although we cannot foresee such changes, it is noteworthy that the subject of digital identity is a very hot topic at the moment, as are certain aspects of criminal justice procedure.

As technology improves, some new opportunities may arise which are not covered by these guidelines. For instance, it might become technically straightforward to record sound synchronously with CCTV video. (At present the bus environment is too noisy and acoustically complex.) Such recording would almost certainly require a number of independent microphones and some sophisticated filtering systems. For evidence purposes this would need to be tied tightly to the video. This is not yet covered by the existing secondary legislation.

Another potential change arises from the development of automated image analysis. Machine "intelligence" can already be set to detect, for example, abandoned objects or individual faces – though the systems are expensive and reliability is not yet consistent. Such automation clearly has the potential to improve dramatically the depth and coverage of security monitoring, without requiring armies of operators. This change would impact dramatically on operations in complex ways.

Finally, at present CCTV on vehicles (and some roadside CCTV) is recorded to disc, and then viewed later. This means there is no opportunity of contemporaneous monitoring and response. If it were economically feasible to communicate video out from the bus to a control centre, there would be much more opportunities to respond early to (or event forestall) security incidents. Again, the procedural change required would be substantial. TfL are understood to be considering this at the moment.

Future updates to these Guidelines will, of course, take into account relevant technical developments of this kind.