Passive data generators

This page is from APP, the official source of professional practice for policing.

First published 23 October 2013 Updated 7 August 2023
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.

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