ASSOCIATION OF
CHIEF POLICE OFFICERS

NPIA
National Policing Improvement Agency
PRACTICE IMPROVEMENT

Practice Advice on

THE USE OF CCTV IN CRIMINAL INVESTIGATIONS

This has been published as an interim product due to the development of Authorised Professional Practice (APP) and may be published in an alternative format in the future as part of the APP programme.

2011

Produced on behalf of the Association of Chief Police Officers
by the National Policing Improvement Agency

This practice advice contains information to assist policing in the United Kingdom. **It is NOT PROTECTIVELY MARKED under the Government Protective Marking Scheme.**

This practice advice has been produced by the National Policing Improvement Agency (NPIA) on behalf of the Association of Chief Police Officers (ACPO). It will be updated according to legislative and policy changes and re-released as required.

The NPIA was established by the Police and Justice Act 2006. As part of its remit the NPIA is required to develop policing doctrine, including practice advice, in consultation with ACPO, the Home Office and the Police Service. Practice advice produced by the NPIA should be used by chief officers to shape police responses to ensure that the general public experience consistent levels of service. The implementation of all practice advice will require operational choices to be made at local level in order to achieve the appropriate police response.

(This publication is available as a PDF only.)

If you would like to receive this publication in an alternative format, please contact:

Specialist Operations Centre
Wyboston Lakes, Great North Road
Wyboston, Bedfordshire MK44 3BY

Telephone: 0845 000 5463
Email: soc@npia.pnn.police.uk

All other enquiries relating to this publication should also be addressed to the Specialist Operations Centre at the above address.

ASSOCIATION OF
CHIEF POLICE OFFICERS

NPIA
National Policing
Improvement Agency

PRACTICE
IMPROVEMENT

Practice Advice on
THE USE OF CCTV IN CRIMINAL INVESTIGATIONS

2011

Produced on behalf of the Association of Chief Police Officers by the National Policing Improvement Agency

First published 2011
National Policing Improvement Agency
Fry Building, Marsham Street
London SW1P 4DF

ACPO and the NPIA would like to express their thanks to all those involved in the drafting of this document. All of the responses during the consultation phase of this project were appreciated and contributed to the final document.

Contents

Introduction

Closed-circuit television (CCTV) can provide compelling evidence and investigators should consider it in every investigation. Although CCTV is primarily used for corroborating what is already known or suspected in volume crime incidents, it is a powerful tool for triggering further investigative opportunities. It can be used, for example, to show the nature and severity of offences and to identify suspects and witnesses, inconsistencies in accounts and forensic or scientific opportunities, such as the location of discarded property or vehicles, especially where it may seem that an investigation has come to a standstill.

Chief officers should demonstrate their leadership in this area by:

- Ensuring that investigators are provided with appropriate and up-to-date training and refresher courses in the basic processes of acquiring and preparing CCTV material from the numerous systems in use;
- Ensuring that basic, fit-for-purpose equipment and facilities are available to investigators for the timely viewing and copying or retrieval of CCTV material, including software that enables compatibility between the many and varied CCTV systems available;
- Establishing, implementing and overseeing policies to ensure that the use of CCTV (and its supervision) in investigations achieves its full potential.

The value of images cannot be overstated. They present evidence in a unique way, and allow those involved with the criminal justice system to visualise the crimes in question. When a case goes to court reinforced by good CCTV material, the prosecution is more likely to achieve a conviction.

In addition, CCTV can be a deterrent to potential offenders, can help to reassure the public, can assist public authorities to manage ongoing incidents, and helps to protect businesses, vulnerable premises and national facilities. It is also a useful tool when risk assessing scenes prior to the deployment of the emergency services.

This practice advice offers good practice to Professionalising Investigation Programme (PIP) Level 1 and 2 investigators in the use of CCTV as an investigative tool. It does not define roles and responsibilities, nor does it cover any specialist techniques. It provides the volume crime investigator with a comprehensive set of fundamental processes and procedures for acquiring useful and usable CCTV material. The same principles will apply in serious or major incidents, but processes and procedures will require appropriate scaling and resourcing, with responsibilities and functions being assigned to CCTV specific roles. This practice advice covers only the post-event use of CCTV materials and not real-time CCTV, often found in a police command and control environment. The covert use of CCTV is also outside the scope of this document.

Technical Terms

CCTV systems, ie, surveillance items comprising cameras and associated equipment for monitoring, recording, transmission and controlling purposes, for use in a defined zone, come in many different forms. The technology used is also continually changing. For the purposes of this document, a ground-level understanding of the fundamentals of CCTV systems is assumed. A brief definition of the most commonly used terminology is given below.

Analogue CCTV

Analogue CCTV is a method of recording video using a VHS tape.

Digital CCTV

Digital CCTV surveillance uses computer technology to digitise the CCTV camera images and compress them. CCTV can be stored on a PC-based system or a dedicated digital video recorder (DVR).

Hard Drive

The hard drive houses the hard disk where files are stored on a PC-based system.

Managed Systems

This is a network of cameras sited in public areas, usually managed by the local authority, shopping centres or larger organisations. CCTV from these managed systems is not always stored on site.

Network Video Recorders ('Hybrids')

A Network Video Recorder (NVR) or hybrid is a a digital video recorder that has either a VHS or DVD recorder attached to record its output. They use standard network cabling and management to transfer the digital image from the camera to the recorder. These are often used in large corporate environments, but can result in a poor-quality output.

Private Systems

These can be stand-alone or a network of cameras owned and managed by an individual, independent business or trader.

Resolution

This is a measure of the quality of definition and clarity of picture that an imaging device is able to accurately reproduce.

Time-Lapse Video Recording

This is a method of extending the recording duration of the system by reducing the number of frames per second that are stored.

1

The Basics

This section covers the fundamentals of using CCTV in an investigation. It includes setting objectives and parameters for the use of CCTV within an investigation, locating relevant CCTV evidence and prioritising trawls and retrievals to make best use of available resources.

Contents

Figures

1.1 Introduction

ACPO (2005) Practice Advice on Core Investigative Doctrine provides national guidance on investigative good practice, as defined by PIP, which requires investigators to be able to perform their role to an agreed national standard. The use of CCTV, within these frameworks, provides PIP Level 1 and 2 investigators with another tool and potential source of evidence when tackling volume crime. ***ACPO (2009) Practice Advice on the Management of Priority and Volume Crime (The Volume Crime Management Model),* Second Edition** gives further information on volume crime.

1.2 CCTV in Investigations

Given the increasing importance of CCTV to police investigations, it is crucial that investigators are able to correctly collect and use footage to provide the best evidence for prosecutions.

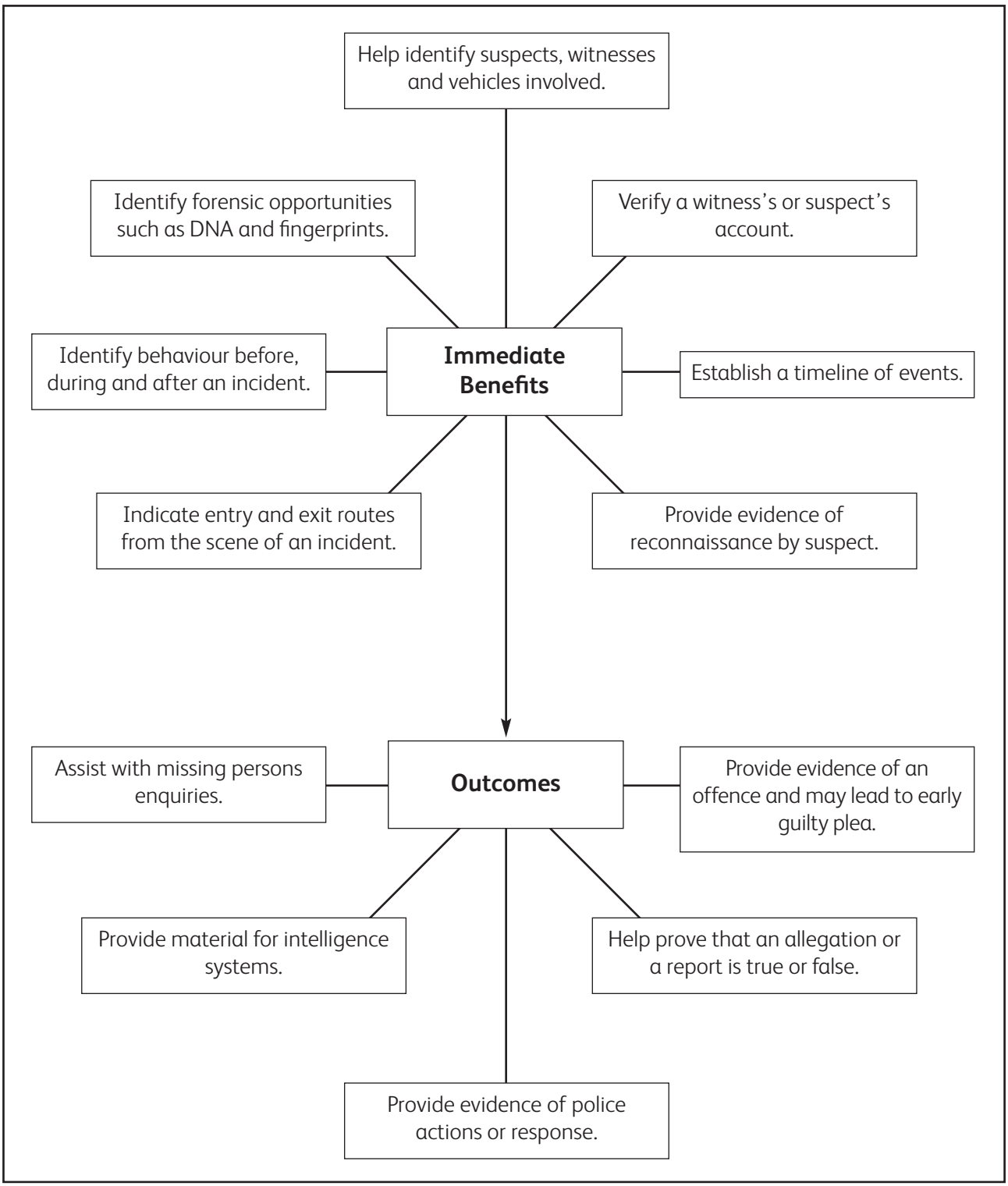
The first opportunity to use CCTV material in an investigation usually occurs during the initial response to the report of a crime. During this phase of the investigation, the location of the offence, the time it occurred and the identity or descriptions of victims, witnesses and offenders will usually become known to the police. These will form the basis of the first trawl for CCTV material. In some cases, investigators will have more material to work with, such as descriptions and registration details of vehicles that are relevant to the offences and the access and exit routes used by offenders.

While it may not be possible for the investigator to view the CCTV material straight away, it is vital to the investigation that footage is obtained as soon as is reasonably practicable.

Although the levels of information available will vary from case to case, it will be highly unusual for there to be so little information that an intelligence-led CCTV trawl cannot be carried out at this stage. Even where only the approximate time and location is known, viewing nearby CCTV may reveal material that provides the basis for further lines of enquiry.

CCTV can be useful in all types of investigations. **Figure 1** shows some of its immediate benefits and outcomes.

Figure 1 – Immediate Benefits and Outcomes of CCTV in an Investigation



Once investigators have gathered all the information they can from victims and witnesses, and have secured scenes for forensic examination, they should consider their CCTV strategy in proportion to the type of offence. This will include:

- Setting objectives, eg, to trace the suspect's movements after leaving the scene;
- Setting parameters, eg, look at CCTV recorded in the one hour period after leaving the scene between that location and the suspect's home address;
- Locating CCTV;
- Prioritising trawls, eg, concentrate on the home address and then move nearer to the scene;
- Legislation, eg, whether Police and Criminal Evidence Act (PACE) 1984 warrants may be needed, data protection requirements;
- Viewing and retrieving;
- Ensuring the continuity of exhibits;
- Disclosure, retention and disposal.

The strategy should be decided as soon as possible because it may lead to the identification of lines of enquiry that will enable more material to be secured quickly. This is particularly important in the case of forensic or fingerprint material, which may deteriorate over time. It may also provide a focus for subsequent appeals to identify suspects.

1.3 Logistics

1.3.1 Setting Objectives

The first thing to do is to identify the objectives of the CCTV strategy. In many cases this will be obvious and it will consist of locating CCTV images of the event itself or images of victims, witnesses or offenders going to or leaving the scene. There will be occasions where the objectives are more complex and these usually occur later in the investigation when there is a need to verify the accounts given by individuals or to test the hypotheses investigators have developed to help them make progress in the investigation. In either case, it is essential for investigators to have a clear understanding of what it is they are hoping to find on CCTV images.

As an absolute minimum, investigators should seek to identify any CCTV material that shows the offence being committed. They should do this even where there appears to be other material indicating a suspect's involvement because, at this early stage of the investigation, it is impossible to predict what material will be relevant. **Investigators should also bear in mind that CCTV footage that does not directly show the offence may be just as relevant as that which does.**

1.4 Parameters

After considering the objective(s), the next step is to focus the search for CCTV on specific times and locations that are relevant to the objective(s). This requires setting the time and location parameters.

1.4.1 Time Parameters

In some cases the time that is of interest to an investigator will be reasonably clear, especially where victims and witnesses have been present during a crime, such as an assault, and can estimate with some accuracy when it occurred. Even when no one is present, information such as the times that alarm systems were activated or when someone heard a window break may provide a time around which parameters can be set.

In other cases this will not be so easy. For example, in many burglaries and thefts from unattended vehicles, victims may only be able to provide the time at which they left the building or vehicle secure and the time at which they returned and discovered the offence. This may cover a period of several hours.

When the time of the crime is known, the time parameters should include a contingency period before and after. This will provide a safeguard against errors in estimating the time of the crime. It will also capture events leading up to and following the crime which may be relevant. The contingency period will vary depending on the offence, but it is advisable to keep it as short as possible. In straightforward cases, ten minutes either side of the reported time should be sufficient. Setting wide parameters can **significantly** slow down the CCTV recovery process and may necessitate the seizure of hard drives/DVR units. Where this is necessary, plans for replacement units must be put in place **prior** to seizing the units themselves.

After confirming the system time difference (see **3.2 How to Note the Correct Time and Date on the CCTV System**) and viewing the footage on site, if nothing of value can be obtained from the CCTV material within the set time parameters, investigators may need to reassess these time parameters after further review of the intelligence or information that they have on the crime.

Investigators should bear in mind that, in some cases, offenders may have visited the scene beforehand in order to plan the offence. In addition, some offenders may return to the scene to witness the consequences of their actions, for example, a person who has committed an arson attack.

In cases where the crime could have been committed over a longer period, investigators could set the parameters for the whole of the period, which may involve viewing a large amount of material, or they could focus the parameters on times when the crime was most likely to

have been committed. For example, in the case of theft from a vehicle in a public car park, intelligence may indicate that other offences have only occurred between specific times, or that there may be circumstances, such as the presence of an attendant, which would make it unlikely that the offence took place at certain times. Such factors may enable the time parameters to be set more closely than would otherwise be the case. In making such decisions, investigators need to balance the risk of missing relevant information by not viewing the whole of the CCTV material against the time they have available to devote to this particular line of enquiry.

Where the investigator is relying on the goodwill of an independent system owner to view and copy or acquire CCTV footage, the investigator must be sensitive to the owner's requirements. This may mean providing the owner with a specific, and sometimes narrow, timeframe within which to queue the footage in preparation for the investigator to view, or it may mean arranging a return visit if they are busy. If a return visit is required, investigators must ascertain what the overwrite times are when arranging the return date and time, see **3.3 How to Establish the Overwrite Period.**

1.4.2 Location Parameters

In many cases, the locations that are of interest to an investigator will be obvious and will focus on the scene, together with access and exit routes from it. As more material becomes available, it may be possible to extend these original parameters to include such things as the route an offender took home after an offence. This may in turn indicate forensic opportunities relating to discarded items, or the location of relevant vehicles.

Where it becomes important to test the accounts people give of their movements before and after a crime, location parameters can be set to include key locations they are known or believed to have been in.

1.4.3 Changing Parameters

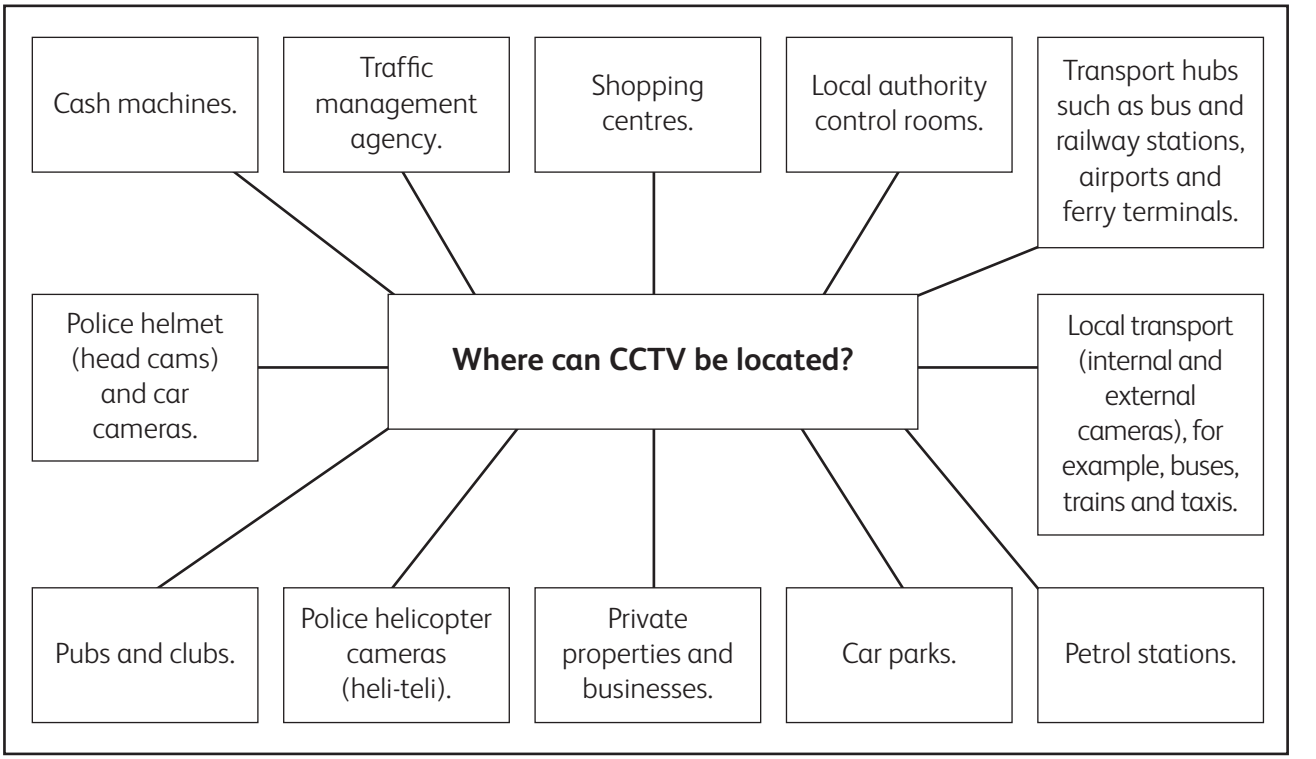
Initial parameters will be based on the material to hand but are likely to change as new information becomes available. Investigators should not be afraid of making such changes when they are needed, but they should bear in mind that some CCTV systems will only retain material for relatively short periods of time, and images that are not gathered quickly may be lost to the investigation.

Any changes to the parameters should be documented in full in the CCTV strategy, along with detailed rationales and intelligence evidencing the changes.

1.5 Locating CCTV

Once the time and location parameters have been set, there should be some consideration of the types of places from which footage can be retrieved. Some of these are highlighted in **Figure 2.**

Figure 2 – CCTV Locations



Investigators need to be aware of the wide variety of public and private systems that may be in use in the locations within their parameters. Some of these systems will be single cameras in retail premises, homes and businesses, which will only be discovered by walking through the area and making detailed enquiries to obtain contact details of those who have practical knowledge on how to operate the system. It is good practice to maintain a forcewide list of CCTV systems, owners and engineers that is accessible to all force staff.

Investigators should also check to see if cameras sited inside premises are focused on the doorway or window, thus catching images of outside activity.

A record of the locations visited, and whether any CCTV could be located, should be maintained to avoid duplication of effort should the investigation be passed to another investigator. This will also enable any premises that investigators could not access initially to be revisited at a later date if required.

1.6 Prioritising Trawls

If there are several areas where trawls for CCTV will be made, it is advisable to prioritise them, so that the ones most likely to be productive are visited first.

1.6.1 Factors to Consider

Some factors investigators may wish to consider when prioritising which CCTV systems to access first include the following:

- Location of the offence;
- Nature of the offence;
- Major roads to or from the scene of the offence;
- Travel routes taken by persons of interest to the investigation;
- Areas frequented by persons of interest, for example, public houses, homes of relatives, gyms;
- Places of significant purchases linked to the investigation and cash withdrawals;
- Areas linked to telephone usage, including both landline and mobile phones;
- Areas linked to Automatic Number Plate Recognition (ANPR) hits;
- Retention period of systems;
- Accessibility of systems, eg, business hours.

If the available resources mean that certain areas will not be visited for some time, it may be possible to contact those controlling the CCTV systems in those areas, eg, local authorities, garages and large business premises, as well as agencies such as the Highways Agency, to request them to retain material within the defined time parameters so that it can be viewed later. This will ensure that material is available to view, even if there is not time to visit all of the locations straightaway.
A request for the footage within known parameters can be made using an appropriate form, see **Appendix 3.**

1.7 Prioritising Retrievals

Where investigators need to delay the collection of footage, they should ensure that they maintain contact with those holding the CCTV material to update them on when collection will be. Every effort should be made to do so as arranged, or let them know if the material is no longer required.

1.7.1 Retrieving CCTV from Vehicles

If CCTV is to be retrieved from vehicles such as taxis, buses and trains, it may be difficult to obtain the footage without the vehicle registration mark (VRM) or other identifying feature (see **1.5 Locating CCTV**). There may, for example, be several 'number 10' buses or black cabs passing through the same area in a short period of time. Furthermore, in order to retrieve footage, vehicles may need to be taken off the road. It is important that investigators do not place unrealistic demands on transport operators that may sour relations in the future. Therefore, it is strongly recommended that, prior to seeking CCTV footage from transport companies, investigators consider using other sources of CCTV or ANPR to establish the VRM before making requests for footage. For information on retrieving footage and powers of seizure, see **3 Viewing and Retrieving.**

If footage from trains or rail property is to be retrieved, early contact should be made with the British Transport Police (BTP) Head of CCTV, who will make the necessary arrangements for the capture of images. This may help to minimise the possibility of carriages from one train ending up in completely different areas of the country.

Further information about BTP and CCTV can be found at **http://www.btp.police.uk/passengers/issues/cctv.aspx**

2

Legal Responsibilities

Currently, there is no primary legislation specifically controlling the use and publication of CCTV images. This section identifies the legal and policy frameworks within which CCTV footage should be viewed, retrieved and managed as police information.

Contents

2.1 Legislation and Policy

To use CCTV effectively, investigators should have a clear understanding of relevant legislation, together with force and national policy relating to its use.

The existing applicable legislation that encompasses the management of evidence, including CCTV, comprises the following:

- Criminal Justice and Police Act 2001;
- Criminal Procedure and Investigations Act 1996 (CPIA);
- Police and Criminal Evidence Act 1984 (PACE);
- Police Reform Act 2002.

In addition, footage should be subject to robust processes and procedures in accordance with:

- ***ACPO (2005) Code of Practice on the Management of Police Information;***
- ***ACPO (2010) Guidance on the Management of Police Information,* Second Edition;**
- ***ACPO (2007) Practice Advice on Police Use of Digital Images;***
- ***ACPO (2007) Good Practice Guide for Computer-Based Electronic Evidence,* [Official Release Version].**

ACPO (2005) Code of Practice on the Management of Police Information, Subsection 2.2 Information for Police Purposes states that all information, including intelligence and personal data obtained for police purposes, is referred to as police information. Images are a form of police information.

Policing purposes are defined as:

- Protecting life and property;
- Preserving order;
- Preventing the commission of offences;
- Bringing offenders to justice;
- Any duty or responsibility of the police arising from common or statute law.

2.2 The Data Protection Act 1998

CCTV recording is covered by the Data Protection Act 1998 (DPA) when the information relates to a living individual who may be identified.

CCTV systems used in large shops, railway stations, town centres and other places where large numbers of people gather are designed to focus on particular people or to identify criminal activity and are

covered by the DPA. When the police wish to view this type of CCTV, the use of a Request for Disclosure of Personal Data under section 29(3) of the DPA may be requested by the system owner or operator, see **Appendix 3.** A DPA Request for Disclosure provides a means for the police to obtain CCTV material and it allows data controllers (CCTV operators) to disclose personal information to the police.

For further information on the DPA and use of images, see ***ACPO (2007) Practice Advice on Police Use of Digital Images.***

2.3 The Criminal Justice and Police Act 2001

Part 2 of the Criminal Justice and Police Act 2001 provides a power to seize and sift which is not confined to PACE. One key purpose of the legislation is that it enables investigators to remove material from premises for examination elsewhere, for example when there is insufficient time to conduct an effective examination on the premises, or there is a need to use some special technical equipment which can only be made available elsewhere.

Under the legislation, an entire computer disk or hard drive can be seized and retained where it is necessary to prove when specific items of information were created or amended.

The key issue is that the legislation allows the data (images) on the computer hard drive or storage medium to be sorted through and images removed that are evidentially relevant and can, therefore, be seized in circumstances where a requirement under PACE section 20 would not be practicable. Application is subject to PACE Code B paragraphs 7.7 to 7.13, which set out the additional rights of owners.

All these powers are accompanied by safeguards such as the ability to apply to a judge for the return of material which has been seized and restrictions on how seized material can be retained and used.

The powers are relevant to a wide range of circumstances, but they are established on the principle that they can only be used where a person could have exercised an existing power of seizure. All these existing powers are listed in Schedule 1 of PACE.

For full details see ***Home Office Circular 019/23, Home Office (2003) Guidance on operating the new powers of seizure in Part ll of The Criminal Justice and Police Act 2001*** available at **http://www.homeoffice.gov.uk/about-us/home-office-circulars/circulars-2003/019-2003/**

2.4 The Criminal Procedure and Investigations Act 1996

The CPIA concerns the disclosure of what has been seized under powers, and places a duty on the police to pursue all reasonable lines of enquiry to obtain evidence. In conducting an investigation where the inherent difficulties in retrieving footage from digital systems occur, the CPIA Code of Practice paragraph 3.5 section 23(1) requires that

investigators do not simply dismiss potential sources of evidence because, for example, footage may be difficult to extract from a system. All reasonable attempts must be made to successfully retrieve the images. This is underpinned by the powers and means to do so derived from PACE and other legislation. Advice should be sought from senior officers on what constitutes 'reasonable' in the type of offence being investigated if this is unclear.

It is critical that the Code of Practice issued under section 23(1) of the CPIA is followed by all investigators. It sets out the manner in which police officers are to record, retain and reveal to the prosecutor material obtained in a criminal investigation that may be relevant to the investigation and related matters. It states in paragraph 2.1 that:

> Material may be *relevant* to an investigation if it appears to an investigator, or to the officer in charge of an investigation, or to the disclosure officer, that it has some bearing on any offence under investigation or any person being investigated, or on the surrounding circumstances of the case, unless it is incapable of having any impact on the case.

Section 5 of the Code also sets out a 'relevancy test' to help determine whether CCTV evidence should be retained and states how long relevant material should be retained when the accused is convicted. It applies to:

- Obtaining and retaining CCTV material;
- Disclosure of CCTV material in court;
- Storage of CCTV material.

Failure to comply with this code may make evidence inadmissible. For further information on the CPIA and the use of images, see ***ACPO (2007) Practice Advice on Police Use of Digital Images.***

2.5 The Police and Criminal Evidence Act 1984

CCTV material is owned by the person or organisation to which the CCTV system that generated it belongs. Under PACE section 19, an investigator who seeks entry to premises with the occupier's consent must state the true purpose for seeking entry. If it is in order to view CCTV images with the objective of determining their evidential value and securing them for evidence, for example, by copying or seizing, then this must be stated from the outset. The explanation should include that replacement media will be provided and detail any other steps that will be taken to minimise inconvenience to the occupier.

In a situation where an owner refuses access to the CCTV footage, the power to seize depends on whether the investigator is lawfully on the premises, ie, whether they have been invited on to the premises.

This invitation can be withdrawn at any time. Therefore, if and when an investigator is refused the CCTV material and told to leave, the invitation has been withdrawn and the investigator no longer has the power of seizure. In this case an investigator will, in the first instance, need to use their powers of negotiation and, as a last resort, apply for a warrant under PACE section 8. This is only possible if the information sought, ie, CCTV images, is **not** special procedure or excluded material for the purposes of PACE sections 11 and 14.

Images captured by CCTV systems used for internal purposes, ie, inside shops, railway stations and town centres (see **1.5 Locating CCTV**), not public space, and acquired during the course of business, are special procedure material, ie, held in confidence. In order to obtain such material without the owner's consent, investigators will need to apply for a production order or search warrant under section 9 and Schedule 1 of PACE, not section 8.

When equipment is seized, a receipt should be issued to the system owner with details of the make, model and serial number. Investigators do not have a right to seize anything that they have reasonable grounds for believing is subject to legal privilege. This is set down in PACE section 19(6).

2.6 The Police Reform Act 2002

Section 38(2) of the Police Reform Act 2002 gives provision for, and governs, the designation of directly employed police authority staff as investigating officers. This means that the power of seizure can be granted to civilian staff by the chief constable of their force. This may be useful in larger investigations when vast amounts of CCTV material need to be retrieved quickly.

For full details, refer to section 38(2) and Schedule 4 of the Police Reform Act 2002.

3

Viewing and Retrieving

This section focuses on viewing CCTV at the scene, and how to retrieve footage that is relevant to an investigation. Figures 3 and 4 give a summary of the process to follow when retrieving analogue and digital CCTV.

Contents

Figures

3.1 Viewing CCTV at the Premises

Footage should be viewed at the scene to establish relevance prior to seizure. Where system owners agree to provide access to the system for onsite viewing, it is preferable that they, or someone familiar with the system, operate the equipment under the direction of the investigator.

If neither the system owner nor the person in charge is familiar with the operating system, the investigator should ascertain whether or not the technical engineer, ie, the person who installed the system, is available to assist. If this is not possible or the delay will be excessive, the investigator should enquire whether there is an instruction manual available. If the officer is confident and has the owner's or agent's permission, they may operate the system, ensuring that they leave it in its original state. Failing this, the investigator will need to seek advice from their force technical CCTV specialist (FTCS).

In judging whether an image is relevant or not, investigators need to be mindful of their obligations under the CPIA and should apply the relevancy test contained in that Act. See **2.4 The Criminal Procedure and Investigations Act 1996.**

Examples of CCTV material which would pass the relevancy test include CCTV which:

- Captures the defendant committing the alleged offence;
- Reveals that the wrong individual has been arrested for the alleged offence;
- Does not support the account given by the complainant and/or witnesses, for example, mistaken identification;
- Reveals the alleged complainant as the perpetrator (and supports a defence of self-defence);
- Shows that the parties are not captured on the video when, on the eyewitness evidence, they should be (and there is no suggestion of a technical fault and/or video overrun);
- Reveals the demeanour of witnesses;
- Captures the immediate aftermath of the alleged offence;
- Reveals the actions of witnesses;
- Reveals the crime scene;
- Reveals potential witnesses.

If it is discovered that a CCTV system is of such poor quality that footage cannot be downloaded, copied and/or properly viewed, it is advised that a Crime Reduction or Crime Prevention Officer (CRO/CPO) is informed.

It is recommended that, where possible, investigators view the footage on the originating system to check the quality of the footage and verify colour capture as this may not be accurate on all CCTV systems. Colour differences can be caused by incorrectly set cameras or by the use of infrared (IR). Colours can also be misrepresented on specific fabrics/materials and can be affected by environmental factors such as the sun and street lamps. Any discrepancy should be noted, especially if the item is to be used as evidence.

3.1.1 The Presence of Victims or Witnesses

Victims and other witnesses or potential witnesses to a crime should not be present when investigators view CCTV material. This is especially important if the witness has not yet made a statement, as it is necessary to avoid any contamination of the witness's memory. If victims, witnesses or potential witnesses do happen to view the footage before they make a witness statement, this **must** be recorded in their statement. This is most likely to happen where the victim is the owner of the CCTV system; particular care should be taken in these situations.

3.2 How to Note the Correct Time and Date on the CCTV System

Before viewing the CCTV images, it is important to establish if the time and date displayed by the system is accurate. The time and date that the suspect appeared, or that the crime occurred, will be crucial when trying to piece together evidence. CCTV equipment is rarely changed to take into account differences between Greenwich Mean Time (GMT) and British Standard Time (BST). In addition, some systems can simply display the wrong time and date. The actual time and date of the footage must be checked or timings may be inaccurate. The best way to ensure that timings and dates are correct is to compare the current time and date shown on the CCTV system with a known, reliable source, eg, the speaking clock (dial 123). Investigators should then make a note of the two times and dates and the difference between them. Investigators must **not** change the system's time or date.

3.3 How to Establish the Overwrite Period

It is essential that investigators note the overwrite period of the CCTV system so that they are aware of how much time they have to extract images before they are irretrievably lost.

It is not enough to simply ask the owner what the overwrite period is. An estimation of the overwrite time can be obtained by viewing the earliest footage saved on the system. The number of days between the date of the earliest recorded material and the date of attendance is a guide to the overwrite period. If there are gaps in the recording, or where there is protected data on the system, this can give a false impression of the apparent overwrite time. Investigators should not leave this check until the last minute, otherwise the system may begin to overwrite.

3.4 Retrieving CCTV from the Premises

When investigators find relevant CCTV footage, they should make appropriate notes. If the investigator attending believes the footage is of no relevance, they must record the reasons why they chose not to retrieve the footage in their pocket book, together with the name of the system searched, the objectives, time and location parameters and the name of the person operating the system.

Force policies should make it clear who is responsible for retrieving and replacing media and equipment in the event of it being required as evidence. This may vary depending on the severity of the crime.

Analogue footage should not be copied at the scene. Investigators are advised to simply remove the relevant VHS tape, break the record tab to prevent accidental erasure or overwriting, label and bag it.

Depending on the type of VHS tape used, there are two methods that can be employed to avoid accidentally recording over footage:

1. If the VHS tape is held ready for insertion into a video cassette recorder (VCR), the record tab appears on the left-hand side of the back end of the VHS tape. Break this tab off. This will leave a hole that prevents the recording of any further footage.
2. If there is no record tab, a small shutter will be seen instead. This shutter should be opened to prevent further recording.

Whenever possible, a blank replacement VHS tape should be provided.

It is recommended that, where practicable, footage believed to be relevant should be exported from digital systems rather than seizing the whole system. This should only be considered as a last resort.
See **3.7 The Removal of CCTV Systems and Hard Drives.**

The same principles discussed in **3.1 Viewing CCTV at the Premises** apply to retrieval in relation to competency to operate the system, exclusion of witnesses and sources of advice.

If the CCTV service provider is to be contacted for help, investigators need to be aware of the potential cost implications of this. In addition, investigators should bear in mind that the competency of these agencies cannot be measured, and that their employees may not be aware of evidential requirements. If the CCTV service provider is unable to assist, investigators should contact their FTCS for help.

In order to replay exported footage, special replay software may be required. Sometimes when footage is exported, replay software is automatically downloaded. In other cases, however, investigators may need to obtain the relevant replay software from the manufacturer's website or other source. Some forces may have CCTV viewing software available to them. Attempting to view the footage on a laptop at the

premises can help investigators decide whether the replay software has been automatically downloaded. See **3.1 Viewing CCTV at the Premises** and **3.6 Viewing Retrieved Footage at the Premises.**

If footage is to be retrieved from places that are not privately owned, such as local authorities and transport companies, the retrieval will usually be carried out by employees of those organisations. Much of the success of this type of retrieval, therefore, relies on good working relationships with these organisations. This is particularly relevant to the FTCS as regular liaison with these agencies can ensure that they have the appropriate technical equipment available if a major incident occurs. This can help to ensure adequate cooperation and the prompt retrieval of images. See also **9.6 Post Trial.**

3.5 How Much Footage Should be Retrieved?

If a very large amount of footage is required, a local authority or other non-police organisation submitting the images may charge for the time it takes to download. This is something that needs to be discussed before the download process begins. The FTCS may be able to assist in providing consumables such as hard disk drives (HDDs) for mass export purposes. A payment may also need to be made to any installers who are required to download footage from larger or complex digital CCTV systems. **Note:** Third party engineers will not be evidentially aware.

3.6 Viewing the Retrieved Footage at the Premises

If non-police organisations download footage, they will be required to complete a continuity statement, preferably at the time of retrieval. See **5.2 Continuity Statements.** In addition, if images have been captured by proactive CCTV operators, for example, if they have taken action as a result of a phone call or have received information via an Airwave terminal, they may have made 'original notes' at the time of the incident. These notes should also be retrieved along with the CCTV product, where possible.

Before an investigator leaves the premises, it is advisable that all retrieved CCTV footage is viewed briefly and checked to confirm that the images have exported correctly, and also that the relevant cameras and timescales have been captured. Investigators should bear in mind that when a DVD is searched in the fast forward mode, at a given speed, individual frames/pictures are skipped. See **6.1 Validation.** Where investigators are unable to export the footage at the scene, they should seek advice from the FTCS.

CCTV systems do not usually have the facility to view exported footage. Where investigators have access to laptops, they will be able to view digital footage at the scene. Alternatively, premises are likely to have computers that can be used. If this is unsuccessful, investigators should ensure that the correct overwrite period, together with the make and model of the system, is noted, before taking the copy to the police station for verification. If investigators are still unable to verify that the

footage has copied successfully, it may be appropriate to seek advice from the FTCS.

In any event, the footage should be viewed at the police station as soon as is practicable.

If the CCTV owner refuses the investigating officer access to the CCTV system and/or the footage, the officer should refer to **2 Legal Responsibilities.**

Figure 3 – Retrieval of Analogue CCTV

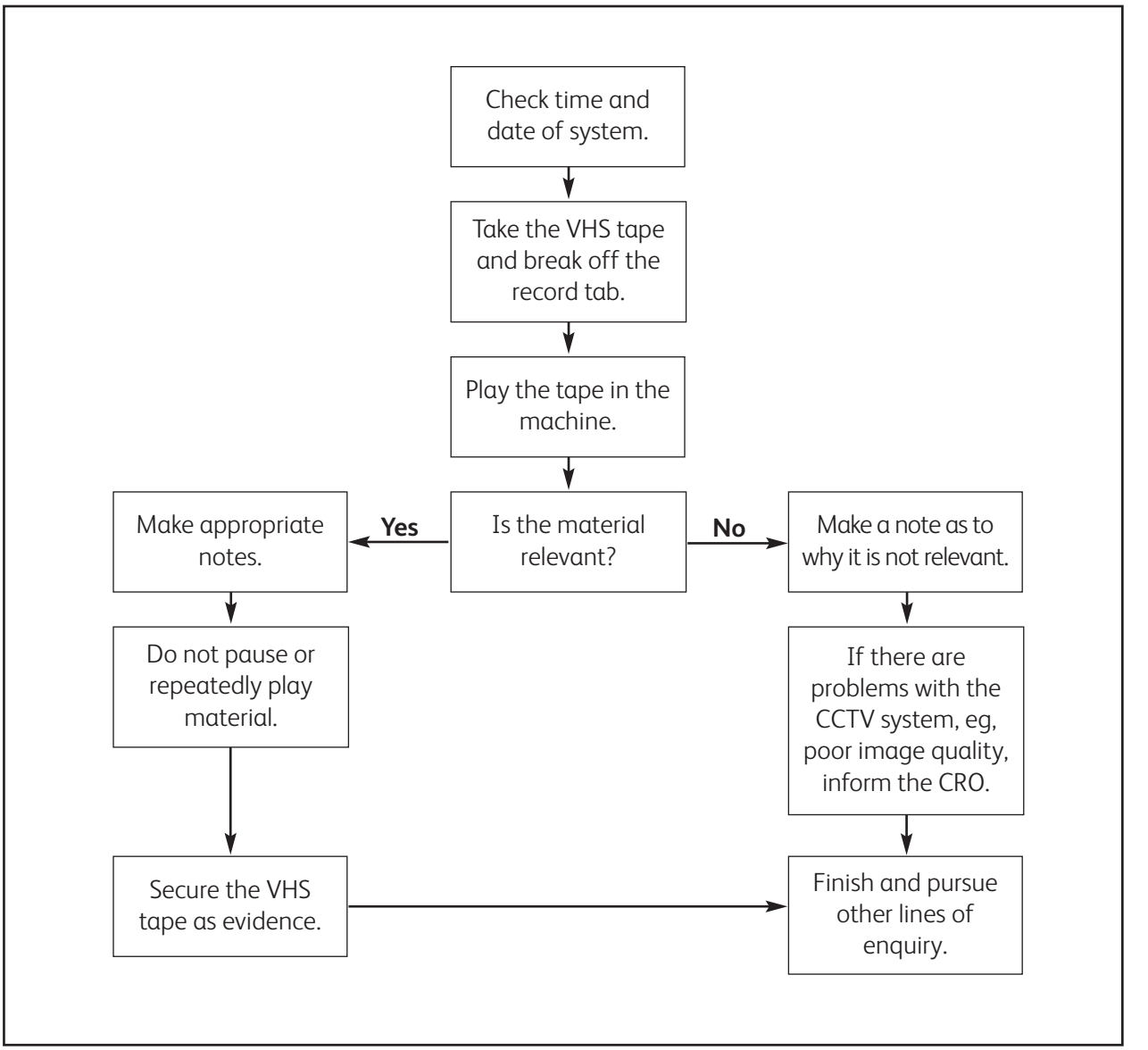
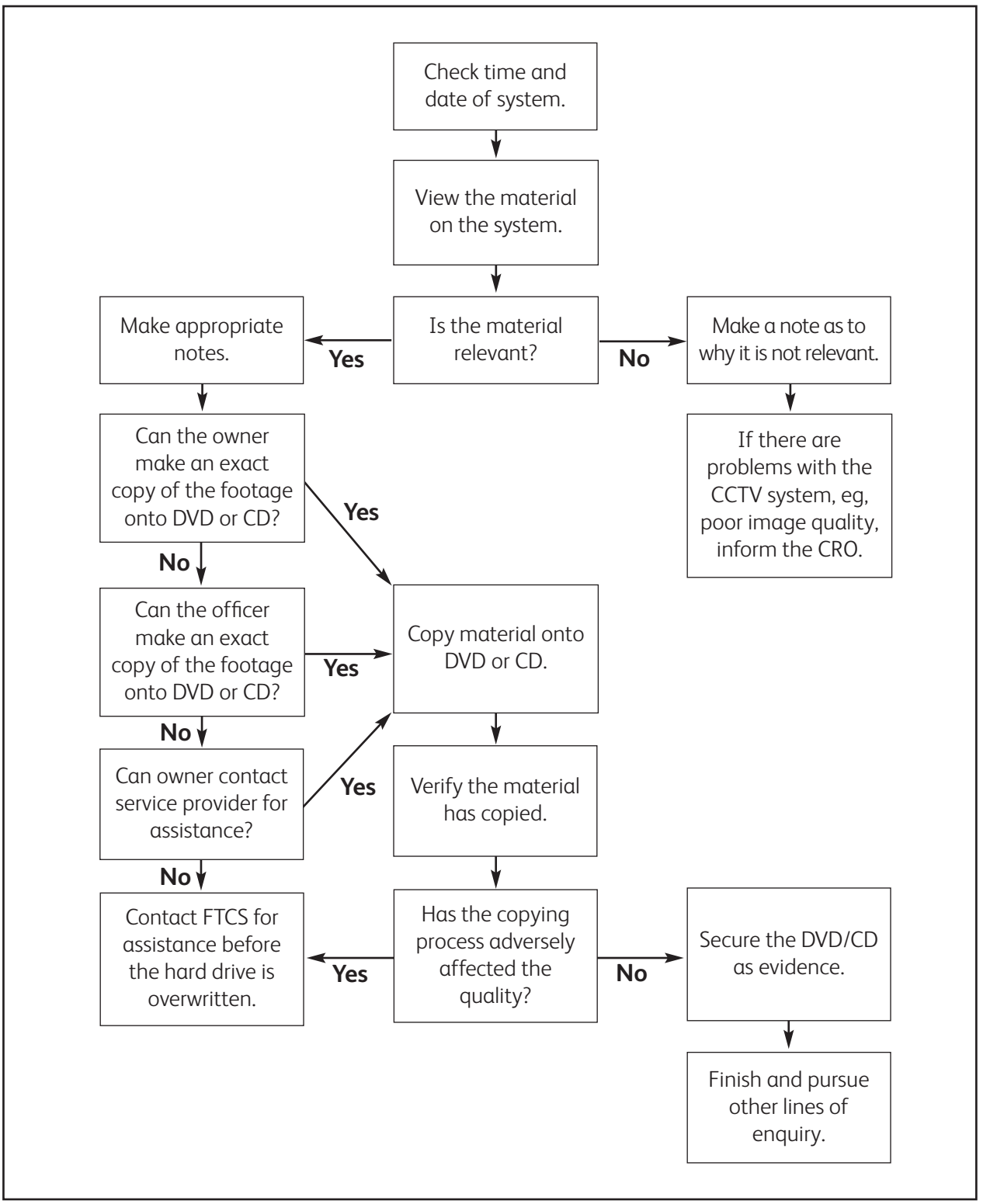


Figure 4 – Retrieval of Digital CCTV



3.7 The Removal of CCTV Systems and Hard Drives

Force policy and standard operating procedures should give clear direction on the removal of CCTV systems and hard drives. A damaged system may not only jeopardise a potential conviction, but may also cause a force to incur huge compensation costs. In addition, investigators may be exposed to electrical safety hazards if, for example, they remove equipment lids or unplug connections.

Before a CCTV system or hard drive is removed, the agreement of several parties may be required. Firstly, the owner must agree, otherwise the system will need to be seized, see **3.8 Refusal of CCTV Owner to Allow Officers to View, Retrieve or Remove CCTV Footage or System.** Secondly, it is good practice to provide the owner with a replacement system or hard drive, see **3.7.1 Physical Removal.** Investigators will need to confirm with the FTCS that there are suitable replacements available. Finally, investigators should be aware that any additional costs for removal of a system will have to come out of the funds allocated to the investigation. These costs may include payment to external contractors to remove a system or the cost of buying additional replacement systems.

As with all evidence retrieval, a continuity statement should be completed. See **5.2 Continuity Statements.**

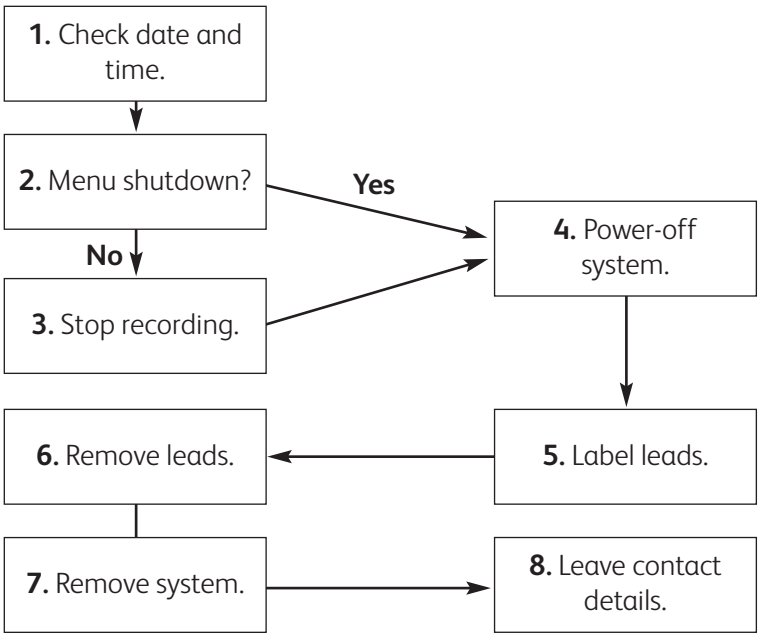
3.7.1 Physical Removal

As a last resort, if an FTCS is unavailable to assist, the investigator may need to remove the recording unit. This will require the investigator to follow **Figure 5.**

When a hard drive or entire CCTV system is removed, the owner should receive a replacement system so that their premises are not left unprotected. See **3.7 The Removal of CCTV Systems and Hard Drives.** This is particularly relevant for banks and post offices, where there is a risk that further offences could be committed. Additionally, there may be insurance and licensing considerations that will prevent the premises from operating without CCTV. In all investigations, the cost implications of this should be considered before investigators begin to trawl.

If resources restrict the number of replacement systems available, there may be a need to arrange additional police resources, for example, foot or car patrols, subject to an appropriate risk and proportionality assessment. Local authorities can also be asked to direct their cameras towards the premises to offer some form of protection to the owners.

Figure 5 – Physical Removal of the Recording Unit



1. Before changing any settings, check the time and date against the speaking clock or similar.

2. Is there a menu option to shut down the DVR? If so, activate it and follow any instructions given.

3. If there is no menu option to shut down the DVR, stop the DVR recording (software or hardware). This is usually a button marked with a white square.

4. Wait at least 30 seconds after step 2 or 3 above, then turn off the power to the machine using either a switch on the machine (if present) or by switching off or removing the plug from the wall.

5. If at all possible, label the leads connected to the machine; this can be done with white tape or sellotape and paper.

6. Carefully remove the leads from the system, retaining any connectors that come loose. If the unit has an external power supply, this must be retained as well.

7. Ideally, place the system in a protected box and then in an evidence bag or otherwise suitably secure transport medium.

8. Ensure contact details are left with the venue for information regarding replacement/return.

3.8 Refusal of CCTV Owner to Allow Officers to View, Retrieve or Remove CCTV Footage or System

To help expedite the acquisition and avoid loss of any CCTV footage, the first responding officer will find that negotiation rather than use of statutory powers is more likely to have the desired outcome.

As a last resort, if the owner refuses to allow officers to view, retrieve or remove CCTV footage, consideration should be given to the issue of a section 66 Serious Organised Crime and Police Act 2005 (SOCPA) retention notice. Although this is not CCTV specific, once served and a copy retained, it can help to provide evidence in support of an attempt to pervert the course of justice if the footage has been allowed to overwrite or has been disposed of. See **Appendix 4.**

4

Post Retrieval

This section looks at the creation of copies of CCTV footage, editing the footage and ways of dealing with poor-quality images.

Contents

Figures

4.1 The Creation of Master and Working Copies

In small and/or uncomplicated investigations, it is advisable to have a master copy and a working copy of every piece of footage retrieved. This may become impractical in larger investigations, but one solution is to use a secure server for the storage of master evidence. Attempts should be made to make a working copy from the master when critical evidence or intelligence is identified, or when technical issues require it. If no copy can be made, investigators should ensure the integrity of the master and protect it from being altered. Transport media such as USB pen drives can be used to transport larger amounts of CCTV footage but are not themselves used as exhibits. The footage on the transport media will be copied to write once, read many (WORM) media, eg, CD-R or DVD-R disc, and then exhibited. See ***Home Office (2007) Digital Imaging Procedure,* Version 2.1 November 2007 58/07** available from **http://tna.europarchive.org/20100413151426/http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/DIP_2.1_16-Apr-08_v2.3_(Web)47aa.html?view=Standard&pubID=555512**

Investigators will also need to determine whether or not copying the footage has adversely affected the quality of the working copies. A loss in video or image quality is acceptable if there is no loss in evidential quality. For example, a man wearing a black and white striped shirt is seen to commit an offence. If copying or converting the footage changes the black part of the shirt to appear grey then this may be acceptable if he does not dispute that the person in the footage is him. If he disputes the fact, then a loss in video quality would not be acceptable.

4.2 The Creation of Working Copies from VHS Tapes

The copying of VHS tapes must often be done in real time and can be very time-consuming. Investigators may, therefore, wish to create a working copy of the footage and store the master. When making this decision, there are several points that investigators should consider:

- Although VHS is quite a robust format, pausing the tape at the same place can degrade the image.
- If working copies are to be made, investigators should bear in mind the practicalities of this, especially if there are many tapes to copy. Proportionality and resource implications should, therefore, be considered.
- It is important for investigators to consider whether the analogue footage will be copied onto another VHS tape or converted into digital format. Converting footage into digital format may mean that footage is easier to edit and copy. It may also be the most practical option for court purposes and for long-term storage. However, it can also cause a marked drop in image quality, which is a cause for concern. Problematically, investigative decisions may then be made on the basis of inferior evidence. See **4.1 The Creation of Master and Working Copies.**

- If the analogue footage is multiplexed, ie, it displays footage from more than one camera at the same time, it is advised that the footage is demultiplexed. The master can be split and individual data extracted using software commonly called a file splitter. This is something that the FTCS may be able to assist with. The demultiplexed footage becomes a new master exhibit.

4.3 Sending Footage to the FTCS for Editing

Depending on the circumstances of the offence and force policy, the footage may need to be edited or copied by the FTCS. If this is the case, once the CCTV is retrieved, a note should be taken of the camera number and the exact time that the relevant images appear. This will aid the FTCS and avoid requiring them to watch half an hour of footage in order to spot ten minutes of relevant images. A description of what to look for is also helpful, for example, 'white man wearing a red sweater entering premises'. Investigators should bear in mind, however, that poor-quality footage may cause ambiguity regarding the description.

Investigators will need to ascertain whether or not the data has changed. If it has, then it is a new exhibit. If, however, only the container has changed, it is not. For example, the file theft.avi is converted to theft.mpg; the video footage is the same but the data itself is different. This is a new exhibit. If, on the other hand, theft.avi was on a USB flash memory device and copied to a CD-Rom (WORM media), as per ***Home Office (2007) Digital Imaging Procedure,* Version 2.1 November 2007 58/07** and ***Home Office (2008) Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems,* Version 2.0 publication number 66-08,** then theft.avi has not changed, just the medium that it is stored on and it is, therefore, a copy of the original exhibit.

Any format conversion or data changing should be carried out by an FTCS or other skilled department. A person tasked with carrying out this role should be able to explain what they have done to a court.

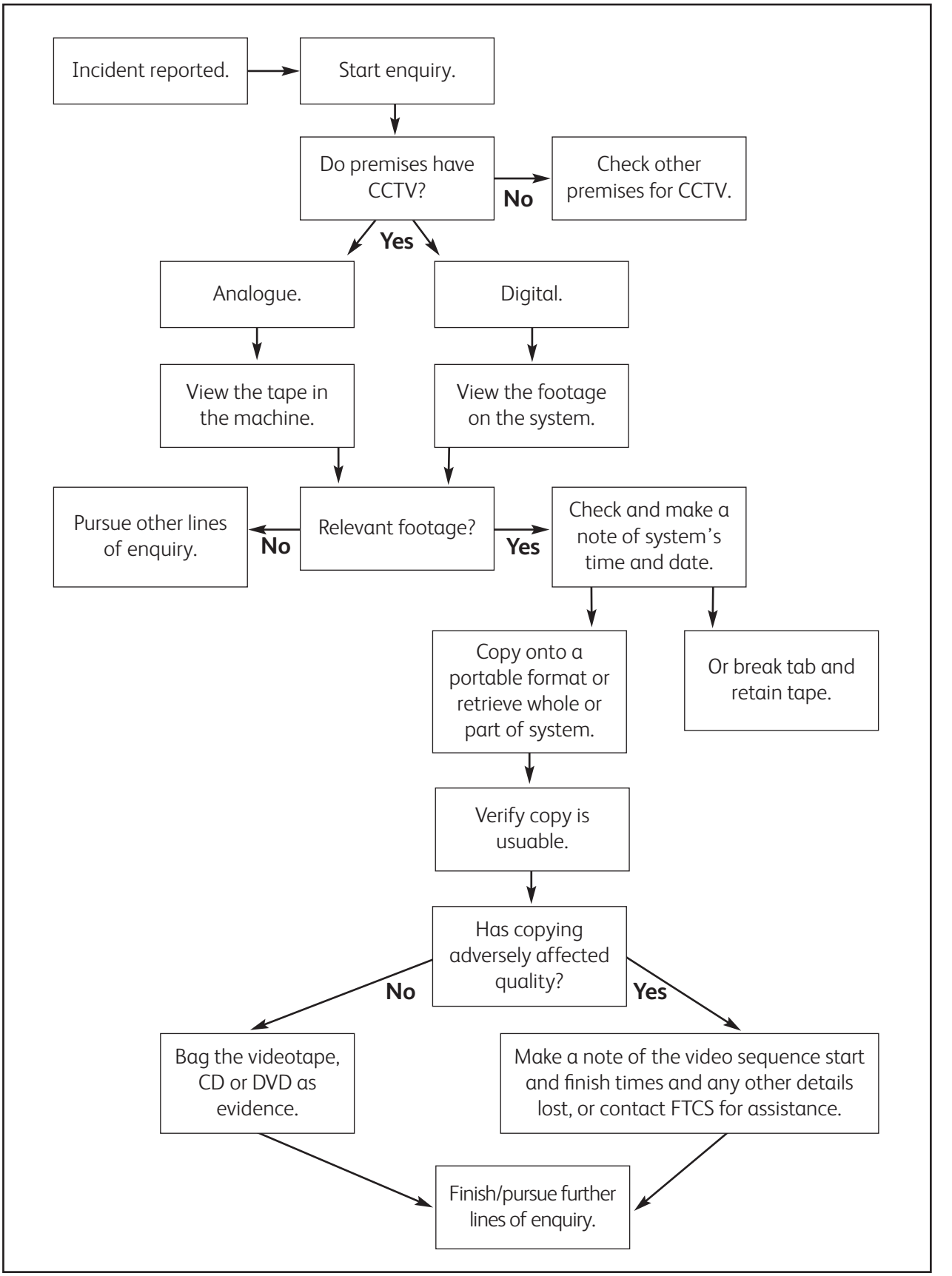
4.4 Poor-Quality Images

CCTV image enhancement is extremely limited and is not possible in the majority of cases, beyond the basic adjustment of brightness or contrast.

Images are made up of a series of pixels, which are digital squares. Each square has a colour and when placed together, they make an image. In basic terms, if a suspect's face or vehicle registration plate is blurred so that it is only possible to see colour with no definition, this usually means that there are not enough squares to give the resolution needed for a sharper, clearer image.

If unsure, investigators are advised to seek advice from the FTCS.
See also **4.1 The Creation of Master and Working Copies.**

Figure 6 – Basic CCTV Locating, Copying and Retrieval Process



5

Exhibits

CCTV footage can be compelling evidence against an offender at trial. It is therefore imperative that a robust audit trail is in place which documents the movements of CCTV products. This is particularly relevant when a CCTV product becomes an exhibit and when the reviewing process begins.

Contents

5.1 CCTV Exhibits

All CCTV exhibits coming into the possession of the investigator should be recorded to show:

- The name of the officer who collected the footage;
- From where the footage was retrieved;
- When the footage was retrieved, including GMT-corrected time, as well as the system time (this greatly assists in creating sequences of relevant events);
- What period of time the footage covers;
- The overwrite period;
- The exhibit number.

Exhibits must be stored safely and should be logged both in and out of storage. Force policy on exhibits should always be referred to.

5.2 Continuity Statements

The person who retrieves the footage from the CCTV system will need to complete a statement to ensure the continuity of the evidence. This person could be the owner of the system, a police officer or an FTCS. The statement need only contain the details of what the person did to retrieve the footage. This may be just a few sentences, outlining the date, time and how the person copied or exported the footage, eg, downloaded the images onto a DVD. Many forces have pro forma MG11 forms, specifically designed for this type of situation, which can be quickly filled in at the premises. Any discrepancies between the time shown on the CCTV system and the actual time of the footage should also be noted in the statement. See **3.2 How to Note the Correct Time and Date on the CCTV Footage** and **3.3 How to Establish the Overwrite Period.**

CDs and DVDs are damaged by light and heat and should be kept in a hard CD or DVD case. Suitable storage cases include clams, ejectors and jewel cases. There should be one CD/DVD per case to avoid the discs being scratched and damaged. Labels should not be stuck on discs, nor should they be written on with a ballpoint pen. Discs should be labelled using a multimedia marker pen, not a general permanent marker. It is good practice to mark the disc with identifiable/unique features, such as exhibit numbers, the source location for the disc creation, date and copy number. Such marking identifies the specific disc against any additional copies created.

5.3 Maintaining Continuity and Integrity of Exhibits

CDs and DVDs should be stored in a way that proves the integrity of the product and also shows that it has not been subject to any unauthorised access.

Transport media, such as pen drives, flash drives and CD-RWs/DVD-RWs are not suitable for long-term storage and data should be copied onto

WORM media as soon as reasonably practicable. See ***Home Office (2007) Digital Imaging Procedure,* Version 2.1 November 2007 58/07** available at **http://tna.europarchive.org/20100413151426/http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/DIP_2.1_16-Apr-08_v2.3_(Web)47aa.html?view=Standard&pubID=555512**

If there is a need to keep the media for other evidential opportunities, eg, fingerprints, they can be stored in a suitable evidence bag.

Hard drives are fragile devices. If they are to be stored, they should ideally be kept in appropriate shock resistant packaging and stored away from magnetic sources and high voltage mains or equipment. Individual boxes or hard cases should be used with anti-static bags. The protective packaging in which hard drives are bought is also suitable and can be reused. Only one hard drive should be stored in each box. Putting more than one in the same packaging may result in the drives being damaged.

6

Viewing CCTV

This section provides advice on viewing seized CCTV material.

Contents

6.1 Validation

The purpose of viewing seized material is to identify that which is of use to the investigation and document it so that it can be used as evidence or intelligence. CCTV exhibits should be assessed and a documented decision made about whether to undertake a detailed viewing or simply retain them. It is good practice to summarise at an early stage what can be seen in the footage that will be produced for the Crown Prosecution Service (CPS). This will enable a charging decision to be made.

Once material has been seized, it should be viewed as soon as possible. This ensures that time is not wasted collecting huge amounts of footage when early viewing may have taken the investigation in a different direction or highlighted other investigative opportunities. In addition, any potential problems with the data that may have been missed when viewing took place at the premises can be identified. When checking, investigators should bear in mind that when a DVD is searched in the fast forward mode, at a given speed, individual frames/pictures are skipped. See **3.6 Viewing the Retrieved Footage at the Premises.**

Viewing will often be simply a case of confirming what has already been identified during the initial viewing and documenting it.

6.2 Visiting the Location of the Incident

In cases where the location has not been visited, investigators viewing footage may find it beneficial to visit the areas from where the CCTV images were taken. This will help viewers familiarise themselves with the relevant locations and visualise where events have taken place. The advantage of this is that viewers may then find it easier to piece together routes taken by vehicles or persons of interest. It also means that the footage is viewed in the context of the area as a whole.

Another option is to use an online map that has a street view function. This will allow the investigating officer to see an area from ground level and help them to develop situational awareness of the scene. If any of the above methods are used, the procedure must be included in subsequent statements the investigator makes.

Layout plans of premises showing the coverage of each CCTV camera can also be useful. This is particularly the case when suspects and witnesses move around a large building, such as a licensed premises, which could have a number of cameras. The layout plan will assist the viewing officer to change cameras and follow an individual.

6.3 Viewing Conditions

Under the Health and Safety at Work etc. Act 1974, chief officers have a responsibility to ensure the health and safety of their employees. ***Health and Safety Executive (2009) Striking the balance between operational and health and safety duties in the Police Service*** sets out clear expectations of how the Police Service will apply health and safety legislation in challenging operational environments. This document is available at **http://www.hse.gov.uk/services/police/duties.pdf**

Viewing CCTV images for the purpose of analysis can be demanding, especially where there is a large amount of footage that needs to be analysed. Sustained viewing should, therefore, take place in areas that have appropriate lighting and ventilation, and limited distractions.

Given the difficulty of maintaining concentration for long periods of time, viewers should take regular breaks. Breaks should be taken away from the viewing area and computer screen. Viewers should consider going outside the building to refresh themselves and to allow their eyes to focus on other things.

6.4 Viewing Parameters

As with retrieval, viewing parameters and priorities should be set and these should be based on information and evidence already received.

If multiple staff are tasked with viewing footage of the same crime, advice should be sought from the FTCS in relation to various strategies for managing this.

> Viewers able to present a comprehensive reconstruction or interpretation of an incident from extensive review and analysis of CCTV images and other material, such as photographs taken at the scene and the time of the crime, should be aware that they may be called to give evidence in court as ad hoc expert witnesses. See **Appendix 2.**

6.5 Reference Images

It may be useful to have reference images to hand as a reminder to viewers of what they should be looking for. This could, for example, be a photograph of the suspect's vehicle or a distinctive item of clothing. If this method is to be employed, caution should be taken if the area is open to members of the public or other non-members of the investigation.

6.6 Viewing Logs

A viewing log should always be completed when viewing CCTV. An example of this is available in **Appendix 5.**

Viewing logs should:

- Document what has been seen in the footage;
- Describe the actions of individuals (especially victims and suspects) in a neutral manner.

Emotive language such as 'viciously' or 'unprovoked' should be avoided.

Defence solicitors may apply to view unused and unviewed footage. If all relevant CCTV images have been viewed and the viewing logs completed, this will reduce the risk of defence solicitors discovering further relevant footage from CCTV that officers have not viewed.

It is strongly recommended that supervisors quality assure the work of viewers by, for example, spot checking viewed footage and logs.

7

Using CCTV as an Investigative Tool

This section covers identification and recognition of persons from CCTV footage. It must be read in conjunction with Code D to the Police and Criminal Evidence Act 1984 and Annexes A and E.

Contents

Figures

7.1 Ways in Which CCTV Can Assist an Investigation

There are a number of ways in which CCTV can assist an investigation. It can, for example:

- Show the offence and reflect its nature and severity;
- Help to identify the suspect and others who were present at the time the offence was committed, who may be witnesses or co-offenders;
- Lead to recognition by non-witnesses where the identity of someone in an image is unknown. This will then enable enquiries to focus on gathering further evidence against them by other means, such as searching their homes, and enable identification procedures under Code D of PACE 1984 to be carried out by eyewitnesses.
- Show inconsistencies in witness and suspect accounts;
- Help to identify other investigative opportunities, such as:
  - Forensic opportunities resulting from actions captured in the image or clothing worn or weapons used which can be recovered for examination, eg, a discarded cigarette;
  - Location of discarded property;
  - Tracking the movements of offenders and witnesses to and from the scene by capturing them on different CCTV systems, which may provide improved images that make it easier to identify the individual, associates or clothing, as well as identifying locations that may be of interest.

7.2 The Dissemination of CCTV Evidence

In the early stages of an investigation, the priority will be to identify the offender(s) responsible for the commission of the offence. However, when viewing footage, investigators should regard all persons depicted on the CCTV material as potential witnesses. The CCTV images may also show that there are co-offenders, whch is another reason why it is important to view a reasonable period of time on either side of the actual offence.

In any case, the investigator will need to identify as many persons in the CCTV material as is practicable. To achieve this, it is extremely likely that some of the CCTV images obtained will need to be disseminated.

To ensure optimum exposure and use of resources, the following staged approach is recommended:

- Dissemination to police personnel;
- Dissemination to partner agencies;
- Poster campaign;
- Dissemination to the media, including Crimestoppers Most Wanted.

Investigators should refer to their force policy in relation to the release of CCTV images. Exhibited images must have an audit trail back to the original CCTV exhibit they came from prior to publication.

If the intention is to obtain evidence of recognition from the dissemination of CCTV images, it is important that the correct procedures are adhered to. See **7.4.4 Obtaining Recognition Evidence from Witnesses.**

7.2.1 Dissemination to Police Personnel

There are several ways in which police personnel may view CCTV images for recognition purposes. The first is via a mass circulation of images, for example, on the force intranet. A second (much less common) method includes group viewings of images, for example, at briefings (see **7.4.5 Group Viewing of CCTV Images**). In addition, an investigator may ask staff to view images if it is believed that they may have information regarding the identity of the person portrayed in the footage. This information may, for example, be based on personal dealings with the suspect or with previous investigations carried out in that particular area.

7.2.2 Dissemination to External Partners

Depending on the offence under investigation, circulating images to police partners, such as those shown below, may assist.

- Members of Community Safety Partnerships (CSPs), formerly known as Crime and Disorder Reduction Partnerships (CDRPs), such as:
  - Police and criminal justice agencies;
  - Council services;
  - Children and young people's agencies;
  - Health services;
  - Community and voluntary sector;
  - Neighbourhood Watch;
  - Local authority control rooms.
- Other law enforcement agencies, such as:
  - UK Border Agency;
  - HM Revenue and Customs.

Using publications such as the Police Gazette to disseminate images to the police and police partners is also a useful method.

7.2.3 Dissemination to Covert Human Intelligence Sources (CHIS)

In some circumstances it may be necessary to allow a CHIS to view a still image or section of CCTV footage. Investigators will need to follow force procedures and liaise with the designated force officer or authorising officer. For further information see ***ACPO, HMRC and SOCA (2009) Guidance on the Lawful and Effective Use of Covert Techniques – Legal Framework and Covert Operational Management*** **[RESTRICTED]** and ***ACPO (2009) Guidance on the Lawful and Effective Use of Covert Techniques - Local Volume Crime and Disorder*** **[RESTRICTED].**

7.2.4 Poster Campaigns

Before a poster campaign is launched, investigators should carefully consider the information to include. No information should be included that could jeopardise a fair trial or violate the human rights of the individuals in the images. There must be a legitimate purpose, which is necessary and proportionate, to release an image. The way in which it is released must also be proportionate. The more serious the offence, the easier it will be to justify the way it is released, but if, for example, it is in relation to an incident of anti-social behaviour or to identify a group of underage drinkers, this may not be seen as proportionate. ***ACPO (2009) Guidance on the Release of Images of Suspects and Defendants*** recommends that, even for relatively minor offences, the release of an image can still be proportionate if one of the following is present:

- National interest;
- Vulnerable victims;
- Prevalent local crime;
- Community interest.

There are several benefits to a poster campaign. It publicises to criminals that CCTV is monitored. This is particularly relevant if, for example, posters are put up in the shopping centre where the offence took place. In addition, it shows offenders that there is a consequence to their actions. This can be most effective if posters are displayed in places where they are likely to be seen by offenders, including fingerprint rooms and cells within police stations. A poster campaign also helps build public confidence, highlighting that the police are working hard to fight crime.

In order to prevent posters remaining on display indefinitely, it is good practice to include a date (eg, in three month's time) on the poster to indicate when it should be removed, either by the person(s) displaying

the poster on behalf of the police or by local officers on patrol.

7.2.5 Dissemination to the Media

When deciding whether an image should be released to the media, the considerations outlined in **7.2.4 Poster Campaigns** are relevant. The same points will need to be considered to ensure that the release of images complies with the law. The extent of the coverage required will depend on the circumstances of the offence. There are, however, many options available to investigators who wish to circulate images to the media and the public at large. The following is a list of possibilities:

- Local and national newspapers;
- Local, national and international news;
- Force website;
- Crimestoppers Most Wanted;
- Crimewatch.

If the investigator decides to use a blanket poster/media approach to seek recognition of an unknown suspect, they will need to plan and implement a coordinated approach comprising circulation to internal and related bodies, and public dissemination tools, including Crimestoppers Most Wanted.

7.3 Third-Party Images

Whichever method(s) investigators prefer to use, they should be aware of the rights of third parties depicted in the footage before any images are released. Images of both third parties and VRMs are considered personal data under the DPA. In addition, diclosure of third-party images may violate their right to respect for private and family life as set down in Article 8 of the European Convention on Human Rights. It is advised, therefore, that before any images are released, images of third parties and other personal data are blurred out. This is something that the FTCS should be able to assist with.

7.4 Identification Versus Recognition

An eyewitness identifying an offender is often the turning point in an investigation, forming an important element of a prosecution's case.

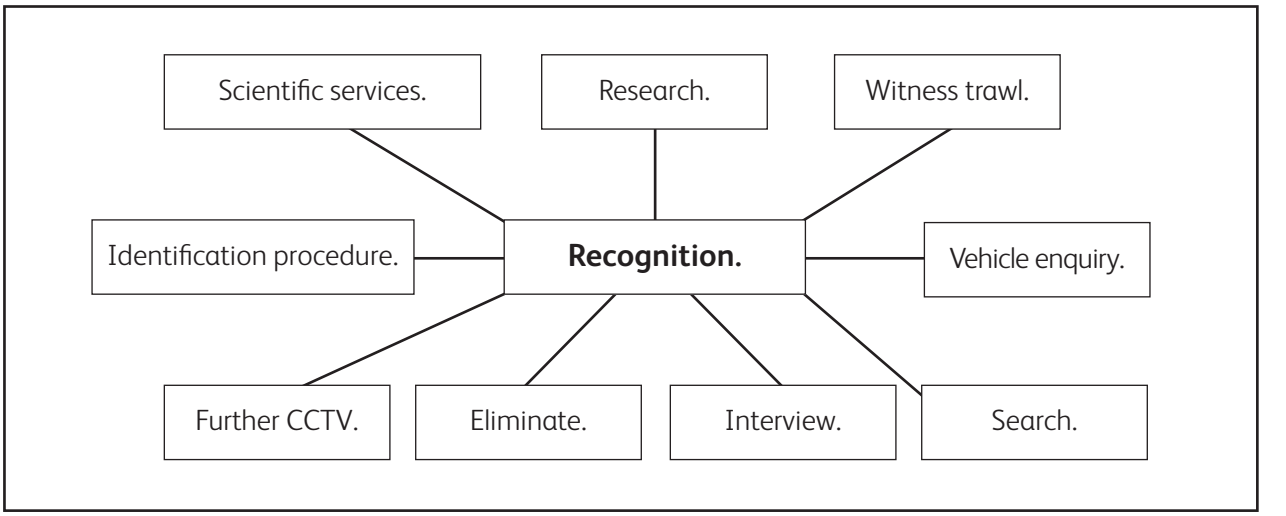
There can be confusion about the difference between recognition and identification. Although the main aim of disseminating CCTV images is to identify an offender, **identification** is actually a formal legal procedure that draws on a combination of established procedures. This includes the use of competent eyewitnesses, who are likely to become key witnesses for the prosecution. It tests their ability to identify a person suspected of committing the offence under investigation as the person they saw on a previous occasion, through the use of an identity parade, video identification or similar procedure.

Recognition is where someone who is not an eyewitness to the offence

under investigation claims to recognise someone depicted in an image who is well known to them. This is usually what investigators are hoping to achieve through circulation of CCTV images. See **7.1 Ways in Which CCTV Can Assist an Investigation.**

A successful suspect recognition process can trigger other investigative options for investigators. They can then gather a chain of evidence (see **Figure 7)** leading to, and in support of, the formal identification procedure. In the absence of other supporting evidence, evidence of recognition in itself can be adduced in evidence providing it is gathered in a robust manner that is open to scrutiny.

Figure 7 – Recognition Triggers



Where a suspect is recognised by a member of the public, following a poster campaign, the investigator can search national, regional and local databases for any intelligence or information already held on that subject. This in turn can trigger the Trace Interview Eliminate (TIE) process. It may also point the investigator to forensic or scientific evidence, or lead to additional, corroborating CCTV material. All of this will help to bring the investigation to the formal identification procedures. Evidential material pertaining to the identification, or recognition, of a suspect is considered to be very valuable by the courts, but the integrity of the process by which it has been produced must be robust and withstand the tests and scrutiny that it will need to undergo in order for the courts to accept it.

R v Smith and others [2008] EWCA Crim 1342 illustrates recognition, see **Appendix 2.** For a full explanation of identification procedures, see PACE (1984) Code D.

7.4.1 Eyewitnesses

The eyewitness identification procedures in Part A of section 3 of Code D of PACE 1984 should not be used to test whether a witness can recognise a person as someone they know. In these cases, the procedures in Part B apply.

7.4.2 Suspect Is Known to the Police

Section 3 of Code D of PACE 1984, Identification by Witnesses, together with Annexes A and E, provides guidelines for conducting identification procedures.

If the identity of the suspect is known to the police, and the suspect is available to take part in a formal identification procedure, arrangements must be made in accordance with Code D of PACE 1984.

An eyewitness must not be shown photographs, including CCTV, computerised or artist's composite likenesses or pictures (including E-FIT images), prior to a formal identification procedure. It is essential that where there are images of the offender or a suspect, witnesses must not be able to see them or be given any other indication as to the suspect's identity before making a formal identification under Code D of PACE 1984. If the court learns that the attention of any one of the witnesses has been drawn to any images of the suspect before formal identification, it may consider the identification evidence unreliable, and exclude it on the basis that the witnesses might have been influenced by seeing the image.

7.4.3 Suspect Is not Known to the Police

Under certain circumstances, a victim may view CCTV footage providing that the suspect is unknown to the police. This is outlined in *R v Johnson* [1996] Crim LR 504, see **Appendix 2.** All other reasonable enquiries to identify the suspect must have been exhausted prior to a victim viewing the images.

When introducing CCTV footage to eyewitnesses, care must be taken to avoid allegations of contaminating the memory of the witnesses involved. Consequently, it is advised that eyewitnesses to an incident are **not** shown CCTV footage unless there is a real ambiguity that the investigating officer needs to clarify. This may be required should the victim need to point themselves out or if the offence location needs to be confirmed (for example, if the scene was crowded). If eyewitnesses are shown CCTV footage, the defence could argue that the witness is only remembering what they saw on the CCTV footage and not what they witnessed during the offence. If eyewitnesses are to be shown footage, this should be done after they have made their initial witness statement, and a record subsequently made of that viewing.

R v Johnson [1996] Crim LR 504: Identifying an offender from CCTV footage

There is a distinction between showing video film to individuals or groups in order to try to establish the name of an offender, eg, using television's Crimestoppers and Crimewatch videos, and using a video as part of a formal identification procedure where the suspect is known. See **Appendix 2.**

7.4.4 Obtaining Recognition Evidence from Witnesses

In the absence of any eyewitness evidence, for example if the victim did not see the offender's face but it was captured on CCTV, recognition evidence from any non-eyewitnesses via television images may be used. When staff view CCTV footage or stills in an attempt to recognise an individual on the images, it is critical that the correct procedures are followed.

When CCTV is shown for the purposes of obtaining evidence of recognition, the procedures in Part B of section 3 of Code D of PACE, Evidence of Recognition by Showing Films, Photographs and Other Images, will apply when any person, including a police officer:

(a) Views the image of an individual in a film, photograph or any other visual medium;

(b) Is asked whether they recognise that individual as someone who is known to them (paragraph 3.34 of Code D of PACE 1984).

The footage must be shown on an individual basis in order to avoid any suggestion of collusion or influence. A record of the circumstances and conditions under which the person is given an opportunity to recognise the individual must also be made.

That record, as set down in paragraph 3.36 of Code D of PACE 1984, must include the following:

- Whether the person knew or was given information concerning the name or identity of any suspect;
- What the person has been told before the viewing about the offence, the person(s) depicted in the images or the offender and by whom;
- How and by whom the witness was asked to view the image or look at the individual;
- Whether the viewing was alone or with others and, if with others, the reason for it;

- The arrangements under which the person viewed the film or saw the individual and by whom those arrangements were made;
- Whether the viewing of any images was arranged as part of a mass circulation to the police and the public or for selected persons;
- The date, time and place images were viewed or further viewed or the individual was seen;
- The times between which the images were viewed or the individual was seen;
- How the viewing of images or sighting of the individual was controlled and by whom;
- Whether the person was familiar with the location shown in any images or the place where they saw the individual and, if so, why;
- Whether or not on this occasion, the person claims to recognise any image shown, or any individual seen, as being someone known to them, and if they do:
  - The reason;
  - The words of recognition;
  - Any expressions of doubt;
  - What features of the image or the individual triggered the recognition.

As per paragraph 3.37 of Code D of PACE 1984, the record may be made by:

- The person who views the image or sees the individual and makes the recognition;
- The officer or police staff member who is in charge of showing the images to the person or is in charge of the conditions under which the person sees the individual.

The admissibility and value of evidence of recognition obtained when carrying out the procedures in Part B may be compromised if, before the person is recognised, the witness who has claimed to know them is given or is made, or becomes aware of, information about the person which was not previously known to them personally but which they have purported to rely on to support their claim that the person is in fact known to them.

One method of disseminating CCTV images to staff is by putting images on the force intranet. It is advisable that staff viewing the footage or stills do so individually to avoid collusion.

The intranet page displaying images should not have the capacity to allow staff to save or remove footage or stills. If this capacity is not disabled, investigators must not make copies of the images or email them to colleagues. These measures will help to maintain the integrity of any recognition made.

7.4.5 Group Viewing of CCTV Images

In some rare instances, it may be necessary to conduct group viewings of images, such as during briefings. However, this is not considered good practice if the intention is to obtain evidence of recognition (*R v Caldwell and Dixon* [1994] 99 Cr App R 73). Images that are shown in this manner may be in relation to matters of immediate officer safety, for example, where it is impractical for every officer to check the force intranet or their email account before leaving the station. The officer in charge of showing the images should put safeguards in place in the event of a recognition by one or more of the group, ie, officers put their hands up and are spoken to outside the briefing.

> *R v Caldwell and Dixon* [1994] 99 Cr App R 73 and *R v Johnson* [1996] Crim. LR 504
>
> Identifying an offender from CCTV footage.
>
> Ensure that evidence is regulated so that identification is, as much as possible, spontaneous and independent. For full details see **Appendix 2.**

This method of showing images is a last resort and other means should be sought on a routine basis. If showing images to a group of staff is unavoidable, it is unlikely that any subsequent recognition could be used as evidence, although it could still be used for intelligence purposes.

7.4.6 Controlled Viewing of CCTV Following a Request from an Investigating Officer

If a controlled viewing is to take place, staff requested to take part must view the images alone. The viewing should be overseen by an individual of the rank of sergeant or above with no direct involvement in the investigation. During the procedure, a record of the information outlined in **7.4.4 Obtaining Recogition Evidence from Witnesses** should be made as soon as is practicable, even if there is no recognition made. In investigations into serious crime, consideration should be given to videoing the procedure. This will ensure greater transparency.

It should be noted that when an officer recognises a suspect from any of the recognition procedures outlined previously, they do not become

eyewitnesses to the offence. Accordingly, the law does not require that officer to take part in any further Code D identification procedure.

7.5 Specialist Methods Used to Identify Suspects

For further information on specialist identification techniques, including facial recognition, gait analysis, height measurement and facial or other image comparison, contact the force forensic services or the NPIA Specialist Operations Centre, telephone: 0845 000 5463.

Before speaking to any outside agency or company, investigators should liaise with their FTCS to discuss what is required from the CCTV evidence, as the FTCS may be able to suggest other in force methods to achieve the same result. If an outside agency or company is consulted, their understanding of CCTV should be clarified first. For example, CCTV imagery is sent to an external expert in facial and body morphology. A large and detailed report is completed, but an edited, re-encoded copy of the CCTV material has been used to produce the findings. Although an expert in the human structure, this person was not an expert in CCTV and, as such, if their evidence had been used, all findings could have been inadmissable. The re-encoded copy had changed the pixel make-up of the image so all measurements were inaccurate.

7.6 Research and Intelligence to Confirm the Identity of an Individual

Once circulation of images has produced the name of a suspect(s), the suspect(s) details should be compared with other sources of intelligence in order to gather supporting evidence before arrest. This could include the custody photograph of the individual, address, previous convictions, and where and with whom they associate. The information may be obtained from the force intelligence system.

Once sufficient intelligence or evidence relating to the released images has been gathered or an arrest has been made and the person identified, the images must be removed from public view. Consideration may be given to re-releasing them if necessary.

7.7 The Use of Social Networking Sites

Social networking sites can also be used as a tool to help confirm the identify of an individual. Websites such as Facebook allow users to post photographs of themselves on their profile page. Some users have an open account whereby anybody on the site can access their personal details and photographs. Names suggested as potential matches to CCTV images may be compared with uploaded images. It is also possible that potential suspects are wearing the same clothing as worn at the time of the offence. This is particularly useful if the clothing seen on the footage is very distinctive. Photographs and names may also help to identify co-offenders or potential witnesses. If any relevant information is identified, investigators should contact the FTCS for advice on how to retrieve the images.

In making use of these resources, investigators will need to ensure they do not breach relevant legislation such as the DPA (see **2.2 The Data Protection Act 1998**). Where forces have their own policies and procedures, investigators will need to follow these accordingly.

8

Introducing CCTV Images During Interview

This section explains how to use CCTV footage during suspect interviews, including the preparation required.

Contents

8.1 Preparation before the Interview

Before interviewing a suspect, the following steps should be considered. Alongside this, it is also good practice to consult force interview specialists, such as Tier 3 interviewers and major incident teams.

If an investigator intends to introduce CCTV into a suspect interview, it should form part of the interview plan and structure. This will, in turn, determine the reasons why the footage is to be shown and at what point in the interview it should be presented to the suspect.

8.1.1 The Use of Working Copies in the Interview

The master copy of the footage should not be played in an interview (see **4 Post Retrieval**). Instead, a working copy should be played to suspects or witnesses. It should be checked beforehand to make sure that the working copy is of a similar quality to that of the master copy. For further information see **4 Post Retrieval, 4.1 The Creation of Master and Working Copies** and **4.3 Sending Footage to the FTCS for Editing.**

If poor-quality images are shown to a suspect, it may encourage them to deny participation, in the belief that the CCTV material will not prove their involvement. Every effort should, therefore, be made to get the best quality image possible. If an investigator does discover a discernible difference between the two copies, they should contact the FTCS for advice.

Alternatively, still images may be used in an interview. These can be quicker to present and more easily produced by the investigator as they do not require specialist input.

8.1.2 The Use of Compilation Discs

Depending on the type of offence, the number of sources and the amount of relevant footage that needs to be shown, it may be helpful to produce a compilation disc. This will be an edited version of the master or working copy, which is short and to the point, and shows the footage the investigator wishes the suspect or witness to view. The master or working copy of the footage should be retained in its original format and be readily available for viewing by any party if requested.

It is important that investigators ensure that the strength of the evidence in the footage included on the compilation disc is not misrepresented. This means that the evidence should be portrayed fairly and not edited in such a way as to give the impression that it is more compelling than it really is.

Forces will have different policies and procedures for compilation discs and investigators are advised to refer to these. Whoever produces the compilation discs will require clear instructions on what will be required in the interview. They should be given an edit list containing the following information:

- Exhibit number;
- Relevant camera number;
- Start and finish times of each edit, including hours, minutes and seconds;
- Software used to view the footage.

Depending on the images available in the original footage, the compilation disc should ideally contain the following:

- Best available view of the suspect's face and clothing;
- Approach of victim and suspect;
- Offence taking place;
- Escape route;
- Any other relevant footage.

8.1.3 The Use of Story Boards

Bound or individual images (correctly referenced and exhibited) may be shown to the suspect during the interview. These story boards could show specific events or the lead up to them. They are also referred to as an album or book of photographic stills and can be used for court presentations. See **9.4 Basic Court Presentation.** It is also possible to use digital image portfolios and image charts, which are digital files replayable on a computer or other digital playback device.

8.2 Preparation of the Interview Room

Investigators should check that all the relevant recording and/or playing equipment is available and in working order prior to the interview. It is essential that:

- The material plays on the equipment available;
- The video/DVD player can be fast forwarded and rewound using the remote control;
- The disc or tape is ready to play at the correct place;
- The screen can be clearly seen by the people who will be present during the interview.

Ensuring that the relevant equipment has been prepared will help investigators to make the most impact with the CCTV footage.

8.3 Introducing CCTV Images to Suspects during the Interview

There are several reasons why investigators may wish to introduce CCTV to suspects during the interview and these include:

- As the basis for direct questions to the suspect, eg, is that you? Where is that garment you are wearing? Did you do that? Who is that person?
- The footage could be used during the challenge stage of the interview to highlight that the suspect's account differs from that portrayed in the CCTV.
- It may help a suspect to prove their lack of involvement in the offence at an early stage, thereby enabling officers to pursue other lines of enquiry.

8.3.1 Pre-Interview Disclosure

The investigating officer may find it beneficial to allow the suspect's solicitor to view the CCTV before the interview. If this is to be done, one method that could be considered is to show the solicitor the footage with the detainee present. Investigators should add the following to the pre-interview briefing:

> This is not an interview. I will not be asking your client questions or inviting comment from them. I remind them, however, that they are still under caution and any comments they make are being recorded and may be classed as significant. Any significant comments made will be dealt with as such at the commencement of the interview that follows this briefing.

The benefit of using this method is that the investigator is not then reliant on the solicitor to represent the footage accurately to the suspect. Furthermore, it will avoid requests by the solicitor to view the footage with their client during consultation.

8.3.2 Introducing the Footage

Once an investigator is ready to show the images to a suspect, an introduction to the footage should be given. The introduction should contain the exhibit number of the footage and the invitation for the suspect to view the images or stills. The decision to offer any further information or explanation of the footage rests with the interviewing officer and will depend on the circumstances of the case and the investigator's interview plan.

Investigators can invite the suspect to comment on the images either during or after playing the footage. Any questions investigators may wish to ask should link in to their overall interview strategy and any other relevant material or evidence. After the initial viewing of the CCTV, suspects and their solicitors should be given the opportunity to view all or any part of the footage again should they wish to do so.

9

Disclosure and Preparation of CCTV Footage for Court

After CCTV footage has been successfully located, retrieved and analysed, it can then be presented to the court. It is good practice for forces to have a Standard Operating Procedure (SOP) in place. Careful planning, preparation and efficient liaison with the court and legal teams will enable investigators to make the most impact with CCTV evidence. For example, prior to the use of CCTV in court, a professional exhibit, presented early to the defence, may result in a guilty plea and avoid the need for a trial. The following section provides guidelines on presenting footage effectively in court.

Contents

9.1 Disclosure

In addition to providing the defence with copies, or access to, material on which the prosecution case relies, the defence must also be given access to any material which might reasonably be considered capable of undermining the case for the prosecution, or supporting the case for the defence.

Every investigation should have a disclosure officer, whose primary responsibilities are to be the focus for enquiries, and to ensure that the investigator's disclosure responsibilities are complied with. In many cases the disclosure officer will be the officer in the case. All images should be subject to standard evidential processes which ensure that if an image is required by the criminal justice system, it is viewable and is accompanied by a full audit trail. In complex cases, the exhibits officer, if one is appointed, and the disclosure officer should have ready access to imaging specialists or experts who might be required to respond to more detailed enquiries.

The established procedure for developing a disclosure schedule (MG6 forms) records all relevant information, including digital image evidence relating to a case. The disclosure officer should complete the schedule and ensure that unused images are included. Overtly captured digital images should form part of the information recorded on the non-sensitive disclosure schedule. The schedule should provide a brief description of what is contained in the image or video sequence and any significant processing applied to it. A more detailed description of processes should only be provided if the image becomes an exhibit or is requested by the defence to form part of the defence case. The description of the unused image on the schedule should enable the prosecutor to make a decision about defence disclosure. For example, if an image has been substantially cropped, or only a selective area has been enhanced, it may be necessary for the schedule to state this so that the defence may be made aware of the availability of the uncropped and unadjusted images.

Access to, and disclosure of, digital images which become exhibits should be recorded in the audit trail and case papers when disclosed at police interview stage. At post-charge stage, access should only be allowed after agreement from the CPS. Any access to exhibits and unused material, including copies, should be restricted to those people who have a legitimate role in viewing the image. All access to the images should be documented as part of the audit trail that accompanies each image. All requests for disclosure of unused images should be recorded. Defence requests should be specific about exactly which images are required for viewing. For example, in the case of unused CCTV video sequences, the defence should be asked to specify the viewing period and the camera positions required. If disclosure of an unused image is facilitated, the following should be documented:

- The date and time at which disclosure was made;
- The identification of any third party to whom disclosure was made;
- The reason for disclosure;
- The extent of the information to which access was allowed, or that was disclosed.

For further information on disclosure see ***ACPO (2007) Practice Advice on Police Use of Digital Images*** and ***Attorney General (2005) Guidelines on Disclosure in Criminal Proceedings.***

9.2 Preparation before the Trial

The most important consideration for the preparation of footage for court is the equipment available in the court room. Courts may use antiquated technology for presenting CCTV footage. Unless the force is in a position to provide its own up-to-date equipment or to hire this from an appropriate source, investigators will need to find a suitable format in which to present the images.

Early contact with the court is recommended to ascertain the type of format that will be suitable and to allow as much time as possible to prepare. Some courts may allow investigators to bring in a laptop and plug it into a display screen. Other courts may only be equipped with a VHS player.

In most cases, DVDs will be the most accessible format for court. It should be noted, however, that there are different types of DVDs (data versus movie) and investigators should check that the one they intend to use for the trial works on the equipment available.

Whatever format investigators decide to use to present CCTV evidence, it is essential that they familiarise themselves with the relevant equipment before the trial.

9.3 Liaison

Once it is known what equipment is, or will be, available in the courtroom, investigators should liaise with the CPS to agree a suitable court presentation. Whatever type of presentation is decided on, investigators should ensure that it is flexible enough to have any piece of footage quickly removed without needing an entire re-edit. This ensures that if the judge decides to exclude a piece of footage from the trial, investigators are still able to present their remaining CCTV evidence.

9.4 Basic Court Presentation

In the case of minor offences, there may not be the need for an elaborate presentation of the CCTV footage. Some forces have developed their own software for court presentations and will provide their own guidance and training on this. For investigators from forces without such software, the FTCS can often help with the preparation of a DVD for the court presentation.

Only relevant footage that is to be presented in the trial needs to be included on the DVD. Liaising with the CPS will assist investigators in providing the appropriate footage for the prosecuting team. As long as the editing of earlier versions has been correctly audited and the master copy remains safely stored, there should be no problem with disclosure.

If it is not possible to present a DVD compilation, an exhibit book of photographic stills, also known as a story board, can be used. See **8.1.3 The Use of Story Boards.** Story boards often have narrative comments from the reviewer defining the actions or content of the specific imagery. If a book is to be used, it is recommended that the stills should be produced to a high-quality photograph printing standard to ensure that the quality is suitable for court.

9.5 Detailed Court Presentation

Depending on the scale of the trial and the type of offence, it may be necessary to provide a more detailed court presentation with, for example, graphs, charts, maps, stills and video clips. Liaising closely with the CPS and defence teams will ensure that whatever format is used, it will meet the needs of the legal representatives.

If a more detailed presentation is required, outside help may be necessary. In some forces, there are already technical or imaging teams that are able to provide assistance in presenting more complicated cases. For forces without such resources, it may be necessary to engage the assistance of a private company. Help on selecting a suitable CCTV practitioner can be sought from the NPIA Specialist Operations Centre, telephone: 0845 000 5463. It may also be helpful to contact other forces or the Centre for Applied Science and Technology (CAST) for advice or recommendations. However, if a more technical and detailed approach is taken, officers should ensure that the end product can be played on the facilities available at court.

Whatever method of presentation is chosen, it should be professional, practical, allow CCTV to be viewed in its best quality and, ideally, should appear in one product, ie, not on a variety of portable media with separate hand-held charts and graphs. The purpose of the presentation is to assist the jury in understanding the evidence, and forces should aim for clarity and simplicity. If the equipment or software required is particularly complicated, it is advised that a technician is available during the relevant part of the trial to help with the set up and presentation.

9.6 Post Trial

9.6.1. Feedback to Owners of CCTV

If a person has offered CCTV footage to the police and it has been considered as part of an investigation, investigators should provide feedback on the outcome of the investigation to the owners of the CCTV system. This may be a local authority, a business or a private

individual. Feedback can help to develop good working relationships with communities and can encourage CCTV owners to volunteer their footage should there be a need for this in the future.

Feedback can be of a formal or informal nature. In some cases, a quick telephone conversation may be adequate. If a local authority has offered CCTV footage, the National CCTV Strategy recommends that the feedback is of a more formal nature. One reason for this is that it will help to ensure that local authority control rooms continue to receive adequate funding. In turn, this then allows them to continue to assist the police with their investigations. Local authorities may provide investigators with their own feedback forms to complete. If this is not the case, an example of a formal feedback form that officers can use is given in **Appendix 6.**

10

Retention and Disposal

This section should be read in conjunction with existing legislation, force policy and force SOPs. The main pieces of governing legislation for retention and disposal are the Criminal Procedure and Investigations Act 1996 (CPIA) and *ACPO (2005) Code of Practice for the Management of Police Information.*

Contents

10.1 Retention

Retention refers to the continued storage of, and controlled access to, information held for a policing purpose, which has been justified through the evaluation and review process. After being used or disclosed, CCTV material may be retained but it can only be used or disclosed for the same purposes.

The Code of Practice issued under section 23(1) of the CPIA, see **2.4 Criminal Procedure and Investigations Act 1996,** includes in paragraph 5.9 a requirement to retain all material relevant to an investigation, at least until proceedings are completed and for the length of a custodial sentence or until discharge from hospital, or at least six months from the date of conviction. All material should also be retained in circumstances where an appeal against conviction is in progress or if the Criminal Cases Review is considering an application (paragraph 5.10). The CPIA retention timescales represent a minimum requirement for the retention of police information.

Decisions relating to the retention of images beyond the timescales set by the CPIA Code of Practice, eg, where a case is a specified serious offence under Chapter 5 section 224 of the Criminal Justice Act 2003, should be taken locally by the information or records management team. For long-term storage of CCTV evidence, see **5.2 Continuity Statements** and sections 3 and 4 of ***Home Office (2007) Storage, Replay and Disposal of Digital Evidential Images,* Publication Number 53/07** available from **http://tna.europarchive.org/20100413151426/http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/53_07_Storage_Replay_and_Di17ffe.html?view=Standard&pubID=504030**

CCTV footage that is incapable of having any impact on the case is neither evidential nor unused material and should normally be documented, then destroyed. It is not always easy to determine when material falls within this category. Decisions to release CCTV back to its owner, where later challenged by the defence following an abuse of process application, will be judged on the facts as they were reasonably known at the time of the decision.

Images associated with undetected crime should be retained according to management of police information principles. When retaining undetected crime records, consideration should be given to ensuring that they are easily retrievable and accessible for replay and viewing. An assessment of the possible value of the information to future cases should also be made.

For further information about retention, see PACE 1984 Code D, 3(f) Destruction and retention of photographs taken or used in eyewitness identification procedures, ***ACPO (2007) Practice Advice on Police Use of Digital Images*** and ***ACPO (2010) Guidance on the Management of Police Information,* Second Edition.**

10.2 Disposal

Disposal is the removal of information from all police systems so that it cannot be restored. In the case of images stored in IT systems, this means that no force staff should be able to locate an image or piece of information when carrying out their normal duties. Deletion should suffice, except in circumstances where information is judged to be extremely sensitive.

Images (and all negatives and copies), including those produced from CCTV material, which are taken for the purposes of, or in connection with, the identification procedures set out in PACE, must be destroyed unless the suspect:

(a) Is charged with, or informed they may be prosecuted for, a recordable offence;

(b) Is prosecuted for a recordable offence;

(c) Is cautioned for a recordable offence or given a warning or reprimand in accordance with the Crime and Disorder Act 1998 for a recordable offence; or

(d) Gives informed consent, in writing, for the photograph or images to be retained for policing purposes.

As per paragraph 3.31 of Code D of PACE 1984.

Appendix 1

Abbreviations and Acronyms

ACPO	Association of Chief Police Officers
ANPR	Automatic Number Plate Recognition
APP	Authorised Professional Practice
BST	British Standard Time
BTP	British Transport Police
CAST	Centre for Applied Science and Technology (previously known as Home Office Scientific Development Branch)
CCTV	Closed-Circuit Television
CDRP	Crime and Disorder Reduction Partnership (as of 1 April 2010, known as CSP)
CHIS	Covert Human Intelligence Source
CPIA	Criminal Procedure and Investigations Act 1996
CPO	Crime Prevention Officer
CPS	Crown Prosecution Service
CRO	Crime Reduction Officer
CSP	Community Safety Partnership (previously known as CDRP)
DAT	Digital Audio Tape
DNA	Deoxyribonucleic Acid
DPA	Data Protection Act
DVR	Digital Video Recorder
ECHR	European Convention on Human Rights
E-FIT™	Electronic Facial Identification Technique
EHRR	European Human Rights Reports
FTCS	Force Technical CCTV Specialist
GMT	Greenwich Mean Time
HDD	Hard Disk Drive

HMRC	HM Revenue and Customs
HOSDB	Home Office Scientific Development Branch (as of 1 April 2011 known as CAST)
HRA	Human Rights Act 1998
HSE	Health and Safety Executive
IPLDP	Initial Police Learning Development Programme (Probationer Training)
LA	Local Authority
MOPI	Management of Police Information
NPIA	National Policing Improvement Agency
NVR	Network Video Recorder
PACE	Police and Criminal Evidence Act 1984
PIP	Professionalising Investigation Programme
RIPA	Regulation of Investigatory Powers Act 2000
SIO	Senior Investigating Officer
SOCPA	Serious Organised Crime and Police Act 2005
SOP	Standard Operating Procedure
TIE	Trace, Interview and Eliminate
USB	Universal Serial Bus
VRM	Vehicle Registration Mark
WORM	Write Once, Read Many

Appendix 2

Relevant Case Law

***R v Caldwell and Dixon* [1993] 99 Cr App R 73: Identifying an offender from CCTV footage**

A group of police officers in a police station identified, from a security video camera, some individuals carrying out an armed robbery. On appeal it was argued that such evidence should have been excluded because a proper procedure was not followed.

The appeals against conviction were dismissed.

This type of evidence should be regulated to maximise the prospects of any recognition evidence being spontaneous and independent. **Note:** Evidence which is unfair may be excluded under section 78 of PACE 1984 at the discretion of the trial judge.

***R v Smith and others* [2009] 1 Cr App R 36: Requirements where a police officer makes an identification from CCTV images**

During an unsuccessful attempt by a gang of men to enter a nightclub, one of the group fired a shot, followed shortly after by a further thirteen gun shots, which killed one of the doormen at the club and injured three others. The group then made their escape in cars but were eventually arrested and charged with murder and attempted murder.

The case involved issues surrounding the actions of other members of the group acting in a manner which was not expected, and evidence relating to assertions that some members were not present. However, the issue that is of most concern for the present purposes relates to the identification of one of the group, Christie, made by a police officer from CCTV images.

Christie argued that the evidence that he had been present at the incident by way of identification by a police officer from CCTV images had been in breach of Code D of the Codes of Practice that accompany the Police and Criminal Evidence Act 1984 (PACE) because no record had been kept of the officer's initial recognition of him.

Appeals dismissed. Convictions upheld.

Where a police officer views a CCTV recording or image, there is a difference in comparison with an ordinary witness viewing the same to identify someone seen committing an offence. Code D provides safeguards that are equally important where a police officer has been asked to attempt to identify someone from a CCTV recording.

Regardless of whether Code D applies, a record must be made of the following:

(i) Any initial reactions to seeing the CCTV images;

(ii) Where a police officer fails to recognise anyone on the initial viewing but does so at a later date;

(iii) Where a police officer fails to recognise anyone at all;

(iv) Anything that an officer may say with regard to any doubt;

(v) Where there is recognition, any factors relating to the image that caused that recognition to occur.

The record must be available to assist in measuring the reliability of the claim that a police officer recognises a particular individual. In addition, it is important that any initial reactions are made available for examination as required.

***R v Chaney* [2009] 1 Cr App R 35: Identification from CCTV images by way of recognition not breach Code D**

C was accused of theft, firearms-related offences and driving while disqualified. There was CCTV evidence of an incident that resulted in these accusations. A police officer who was not a party to the investigation but knew C in relation to another unrelated matter received an email consisting of still images from the CCTV footage. The police officer was asked to provide his thoughts regarding the fact that other officers believed the man in the images was C. The police officer replied that he was able to identify C. The police officer also found out the registration number of the car, also in the images, and on checking found it to be registered to C, but the police officer knew that C was, at the time, disqualified from driving. The police officer did not make any statements at the time on any of these matters.

At trial, a question arose as to whether the person in the CCTV images was C and evidence from the police officer was admitted. C was convicted and appealed arguing:

(i) The purported identification by the police officer was procedurally flawed and unfair;

(ii) The evidence was more prejudicial than probative and its admission in evidence at trial rendered the conviction unsafe;

(iii) The trial judge, having allowed the identification in evidence, failed adequately to warn the jury of the 'special need for caution' in cases which rest on identification evidence, and to outline breaches of the principles of Code D and the significance of those breaches;

(iv) The judge failed properly to deal in his directions with the issue of lack of identification parades in respect of other eyewitnesses, which added to the 'unsafeness' of the conviction.

Appeal dismissed. Conviction upheld.

Code D was not directly applicable in this instance in line with the case of *R v Smith* [2009] 1 Cr App R 36 and guidance given following that case. The jury had the police officer's reaction and what he had said in his printed response to the email. That response had not been created in contemplation of him giving evidence, so there was nothing to suggest that his reaction was anything other than spontaneous and genuine. On this basis, the judge had been correct in admitting the evidence. The jury had been in full knowledge of all the circumstances surrounding the recognition and the judge had made it clear that the issue was identification and the police officer's evidence had been fully summarised for them.

This case was one of recognition rather than identification and the judge should have warned the jury of the requirement for care to be taken. However, there was other evidence in this case that was overwhelming and the principle piece of evidence that identified him was his car. There was also other evidence to link him to the theft.

***R v Johnson* [1996] Crim. LR 504: Identifying an offender from CCTV footage**

J was a suspect for two robberies. Just after the second robbery, J and another woman had been caught on a video security camera standing near the scene of the attack. The victim was shown the video after J had become a firm suspect (it is not clear from the report if the video was shown before or after J's arrest, but that is not relevant). The victim picked out J as one of her attackers.

J was subsequently convicted of this offence, but appealed on the grounds that the evidence of the video identification should have been excluded by the trial judge under section 78 of the Police and Criminal Evidence Act 1984.

Appeal allowed in part. Conviction for robbery quashed.

There is a distinction between showing video film to various individuals/groups in order to try and establish the name of an offender, such as with television's Crimestoppers and Crimewatch videos, and using a video as part of a formal identification procedure where the suspect is known.

The purpose, in these particular circumstances, for showing the witness the video was so that the victim could say, 'Yes that was the woman who attacked me'. It was almost identical to a one-to-one confrontation identification, but performed by video.

Once the police have found a definite suspect, Code D states that the procedures in Code D must be followed if the suspect disputes that they were the person involved and there are appropriate eyewitnesses

available. The first step is normally the appointment of an identification officer and the subsequent offering of a parade to a suspect (long before a confrontation could be considered).

J had not been given an opportunity to stand on an identification parade and the identification methods used were flawed. Such evidence should have been excluded at the original trial.

The Appeal Court appears to have considered the police action in this case to be a confrontation by video. The judgment would appear to suggest that if the proper procedures laid down in Code D had been followed then the confrontation by video would have been acceptable.

There may be occasions where such a procedure could be useful. For example, a suspect, who is not being kept in custody, agrees to a parade, but flees the country. Rather than wait several months or even years to hold some form of identification procedure, a 'confrontation by video' using a security videotape could be an identification officer's best choice if he is concerned about the witness's memory fading. However, confrontation evidence is not given a great deal of weight by the courts.

Another aspect of this case worth considering is whether the video could be used to show the suspect's close proximity to the scene. The relatively new requirement for a suspect to account for their presence in a suspicious place (under section 37 of the Criminal Justice and Public Order Act 1994) would now put her in a difficult position at court if no explanation was forthcoming.

R v Smith [2005] EWCA Crim 3375: Identifying an offender from CCTV footage

A man (S) went into a florist where the victim (V) was working alone one afternoon in January 2004. S was holding a knife and told the victim to open the till, she did so and he took the money from it (£45). He left the shop but V did not see where he went.

V had a very good view of S. Ten minutes later she gave a detailed description to the officers who attended her call to them. The officers made enquiries nearby and the manager of a nearby shop stated that he had seen a man fitting the description some thirty to forty minutes earlier. He produced a CCTV tape on which V later identified S again, from a full frontal image. This identification was made within half to three-quarters of an hour after the incident. V gave a statement to the police some six days later but her description this time differed slightly.

S was arrested but refused to answer any questions in interview. He gave evidence at the trial and admitted that he had been in the other shop but not the florists.

During the investigation, a police inspector wanted to carry out a video identification parade. S had refused to leave his cell, although at trial he claimed that he had never been asked (this was dismissed by the judge). The inspector treated this as a refusal to take part in the video parade. Later that day V viewed a video parade using a still image of S and identified S. Evidence of this identification procedure was subsequently not admitted at trial and so the jury did not hear it.

S was convicted at trial and appealed. The conviction was quashed.

V's identification evidence was poor and unsupported with several discrepancies between the descriptions given and the facts accepted and/or established at trial. Her evidence was not supported by any independent evidence, such as fingerprint evidence or a knife found. The defence pointed out that there was good lighting in the shop and that V was close to S. There was some evidence to support the claims in the corroboration of the other shopkeeper and S himself accepted that he had been in the vicinity for a short time.

Of most concern was the way in which the CCTV identification was made. When V viewed the tape, it focused on the image showing S. V's attention was directed only to him and this could have been avoided.

The combination of V being told that the police had CCTV footage of someone fitting the description she had given and her being invited to look at only S's image made the basis of the conviction unsafe.

The court suggested that it would have been more acceptable if the witness had viewed the CCTV footage at greater length so that other people could be viewed as well. PACE Code D paragraph 3.2 states in (b) that the attention of the witness must not be directed to any individual. In addition, the police should avoid saying that the CCTV footage contains an image of someone matching the witness description.

R v Clare; R v Peach [1995] 2 Cr App Rep 333: Interpreting CCTV evidence

Football supporters were filmed and photographed as they entered the stadium. After the match, there was a violent incident involving a number of supporters and members of the public. The incident was recorded on video recorders attached to buildings. On the basis of what could be seen, two men were charged with violent disorder.

At their trial the court allowed PC Fitzpatrick to give evidence. He had used colour photographs and film taken before and during the match and compared it with black and white videotape, in order to analyse what was going on, where violent incidents were taking place and who was involved.

Both C and P were convicted but appealed on the grounds that the videotape should have been shown to the jury without the explanations given by the officer, as he did not know the defendants personally and was not an expert witness.

The appeal was dismissed.

The officer had developed special knowledge, which the jury did not possess, by carefully analysing the video material and photographs. He and a colleague had studied images so that they knew what individuals looked like and what they were wearing on the day. It would have been impractical to give the jury the time to complete the same research. The officer was open to cross-examination and the jury could choose to accept or reject the evidence. It was, therefore, legitimate to allow the officer to assist the jury by pointing to what he asserted was happening in the crowded scenes on the tape.

Taylor v Chief Constable of Cheshire [1986] 1 WLR 1479: When CCTV footage is lost

A recording was made in WH Smith of a man allegedly putting a packet of batteries into his back pocket. He then turned and glanced straight at the camera and walked off. The alleged theft was seen live on a CCTV screen by a store security officer, who immediately showed a recording of the incident to the store manager. Thirty minutes later it was shown to two police officers who both identified Taylor as the offender. A few weeks later, another police officer also identified Taylor from the tape. The recording was taken to Runcorn police station to be shown to the appellant's solicitor, but the video did not work on the police video recorder and so was sent back to WH Smith. Arrangements were made for the solicitor to view the footage, who formed the opinion that no offence had taken place and that it was not clear that the appellant was depicted.

The tape was left at the store to be kept safe but it was accidentally erased by new security staff before the trial when it was to be shown to the magistrates.

Taylor was convicted but then appealed on the grounds that what the officers claimed to have seen on the videotape was hearsay and should have been ruled as inadmissible.

The appeal was dismissed.

Oral evidence given by a witness as to what they have seen on a video recording, which is not produced to the court, should be treated as direct evidence of what was believed to be seen in a particular place at a particular time. There is effectively no distinction between witnessing an event in person and viewing that event on a CCTV screen.

If the recording itself is not produced, the weight and reliability attached to that oral evidence will depend on factors, such as the length and clarity of the recording, and how many times it was viewed by the witness. In this case, there was other relevant information, for example, the appellant admitted being in the place where the incident happened at the time of the incident. The guidelines laid out in *R v Turnbull* [1977] QB 224 will apply if there is uncertainty about the identity of an individual.

***R v Rosenberg* [2006] EWCA Crim 6: Use of footage recorded by others**

R was caught on a private CCTV camera belonging to her neighbours. R and her neighbours, Mr and Mrs Brewer, did not get on and R was aware that a camera was pointed at her house. Mr Brewer had told the police about the video camera and had been warned that it was a violation of R's privacy, but the police had taken the videotapes when they were offered. The appellant knew that the Brewers' camera was recording events happening in the house.

Following reports from Mr Brewer, the police attended R's property in January 2004 where they found a quantity of drugs and money which R claimed were not hers. R was interviewed twice that evening with her solicitor before finding out that the police had the CCTV footage. The footage showed her apparently unwrapping packets of drugs, handing objects to others and being shown how to use a 'crack bottle'. She was then interviewed again.

At trial the defence tried to have the video evidence excluded, arguing that the surveillance had been directed by the police and this was in breach of the Regulation of Investigatory Powers Act 2000 (RIPA). They also argued that the police had failed to inform R that her property was being watched. They asked that the evidence should be excluded under section 78 of PACE.

The trial judge ruled that the police had not breached RIPA. The defence appealed but the conviction and sentence were upheld.

The police knew surveillance was being carried out and were prepared to use it as evidence, but it could not be regarded as police surveillance because the police neither initiated nor encouraged it. It was, however, accepted that the degree of police involvement could be a factor in deciding whether to exclude evidence under section 78 of PACE.

Section 26 of RIPA was not breached because the surveillance was not covert. The camera was visible and R knew it was recording.

Even if there had been a breach of the Human Rights Act 1998, Article 8, the police could have relied on the proviso in the Article that it was necessary for the prevention of crime.

R's interview statements should be admitted as she was told what the nature of the case was against her.

R's house had been searched and incriminating evidence found, but the police at the interview stage were not obliged to disclose the whole of the case and the evidence they held against her. Even if the police should have disclosed the videos prior to the first interview, that was not grounds for excluding the interviews.

Appendix 3

Sample Request for Disclosure of Personal Data Template (Under DPA Section 29(3))

To: ..... Force Details: .....

Data Protection Act 1998 – Request for Disclosure of Personal Data Under Section 29(3) of the Data Protection Act 1998

In order to maintain police confidentiality, you are requested to treat this application as confidential.

I am making enquiries that are concerned with:

*(A) The prevention or detection of crime; *Delete as appropriate

*(B) The apprehension or prosecution of offenders.

Please provide the following recorded data/images CCTV or other recorded video footage/images for the time period(s):

.....

The data/images are necessary for investigating the offence of .....

.....

This section may be left blank due to the sensitivity of the investigation. Where this applies, this form should be signed by an officer of superintendent rank or above.

I can verify that the recorded data/images are required for the reason given above and that failure to disclose same would be likely to prejudice these matters.

I can confirm that to the best of my knowledge the information supplied herewith is complete and accurate.

Signed: ..... Rank: .....

Name (BLOCK CAPITALS): ..... Date: .....

Officer attending: ..... Collar number: .....

System registered under Data Protection: Y/N

If not please contact the Office of the Information Commissioner.

The Office of the Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK 9 5AF
Tel: 01625 545740

This form to be retained for a minimum of 5 years and attached to the case papers.

Appendix 4

Sample Retention Notice Template (Under SOCPA Section 66)

NOTICE UNDER S.66 SERIOUS ORGANISED CRIME AND POLICE ACT 2005

Crime ref no:	
Name (BLOCK CAPITALS):	DOB:
Address:	
I have been informed, and understand, that the below described property which is held by me is currently the subject of police enquiries. I have also been told, and understand, that this notice is not transferable and, if I dispose of the property subject of this notice, or alter it any material way, I may be liable to civil or criminal proceedings.	
Details of property:	

I acknowledge receipt of a copy of this form:

Signature: Date:

Issuing officer's signature:		Date:
Name (BLOCK CAPITALS):	Rank and No:	Tel no:

White Copy: Retained by OIC. If ownership is in dispute, forward to Legal Services with a WG401 outlining the circumstances relating to the issue.

Green Copy: For person(s) retaining the property.

Appendix 5

Sample Viewing Log Template

Relevant*	**Non-relevant***

*Delete as appropriate

Record of Viewing

Operation/Offence/Incident .....

Exhibit number including seal:	Address where found: Full postcode:
Description from exhibit sheet:	Viewing dates(s): Viewing times: Start: Finish:
Reviewing officer(s):	
Reason for reviewing: Action number:	
Total number of cameras: Cameras viewed: Time accuracy: (eg, one hour fast)	

Entry number:	Camera number/ Time:	Viewing notes:

Appendix 6

Sample Feedback Template

Officer Name ..... Date .....

Local Authority CCTV Control Room .....

Operation/Offence/Incident .....

To [Insert Local Authority CCTV Manager's Name]

Thank you for your assistance in the investigation into [insert operation/offence/incident] on [insert date]. This feedback form outlines the role the footage played in the investigation.

CCTV camera number..... Camera location .....

Was the CCTV Operator controlled or fixed/passive? *(Please delete)*

Was the CCTV real time or post event? *(Please delete)*

	YES	NO
Did the LA CCTV assist the investigation?		
If yes, in what area(s) did it assist?		
Intelligence gathering:		
Eliminating lines of enquiry:		
Proving a suspect's innocence:		
Identification of witnesses:		
Identification of vehicles:		
Clarification of disputed evidence:		
Creation of timeline of events:		
Other, please state:		
If no, why did the LA CCTV not assist the investigation?		
Images not relevant:		
Quality of images not good enough:		
CCTV did not cover the correct area:		
Poor camera work by CCTV operators:		
Poor-quality recordings:		
Product unable to be 'played back' by local police/CPS/defence:		
Other, please state:		
Did the LA CCTV play a role in the interviewing procedure?		
Did the LA CCTV play a role in a defendant deciding on their plea?		
Did the LA CCTV play a role in the court hearing?		

What was the final outcome of the case? .....

.....

Any other points/notes? .....

.....

Appendix 7

References

ACPO (2005) *Code of Practice on the Management of Police Information.* Wyboston: NCPE.

ACPO (2005) *Practice Advice on Core Investigative Doctrine.* Wyboston: NCPE.

ACPO (2007) *Good Practice Guide for Computer-based Electronic Evidence,* Official Release Version [Internet]. London: ACPO. Available from **http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf** [Accessed 10 June 2011]

ACPO (2007) *Practice Advice on Police Use of Digital Images.* London: NPIA.

ACPO (2009) *Guidance on the Lawful and Effective Use of Covert Techniques – Local Volume Crime and Disorder.* London: NPIA. [RESTRICTED]

ACPO (2009) *Guidance on the Release of Images of Suspects and Defendants.* London: ACPO.

ACPO (2009) *Practice Advice on the Management of Priority and Volume Crime (The Volume Crime Management Model),* Second Edition. London: NPIA.

ACPO (2010) *Guidance on the Management of Police Information,* Second Edition. London: NPIA

ACPO and Hampshire Constabulary (2009) *Manual of Guidance: Freedom of Information.* London: ACPO.

ACPO, HMRC and SOCA (2009) *Guidance on the Lawful and Effective Use of Covert Techniques – Legal Framework and Covert Operational Management*. London: NPIA. [RESTRICTED]

Attorney General (2005) *Guidelines on Disclosure in Criminal Proceedings* [Internet]. London: CPS. Available from **http://www.cps.gov.uk/legal/a_to_c/attorney_generals_guidelines_on_disclosure** [Accessed 10 June 2011]

British Transport Police (2009) *CCTV* [Internet]. London: British Transport Police. Available from **http://www.btp.police.uk/passengers/issues/cctv.aspx** [Accessed 10 June 2011]

Crimestoppers (2011) *Crimestoppers* [Internet]. Wallington: Crimestoppers. Available from **http://www.crimestoppers-uk.org** [Accessed 10 June 2011]

Crown Prosecution Service (1997) *Protection from Harassment Act* [Internet]. London: CPS. Available from **http://www.cps.gov.uk/legal/s_to_u/stalking_and_harassment/#a03a** [Accessed 08 August 2011]

Health and Safety Executive (2009) *Striking the balance between operational and health and safety duties in the Police Service* [Internet]. London: HSE. Available from **www.hse.gov.uk/services/police/duties.pdf** [Accessed 10 June 2011]

Home Office (1998) *Guidelines for the Handling of Video Tape*, Publication Number 21/98. London: HOSDB.

Home Office (2003) *Guidance on operating the new powers of seizure in Part ll of the Criminal Justice and Police Act 2001* [Internet]. Home Office Circular 019/23. Available from **http://www.homeoffice.gov.uk/about-us/home-office-circulars/circulars-2003/019-2003/** [Accessed 10 June 2011]

Home Office (2006) *Video Processing and Analysis Training and Reference Manual*. London: HOSDB.

Home Office (2007) *Digital Imaging Procedure*, Version 2.1 November 2007 58/07 [Internet]. London: HOSDB. Available from **http://tna.europarchive.org/20100413151426/http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/DIP_2.1_16-Apr-08_v2.3_(Web)47aa.html?view=Standard&pubID=555512** [Accessed 10 June 2011]

Home Office (2007) *Implementing a strategy for the identification, retrieval and evaluation of CCTV evidence in major investigations* [Internet]. London: HOSDB. Available from **http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/SIO_strategy_2-Nov-07_v1.0.pdf?view=Binary** [Accessed 10 June 2011]

Home Office (2007) *Storage, Replay and Disposal of Digital Evidential Images*, Publication Number *53/07* [Internet]. London: HOSDB. Available from **http://tna.europarchive.org/20100413151426/http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/53_07_Storage_Replay_and_Di17ffe.html?view=Standard&pubID=504030** [Accessed 10 June 2011]

Home Office (2008) *Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems*, Version 2.0 Publication Number 66-08 [Internet]. Available from **http://tna.europarchive.org/20100413151426/http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/66-08_Retrieval_of_Video_Ev12835.pdf?view=Binary** [Accessed 10 June 2011]

Home Office (2008) *The National CCTV Strategy* [Internet]. *London: Home Office Crime Reduction*. Available from **http://www.crimereduction.homeoffice.gov.uk/cctv/index.htm** [Accessed 10 June 2011]

Information Commissioner's Office (2008) *CCTV Code of Practice* [Internet]. London: ICO. Available from **http://www.ico.gov.uk/for_organisations/topic_specific_guides/cctv.aspx** [Accessed 10 June 2011]

NPIA (2006) *Automated Face Recognition Applications within Law Enforcement, Market and Technology Review October 2006* [Internet]. Wyboston: NPIA. Available from **http://www.npia.police.uk/en/docs/Face_Recognition_Report.pdf** [Accessed 10 June 2011]

NPIA (2007) *Police Standard for Still Digital Image Capture and Data Interchange of Facial/Mugshot and Scar, Mark and Tattoo Images*, Version 2.0. Wyboston: NPIA.

Office of Public Sector (2001) *Private Security Industry Act 2001* [Internet]. London: OPSI. Available from **http://www.opsi.gov.uk/ACTS/acts2001/ukpga_20010012_en_1#Legislation-Preamble** [Accessed 10 June 2011]

Reid, S. (2008) Crimewatch Explained, *The Journal of Homicide and Major Incident Investigation*, 4 (2). London: NPIA.

Wright, M. (2008) Focus On… Forensic Gait Analysis, *The Journal of Homicide and Major Incident Investigation*, 4 (1). London: NPIA.

Acts of Parliament

UNITED KINGDOM. Parliament. 1984. *Police and Criminal Evidence Act 1984*. London: TSO.

UNITED KINGDOM. Parliament. 1996. *Criminal Procedure and Investigations Act 1996*. London: TSO.

UNITED KINGDOM. Parliament. 1997. *Protection from Harassment Act 1997*. London: TSO.

UNITED KINGDOM. Parliament. 1998. *Data Protection Act 1998*. London: TSO.

UNITED KINGDOM. Parliament. 1998. *Human Rights Act 1998*. London: TSO.

UNITED KINGDOM. Parliament. 2000. *Freedom of Information Act 2000*. London: TSO.

UNITED KINGDOM. Parliament. 2002. *Police Reform Act 2002*. London: TSO.

UNITED KINGDOM. Parliament. 2003. *Criminal Justice Act 2003*. London: TSO.