Passive data generators

First published 23 October 2013 Updated 19 May 2020
Written by College of Policing
52 mins read

Passive data generators are automated systems that gather and collate information for purposes unconnected with criminal investigation, but can be accessed by investigators. Examples include:

- financial information
- CCTV
- other digital images
- computer-based electronic evidence
- telecommunications information
- customer information, including subscriber information

What distinguishes passive data generators from other types of record-keeping, such as patient records, is that they are automated and require no judgement on the part of the person making them. They are also stored in systems that require technical expertise to access them.

Material

General material

Passive data generators can be used to provide material that assists the investigating officer to understand the circumstances of a case. This is almost exclusively confined to:

- analysing a victim’s telephone activity with a view to identifying contacts
- locating, gathering and viewing images generated within particular areas for the purpose of identifying people and vehicles that may be significant to an investigation

Any material generated in this way may later become evidence when specific suspects are identified.

In the first instance, the objective is to set the parameters within which officers should search for this type of material.

Specific material

Passive data generators can assist when investigating officers are seeking material about specific circumstances relevant to an incident. This could include the:

- presence of victims, witnesses, suspects, vehicles or telephones at particular locations and the times they were there
- relationship between individuals
- times of contact between individuals
- lifestyles of individuals

Setting parameters

Unfocused enquiries are likely to generate a large quantity of data that has to be analysed in order to locate the specific material required. Setting parameters as tightly as possible is, therefore, essential when developing the objectives for these enquiries.

It is important to consider the types of passive data generator that may be useful in the particular circumstance of the case. Technical innovations mean that new passive data generating systems are continually becoming available and it is sometimes difficult to recognise when a certain lifestyle or activity has the potential to generate such data. Investigators should, therefore, consult those who are knowledgeable about the type of activity or lifestyle that is relevant in order to identify the opportunities that may exist.

Reviewing parameters

Given the high cost of implementing the passive data generator strategy, both in terms of the costs imposed by data owners and of enquiry staff time, it is essential that the objectives and the parameters of searches are kept under constant review to ensure they are as precise as possible. This is particularly important when analysing telecommunications data, where the desire to explore the links between telephones can lead to spiralling requests for billing data, as each new set of data reveals more telephone numbers to explore.

Focusing on the objectives of the strategy and making adjustments where necessary in the light of new material, ensures that costs spent acquiring data are kept to a minimum and that the investigator's time is not wasted.

Passive data strategy

The following points should be considered when setting a passive data strategy.

Speed of access

Passive data generators can produce large quantities of data, which is periodically downloaded, archived or deleted. Fast-track action is, therefore, required to ensure that these sources are preserved and retained.

This should be considered when setting objectives as part of a passive data strategy. In many cases data is stored for a limited time only, so if it is not identified and secured it may be lost to the enquiry. The priority is, therefore, to locate the passive data generator and secure the material before it is deleted from the system. For example, CCTV systems usually work on a twenty-four-hour loop, and telecommunications billing is generally kept for a fixed period of time.

Technical issues

There is a wide degree of variation in the types of storage system used by passive data gatherers. In addition to obvious differences, such as those between videotapes to store CCTV images and computers to store telephone billing data, there may be large differences in the technical specification of systems used for storing a particular type of data. Moreover, the speed of technical innovation means that technical advice can quickly become outdated. Investigating officers should ensure that they have access to the most up-to-date technical advice and support available in relation to the passive data gathering systems they are intending to use.

Sources of advice:

- scientific support units
- hi-tech crime units
- forensic providers
- industry specialists

- academic experts
- IT providers
- analysts
- legal and procedural advisers
- **NCA Major Crime Investigative Support**

Volume of data

Passive data generators tend to gather large volumes of data. Even when tight parameters are set, it is likely that those tasked with searching for specific material will have to manage a high volume of data.

When defining the strategy, investigators must consider:

- whether the request for information is proportionate to the circumstances
- precisely what they are seeking to achieve from the material
- the volume of data that may be generated
- when the data is provided, what they are going to do with it
- the length of time it will take to produce the data, the format it will be available in, how long investigators will take to analyse it
- the likely costs in financial, human and technical terms
- who will conduct the analysis, whether the investigation has the capacity or capability to be effectively managed, whether the staff are suitably knowledgeable to understand the material
- the value that the material will add to the investigation

Technical experts should be consulted if needed to assess this.

Ownership

All passive data is owned by someone. While this is no barrier to it being used, there is likely to be a cost involved and some inconvenience caused to data owners. Investigating officers rely on the goodwill of data owners to access records to look for anything that may be of value, and they may have to pay for this.

Legal constraints

Investigating officers should be certain that they have the appropriate level of legal advice to ensure that they are accessing and using passive data in legally valid ways.

Relevant legislation

Access to some of the material which systems generate is governed by legislation such as the Regulation of Investigatory Powers Act 2000 (RIPA) or PACE. Investigators should also take account of the provisions of the Human Rights Act 1998, notably Article 8 Respect for private and family life.

Protocols

Investigators must be aware of agreed protocols, for example, the communication service providers (CSPs) have agreed protocols which permit investigators to preserve and access call data records. To ensure consistency and conformity with these protocols, identified individuals have been trained and accredited to act as single points of contact (SPOC) for each force. Investigators requiring information and advice about obtaining material from CSPs are advised to make early contact with the SPOC.

Legal and procedural advisers

When it is likely that an investigation will make extensive use of particular types of passive data, or it is believed that it will be central to the prosecution, it may be useful to obtain the services of a legal and procedural adviser. This applies particularly to telecommunications data and financial information where, in addition to specific legislation governing its use by the police, there is also a national policy governing the way in which the police liaise with private providers.

Integrity

Maintaining the evidential integrity of material obtained from passive data generators is an important consideration for investigating officers. When they have sufficient understanding of the technical issues involved, they should implement a regime that ensures that courts can be satisfied that the material has been handled in such a way that its evidential value has not been impaired.

In certain circumstances it may be necessary to seek expert advice or to conduct a forensic examination of the material in order to confirm its authenticity and accuracy.

Interviewing

The material obtained from passive data generators can provide a powerful way of corroborating and challenging material supplied by witnesses and suspects during **investigative interviewing**.

Identifying relevant material

Investigative interviews can also identify passive data generators that may provide relevant material. Interview plans should, therefore, include questions designed to obtain information about the suspect's movements, vehicles, financial activity, computer use and material that may, in the circumstances, identify passive data generators.

Interview planning

Those preparing suspect interview plans should have full access to the material obtained from passive data generators. Interviewers can then corroborate a suspect's account of a particular activity, before revealing the existence of the material. Care should be taken not to inadvertently reveal its existence to suspects during arrest or custody procedures. For example, CCTV images, ANPR material, telephone billing data or financial information linking the suspect to the offence should not be used as a justification for detention if it could compromise the interview strategy.

CCTV

CCTV can provide compelling evidence and investigators should consider it in every investigation. Although it is primarily used for corroborating what is already known or suspected in volume crime incidents, CCTV is a powerful tool for triggering further investigative opportunities, and has a number of immediate benefits and outcomes.

Immediate benefits

- Indicate entry and exit routes from the scene of an incident.
- Identify behaviour before, during and after an incident.
- Identify forensic opportunities such as DNA and fingerprints.
- Help identify suspects, witnesses and vehicles involved.
- Verify a witness's or suspect's account.
- Establish a timeline of events.
- Provide evidence of reconnaissance by a suspect.

Outcomes

- Assist with missing persons enquiries.
- Provide material for intelligence systems.
- Provide evidence of police actions or response.
- Help prove that an allegation or report is true or false.
- Provide evidence of an offence which may lead to an early guilty plea.

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. In court, the prosecution is more likely to secure a conviction when a case is reinforced by good quality CCTV material. CCTV can be a deterrent to potential offenders, helps to reassure the public, assists public authorities with managing ongoing incidents, and helps to protect businesses, vulnerable premises and national facilities. It is also a useful tool when risk assessing scenes.

Technical terms

Systems, by which we meani 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.

Analogue CCTV

Analogue CCTV is a method of recording video using 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 or hybrid is a digital video recorder that has either a VHS or DVD recorder attached to 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 poor-quality output.

Private systems

This can be a stand-alone camera or a network of cameras owned and managed by an individual, or an 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.

Training, equipment and policy

Chief officers should demonstrate support for CCTV 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 various CCTV systems available
- establishing, implementing and overseeing policies to ensure that the use of CCTV (and its supervision) in investigations achieves its full potential

First trawl

The first opportunity to use CCTV material in an investigation usually occurs during the initial response to the report of the crime. During this phase of the investigation, the police will usually be able to ascertain the location of the offence, the time it took place and the identity or descriptions of victims, witnesses and offenders. These details form the basis of the first trawl for CCTV material. In some cases investigators 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.

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

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

Strategy

Setting objectives

In many cases the objectives of the CCTV strategy are obvious, and 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. These usually occur later in the investigation when there is a need to verify the accounts given by individuals, or to test the case theory that investigators have developed to help them make progress in the investigation.

In either case it is necessary for investigators to have a clear understanding of what they hope to find on CCTV images.

As an absolute minimum, investigators should aim to identify any CCTV material that shows the offence being committed. They should do this even when 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 not directly showing the offence may be just as relevant as that which does.

Setting parameters

After considering the objectives, the next step is to focus the search for CCTV on specific times and locations that are relevant to the objectives.

Time parameters

In some cases the time that is of interest to an investigator is 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 is not 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.

Time known

When the time of the crime is known, parameters should include a contingency period both before and after. This provides a safeguard against errors in estimating the time of the crime, and should capture events leading up to and following it which may be relevant. The contingency period is likely to 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 require the seizure of hard drives/DVR units. Where this is necessary, investigators must organise replacement units prior to seizing the units themselves.

After confirming the system time difference 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 parameters after further review of the intelligence or information that they have on

the crime.

Scene visits by offenders

Offenders may have visited the scene beforehand in order to plan the offence. Some offenders return to the scene to witness the consequences of their actions, for example, a person who has committed an arson attack. These visits may have been caught on CCTV.

Time not known

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. Alternatively they could focus the parameters on times when the crime was most likely to have been committed. 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.

Example

In the case of theft from a vehicle in a public car park, intelligence may indicate that other offences have occurred only 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.

Owner’s requirements

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 the owner is busy. If a return visit is required, investigators must ascertain what the overwrite times are when arranging the date and time.

Location parameters

In many cases the locations that are of interest to an investigator are 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 committing an offence. This may in turn indicate forensic opportunities relating to discarded items, or the location of relevant vehicles.

Testing accounts

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.

Changing parameters

Initial parameters are 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 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.

Locating CCTV

Once the time and location parameters have been set, places from where footage can be retrieved should be identified.

Places

Places include:

- cash machines
- traffic management agency
- shopping centres
- local authority control rooms
- transport hubs
- local transport (internal and external cameras)

- petrol stations
- car parks
- private properties and businesses
- police helicopter cameras (heli-teli)
- pubs and clubs
- police helmet (head cams)

Systems

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 be discovered only by walking through the area and making detailed enquiries to obtain contact details of those who have practical knowledge of 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, catching images of any outside activity.

Record keeping

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

Prioritising trawls

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

Factors to consider

- 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 and cash withdrawals linked to the investigation.
- Areas linked to telephone usage, both landline and mobile phones.
- Areas linked to ANPR hits.
- Retention period of systems.
- Accessibility of systems, for example, 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 these CCTV systems, for example, local authorities, garages and large business premises, as well as agencies such as Highways England, 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 the locations straightaway. A request for the footage within known parameters can be made using an appropriate form (such as the sample request for disclosure of personal data template).

CCTV legal responsibilities

Currently, there is no primary legislation specifically controlling the use and publication of CCTV images. To use CCTV effectively, investigators should have a clear understanding of the 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)
- PACE
- Police Reform Act 2002
- Data Protection Act 2018 (DPA)

For further information, a summary of these legal and policy frameworks as they apply to CCTV can be found in **ACPO (2011) Practice Advice on the Use of CCTV in Criminal Investigations**.

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

- Human Rights Act 1988 (in particular Article 8)

- **Home Office (2005) Code of Practice on the Management of Police Information**
- **APP on information management**
- **ACPO (2007) Practice Advice on Police Use of Digital Images**
- **ACPO (2012) Good Practice Guide for Digital Evidence**

Retrieving CCTV

When retrieving CCTV, investigators need to consider:

- viewing CCTV footage at the premises
- how to note the correct time and date on the CCTV system
- how to establish the overwrite period
- retrieving CCTV from the premises
- how much footage to retrieve
- the removal of CCTV systems and digital video recorders (DVRs)
- refusal of the CCTV owner to allow officers to view, retrieve or remove CCTV footage or the system

For further information see **ACPO (2011) Practice Advice on the Use of CCTV in Criminal Investigations**.

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 collect as arranged, or let the owner know if the material is no longer required.

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. 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. 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.

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.

Post-retrieval actions

Officers need to have an awareness of:

- the creation of master and working copies
- the creation of working copies from VHS tapes
- sending footage to the force technical CCTV specialist (FTCS) for editing
- dealing with poor-quality images

For further information see **ACPO (2011) Practice Advice on the Use of CCTV in Criminal Investigations**.

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 to maintain continuity and integrity. **Continuity statements** will be needed.

Force policy on managing exhibits should always be referred to.

Continuity and integrity

For further information see **Home Office (2007) Digital Imaging Procedure, Version 2.1 November 2007 58/07**.

CDs and DVDs

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.

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.

Transport media

Transport media, such as pen drives, flash drives and CD-RWs/DVD-RWs are not suitable for long-term storage. Data should be copied onto write once, read many (WORM) media as soon as reasonably practicable.

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

Digital video recorders

DVRs 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 a DVR is bought is also suitable and can be reused. Only one DVR should be stored in each box. Putting more than one in the same packaging may result in the content being damaged.

Continuity statements

The person who retrieves the footage from the CCTV system should complete a statement to ensure the continuity of the evidence. This person could be the owner of the system, a police officer or a FTCS.

The statement need contain only 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, for example, downloaded the images onto a DVD. Many forces have pro forma MG11 forms, specifically designed for this purpose, 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.

Viewing CCTV

The purpose of viewing seized material is to identify anything of value 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 CPS. This will enable a charging decision to be made.

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

Timely viewing

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.

Visiting the incident location

Investigators viewing the footage may find it beneficial to visit the areas shown on the CCTV footage and see the positions of the cameras, if they have not already done so. This helps viewers to familiarise themselves with the relevant locations and visualise where events have taken place. 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.

Online maps

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.

The investigator must include details of any of the above procedures in subsequent statements, where relevant.

Layout plans

Plans of premises showing the coverage of each CCTV camera can also be useful, especially when suspects and witnesses move around a large building, such as licensed premises, which could have a number of cameras. The layout plan assists the viewing officer to change cameras and follow an individual.

Viewing conditions

Under the Health and Safety at Work etc. Act 1974, chief officers have responsibility for 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.

Demands of viewing

Viewing CCTV images 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.

Breaks

Given the difficulty of maintaining concentration for long periods of time, viewers should take regular breaks. These 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.

Viewing parameters

Viewing parameters and priorities should be set, based on the information and evidence already received. See also **setting parameters**.

If multiple staff are tasked with viewing footage of the same crime, advice should be sought from the FTCS regarding the 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.

Reference images

It may be useful to have reference images to hand to remind 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.

Precautions should be taken if the viewing area is open to members of the public or other non-members of the investigation.

Viewing logs

Download template **Record of viewing form**.

These should always be completed when viewing CCTV, and 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 reduces the risk of defence solicitors discovering further relevant footage 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.

CCTV as an investigative tool

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

- 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 when the identity of someone in an image is known
- show inconsistencies in witness and suspect accounts
- help to identify other investigative opportunities

Other investigative opportunities

These may include:

- forensic opportunities resulting from actions captured in the image or clothing worn or weapons used which can be recovered for examination, for example, a discarded cigarette
- locations 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, and locations of interest

Recognition

This enables enquiries to focus on gathering further evidence against suspects by other means, such as searching their homes, and eye witnesses can carry out identification procedures under PACE Code D.

CCTV evidence dissemination

In the early stages of an investigation, the priority is to identify the offender(s) responsible for the commission of the offence. However, when viewing footage, investigators should regard all those depicted on the CCTV material as potential witnesses. The CCTV images may also show that there are co-offenders, which is why it is important to view a reasonable period of time either side of the actual offence. The investigator needs to identify as many people from the CCTV material as is practicable. To achieve this, it is highly 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 the police
- dissemination to partners
- dissemination to CHIS
- poster campaigns
- dissemination to the media

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. The **rights of third parties** depicted in the images must always be considered.

If the intention is to obtain evidence of recognition from dissemination, it is important that the correct procedures for **recognition evidence** are adhered to. In the absence of 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.

Dissemination to the police

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. 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 (a **controlled viewing**). This information may, for example, be based on personal dealings with the suspect or with previous investigations carried out in that particular area.

It should be noted that when an officer recognises a suspect from any of the recognition procedures, they do not become an eyewitness to the offence. Accordingly, the law does not require that officer to take part in any further **PACE Code D** identification procedures.

Mass circulation

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.

Group viewings

Group viewings are 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 relate to matters of immediate officer safety, for example, when 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 have safeguards in place to deal with incidents of recognition by one or more of the group, for example, officers put their hands up and are spoken to outside the briefing.

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.

Controlled viewing

Staff requested to take part in controlled viewings must view the images alone. The viewing should be overseen by an individual, of the rank of sergeant or above, who has no direct involvement in the investigation.

During the procedure, a record of the information set down in **PACE Code D** paragraph 3.36 of should be made as soon as practicable, even if there is no recognition made.

To ensure greater transparency in investigations into serious crime, consideration should be given to videoing the procedure.

Dissemination to partners

Depending on the offence under investigation, circulating images to police partners may assist. These partners include: 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

They also include other law enforcement agencies such as the UK Border Agency and HM Revenue and Customs.

Dissemination to CHIS

In some circumstances it may be necessary to allow a CHIS to view a still image or section of CCTV footage. Investigators need to follow force procedures for this, and liaise with the designated force officer or authorising officer.

Poster campaigns

Before a poster campaign is launched, investigators should carefully consider the information to include. Nothing 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 is be to justify the way the image 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, some methods of release 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

In order to prevent posters remaining on display indefinitely, it is good practice to include a date (for example, in three months time) on the poster to indicate when it should be removed, either by the person(s) displaying that poster on behalf of the police or by local officers on patrol.

Benefits

Using poster campaigns 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, they show offenders that there are consequences to their actions. This can be most effective if posters are displayed in places where offenders are likely to see them, such as fingerprint rooms and cells in police stations.

A poster campaign also helps build public confidence, highlighting that the police are working hard to fight crime.

Dissemination to the media

For further information see:

- **College of Policing (2013) Guidance on Relationships with the Media**
- **ACPO (2009) Guidance on the Release of Images of Suspects and Defendants**

When deciding whether an image should be released to the media, the considerations outlined for **poster campaigns** are relevant. The same points need to be considered to ensure that the release of images complies with the law. The extent of the coverage required depends 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. This should include circulation to internal and related bodies, and public dissemination tools, including Crimestoppers Most Wanted. Advice may be sought from the force press office.

Rights of third parties

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 to be personal data under the Data Protection Act 2018. In addition, disclosure of third-party images may violate the 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, those of third parties and other personal data are blurred out. This is something that the FTCS should be able to assist with.

Recognition evidence

Recognition is usually what investigators are hoping to achieve through circulation of CCTV images. When CCTV is shown for the purposes of obtaining evidence of recognition, the procedures in PACE Code D s3 of Part B, Evidence of recognition by showing films, photographs and other images, will apply.

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.

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 aware of, 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.

Showing CCTV to victims

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. All other reasonable enquiries to identify the suspect must have been exhausted prior to a victim viewing the images.

Showing CCTV to eyewitnesses

Care must be taken to avoid allegations of contaminating the memory of the witnesses involved when introducing CCTV footage to eyewitnesses.

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 after they have made their initial witness statement, and a record must be made of the viewing.

Specialist suspect ID methods

Before speaking to any outside agency or company about specialist identification techniques, investigators should liaise with their FTCS to discuss what is required from the CCTV evidence. The FTCS may be able to suggest other in-force methods to achieve the same result.

For further information on facial recognition, gait analysis, height measurement and facial or other image comparison, contact the force forensic services or NCA **Major Crime Investigative Support.**

Using external providers

If an outside agency or company is consulted, their understanding of CCTV should be clarified first.

For example, CCTV imagery was sent to an external expert in facial and body morphology. A large and detailed report was completed, but an edited, re-encoded copy of the CCTV material was 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 inadmissible. The re-encoded copy changed the pixel make-up of the image so all measurements were inaccurate.

Confirming identity

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.

Social networking sites

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 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 need to ensure that they do not breach relevant legislation such as the Data Protection Act 2018. Where forces have their own policies and procedures, investigators should follow these accordingly.

Interview preparation

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 the point at which it should be presented to the suspect in the interview.

Before interviewing a suspect it is good practice to consult force interview specialists, such as tier 3 interviewers and major investigation teams.

Working copies in the interview

The master copy of the footage should not be played in an interview. Instead, a working copy should be played to suspects or witnesses. This should be checked beforehand to make sure that it is of a similar quality to the master copy.

Poor-quality images

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 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.

Still images

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

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 is an edited version of the master or working copy, which is short and to the point, and shows the footage that the investigator wishes the suspect or witness to view. Whoever produces the compilation discs requires clear instructions on what is required in the interview.

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. An edit list should be provided.

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.

Edit list

This should contain 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

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

Forces have different policies and procedures for compilation discs, and investigators are advised to refer to these.

Storyboards

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.

It is also possible to use digital image portfolios and image charts, which are digital files that can be replayed on a computer or other digital playback device.

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

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

CCTV images and suspects

There are several reasons why investigators may wish to introduce CCTV to suspects during the interview, including:

- as the basis for direct questions to the suspect, for example, 'Is that you?', 'Where is that garment you are wearing?', 'Did you do that?', 'Who is that person?'
- during the challenge stages of the interview to highlight that the suspect's account differs from that portrayed in the CCTV

It may also 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.

Pre-interview disclosure

For further information see **Investigative interviewing**.

The investigating officer may find it beneficial to allow the suspect's solicitor to view the CCTV before the interview. One method of doing this is to show the solicitor the footage with the detainee present, while recording any comments on tape.

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 does not have to rely on the solicitor to represent the footage accurately to the suspect. Furthermore, it avoids requests from the solicitor to view the footage with their client during consultation.

Introducing footage

Once an investigator is ready to show the images to a suspect, an introduction to the footage should be given. This should include 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 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.

Disclosure and court preparation

After CCTV footage has been 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 enables 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.

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.

Disclosure schedule

The procedure for developing a disclosure schedule (MG6 forms) involves recording all relevant information, including digital image evidence, relating to a case.

The disclosure officer should complete the schedule and ensure that any 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 be provided only if the image becomes an exhibit or is requested by the defence to form part of the defence case.

The description of an 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 section of an image has been enhanced, it may be necessary for the schedule to state this so that the defence can be made aware of the availability of the uncropped and unadjusted images.

Digital images as exhibits

Access to, and **disclosure of**, digital images which become exhibits should be recorded in the audit trail and case papers when disclosed at the police interview stage.

At post-charge stage, access should be allowed only 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:

- date and time at which disclosure was made

- identification of any third party to whom disclosure was made
- reason for disclosure
- extent of the information to which access was allowed, or that was disclosed

For further information see **Digital images**.

Trial preparation

The most important consideration for the preparation of footage for court is the equipment available in the courtroom. 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 need to find a suitable format for presenting the images.

Early contact with the court is recommended to ascertain the type of format that is 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 be equipped only with a VHS player.

In most cases DVDs are 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.

Liaison

Once it is known what type of 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.

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 provide their own guidance and training on this. For investigators from forces without such software, the FTCS can usually help with the preparation of a DVD for the court presentation.

Only relevant footage that needs to be presented in the trial needs to be included on the DVD. Liaising with the CPS assists investigators to provide 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 **storyboard**, can be used. 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 are produced to a high-quality photograph printing standard to ensure that the quality is suitable for court.

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 ensures 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 NCA **Major Crime Investigative Support**. 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.

Whichever method of presentation is chosen, it should be professional, practical, allow the CCTV to be viewed in its best quality and, ideally, should appear in one product, namely, not on a variety of portable media with separate hand-held charts and graphs. The purpose of the presentation is to

assist the jury to understand 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 setup and presentation.

Post-trial

Download template **Local authority feedback form**.

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 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 helps to ensure that local authority control rooms continue to receive adequate funding. This, in turn, 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 can be found here**.

CCTV retention and disposal

After being used or disclosed, CCTV material may be retained but can only be used or disclosed for the same purposes.

For further information see:

- **PACE Code D paragraph 3.30 (f) Destruction and retention of photographs taken or used in eye-witness identification procedures**
- **ACPO (2007) Practice Advice on Police Use of Digital Images**
- **APP on information management**

Image retention beyond CPIA

Decisions relating to the retention of images beyond the minimum timescales set by paragraph 5.9 of the code of practice issued under the **Criminal Procedure and Investigations Act 1996 s 23(1)** , for example where the case is a specified serious offence under the **Criminal Justice Act 2003 s 224** should be taken locally by the information or records management team.

CCTV incapable of impacting on case

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.

For further information see **Home Office (2007) Storage, Replay and Disposal of Digital Evidential Images, Publication 53/07**.

Decisions to release CCTV back to its owner, where it is 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.

Undetected crime images

Images associated with undetected crime should be retained in line with the management of police information principles.

When retaining undetected crime records, they should be easily retrievable and accessible for replay and viewing.

An assessment of the possible value of the information to future cases should also be made.

Disposal

Disposal of police information 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.

Under **PACE Code D paragraph 3.31**, 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

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

Digital images

The value of evidential images cannot be overstated as they allow those engaged with the criminal justice system to visualise crimes and present evidence in a unique way.

Digital images as evidence

The proliferation of methods of digital recording and the potential use of different **types of digital images** as evidence in the criminal justice system must be balanced against the ability to provide safeguards and routine auditable processes.

Although digital images are a useful source of evidence for criminal justice purposes, they should not take primacy over other types of evidence, such as a statement from a police officer or another eyewitness. The police service and other criminal justice agencies should resist any suggestions that an absence of digital images in a case in any way weakens it.

Managing digital images

The police have a key role in managing digital images, including those generated by officers, specialist police staff and those supplied by third parties, such as members of the public. 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 accompanied by a full audit trail.

For further information see:

- **ACPO (2007) Practice Advice on Police Use of Digital Images**
- **ACPO (2012) Good Practice Guide for Digital Evidence**

Types of digital images

Digital images include any image (moving or still) captured digitally and stored electronically.

The following list details some of the sources of digital images used by the police service for evidence collection. It excludes details of covert use of digital imaging and any applications which are reconstructions or interpretations, rather than involving the capture of an original image. This list is not exhaustive.

- **ANPR**.
- **Body-worn video devices**.
- In-vehicle camera systems.
- **CCTV**.
- Covert surveillance.
- Crime scene photographs.
- Facial recognition systems.
- Fingerprints.
- **Video identification**.
- **Investigative interviewing** (video-recorded interviews).
- **Public order** evidence and intelligence gathering.
- Road safety cameras.
- **Third-party images**.

Video identification

Video identification applications providing a bank of digital images of possible volunteers for line-ups include video identity parade electronically recorded (VIPER) and profile matching (PROMAT). A central video database is maintained for both applications.

Capturing images of arrestees

This is central to the process of **identification of suspects**. The following issues require consideration at capture stage:

- correct pose including full head, neck and shoulders, face fully visible
- iris and pupil of the eyes to be clearly seen, where possible
- neutral facial expression with both eyes open and mouth closed
- lighting to uniformly illuminate the subject's face and the background
- background to be plain, smooth and flat

Third-party images

Some digital images are not captured by the police but are provided by third parties such as members of the public using mobile phone devices, or as part of non-police capture systems, for example, small business CCTV.

Use of private capture equipment owned by police officers or police staff should be minimal and restricted to use as a last resort. Any images captured on privately owned equipment should be treated as third-party images that have been submitted by members of the public.

There are significant implications of a witness viewing third-party images prior to being asked to attend a formal identification procedure.

For further information see:

- ACPO (2011) Internet Social Networking Sites (ISNS) and Identification Procedures [Restricted]
- R v I [2007] 2 Cr App Rep 316

Computer-based electronic evidence

Information or data of investigative value that is stored on or transmitted by a computer.

Computers can be used in the commission of crime, they can contain evidence of crime and can even be targets of crime. Understanding the role and nature of electronic evidence that might be found, how to process a crime scene containing potential electronic evidence and how an agency might respond to such situations is crucial.

Handling electronic evidence

Electronic evidence should be treated in the same manner as traditional forensic evidence, with respect and care. The methods of recovering electronic evidence, while maintaining evidential

continuity and integrity, may seem complex and costly. However, if dealt with correctly, experience has shown that it will produce evidence that is both compelling and cost effective.

The case officer is responsible for ensuring continual compliance with legislation and, in particular, that the procedures adopted in the seizure of any property are performed in accordance with statute and current case law. The four principles of electronic evidence must be adhered to.

For further information see **ACPO (2012) Good Practice Guide for Digital Evidence**.

Principle 1

No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.

Principle 2

In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3

An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4

The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

Tags

Investigation