NPIA
National Policing Improvement Agency
PROFESSIONAL PRACTICE

THE JOURNAL OF HOMICIDE AND MAJOR INCIDENT INVESTIGATION

Volume 3, Issue 2
Autumn 2007

Produced on behalf of the ACPO Homicide Working Group
by the National Policing Improvement Agency

THE JOURNAL OF HOMICIDE AND MAJOR INCIDENT INVESTIGATION

The aim of *The Journal of Homicide and Major Incident Investigation* is to encourage practitioners and policy makers to share their professional knowledge and practice. The journal will be published twice a year by the National Policing Improvement Agency (NPIA) on behalf of the Association of Chief Police Officers (ACPO) Homicide Working Group. It will contain papers on professional practice, procedure, legislation and developments which are relevant to those investigating homicide and major incidents.

All contributions have been approved by the Editorial Board of the ACPO Homicide Working Group. Articles represent the operational experience or research findings of individuals which may be of interest to Senior Investigating Officers. The views expressed in each article are those of the author and are not representative of the NPIA, nor of ACPO. Unless otherwise indicated they do not represent ACPO policy. Readers should refer to relevant policies and practice advice before implementing any advice contained within *The Journal of Homicide and Major Incident Investigation*.

The ACPO Homicide Working Group welcomes contributions from practitioners or policy makers for inclusion in future issues. These should be emailed to the address below. Submissions should be prepared in Microsoft Word or compatible format. If submitted articles are already published elsewhere they will be reproduced without amendment. Where articles are being published for the first time, NPIA will liaise with the author in relation to any editing that may be required.

All enquiries about the journal should be addressed to:

Dr Peter Stelfox
Head of Investigative Professional Practice
National Policing Improvement Agency
Wyboston Lakes
Great North Road
Wyboston
Bedford MK44 3BY

Email: npia_investigations@npia.pnn.police.uk

Contents

This publication has been printed on material that is certified by the Forest Stewardship Council (FSC). This paper contains fifty per cent recycled fibres processed by means of totally chlorine-free bleaching (TCF), and pulp which is elemental chlorine free (ECF). Its manufacture also embodies well-managed forestry practices, and responsible waste treatment and energy use.

Editorial

Welcome to this special issue of *The Journal of Homicide and Major Incident Investigation,* which focuses entirely on papers concerned with passive data. Passive data is a relatively new concept in investigative practice and the Homicide Working Group felt that it merited a special edition of the Journal to highlight the ways in which it can be used in major crime investigations. SIOs will of course be familiar with CCTV and telephone data, the gathering of which has become a routine part of many investigations. However, they may be less familiar with some of the other sources and we hope that this issue of the Journal will alert them to other possibilities in this area.

The term passive data was coined during the summer of 2005 when three of us were writing the ACPO *Core Investigative Doctrine.* Our aim seemed modest and straightforward: documenting the processes of criminal investigation as the basis for skills development of practitioners. The work mainly consisted of identifying investigative processes and the factors that were relevant to their use. CCTV seemed an obvious subject to cover but as we did so we started to realise that it had a lot in common with other investigative opportunities such as financial records, telephone data, and even information from customer loyalty cards.

In all of these cases the problems and the opportunities seemed to be very similar. The material was usually generated by organisations external to policing agencies, for both public sector functions, such as managing a town centre, or a private sector commercial activity, such as tracking customer spending patterns. Ownership of the material rested with those who had gathered it and so access was something that had always to be negotiated or, where legal powers existed, enforced. Technology was an issue in all cases, in some, such as CCTV, the service had some capability to seize and use the material effectively but in others there was total reliance on the owners of the material making facilities available to enable it to be viewed and used.

These issues were so common that we felt investigators needed a common approach to them, irrespective of the type of data or the technology involved. This would ensure that they sought out the widest range of material that was available to progress an investigation, rather than rely simply on those sources that they were familiar with, such as CCTV and telephone data.

Writing the approach was not in itself difficult and it became Section 6.7 of *Core Investigative Doctrine*, which was later used as the basis for Section 13 of the *Murder Investigation Manual*. But what to call these sources of material? Surveillance Data was an early and tempting prospect, but we felt that the term would necessarily come to include material that had been generated by investigators themselves through mobile and technical surveillance methods. This was a wholly different type of material and was subject to a different set of considerations. What was unique about the type of systems we had in mind was the fact that they were generally going quietly about the business of gathering data without anyone having to focus them on a particular individual or area. And they did it remarkably efficiently. If you shopped in your local supermarket, a computerised system, or more likely several, would note that you had done so. Your journey there may have generated material in several CCTV systems or on ANPR. If you drove there in some types of car, data would have been generated in the car's computerised service log. If you had a satellite navigation system, there would probably be a record in there as well. Loyalty cards and credit card systems would record your purchases. Not all of these systems would tell someone that you went to the supermarket that day, but together they created an electronic footprint which could provide a picture of where you were, what you were doing, what you bought and whose money you spent. It seemed to us that the key feature of this data, and its main value to investigators, was the routine nature of the data gathering; the fact that it runs passively in the background whilst we go about our daily routines. And so that was why we christened it 'Passive Data'. Whether that was a good name or not, the concept certainly seemed to chime with investigators and the feedback from practitioners and trainers is that it has at least highlighted the common characteristics of the varied systems that can provide this type of material to investigations.

What has become apparent since then is the growth in both the use of passive data by investigators and the degree to which questions are being raised about the desirability of allowing the police, and others, relatively free access to it. This increased use, and the concerns around it, are partially due to the extent to which it has been used in counter terrorism investigations. But far more use is also being made of it in volume crime investigations as well. Of course, no one should be surprised by this. Those carrying out criminal investigations have always exploited the technology of their day to do a better job. During the eighteenth century, the development of cheap printing processes led to the widespread use of handbills to broadcast information about crimes over a much wider area than had previously been possible. In the nineteenth century, fingerprints were first used in criminal investigation. During the twentieth century, the techniques of recovering and using DNA has revolutionised crime scene examination. None of these techniques were first developed with the investigation of crime in mind, but once they were found to be useful, they quickly became part of the investigative routine.

What is perhaps different about passive data is the speed and scale of the developments. These appear always to outrun both the police organisation's ability to develop policies, business systems and practice to cope with technological advances and society's ability to decide if or how they wish to regulate the use of such data by investigators. This has a number of implications for both practitioners and policy makers and we hope to explore some of them in this special issue.

The potential of passive data to provide material for investigations is undeniable and this is explored by Kevin Smart in relation to financial investigation. Graeme Gerrard explores similar themes in relation to CCTV and highlights some of the technical and logistical difficulties that the sheer volume of material can present. Stuart Kirby shows how various elements of passive data and the technology that supports it have come together to provide the Police Service with its ANPR facility and how this can be used by SIOs. Andy Tennet's case study about an investigation into a fatal road collision which led to the successful prosecution of a company for corporate manslaughter shows how all of these technologies can come together into a single investigative strategy.

An aspect of passive data that is not often considered by investigators is the role of the private industries which pay for the technological developments and which gather and own the data. Ray Green explores the issue of gathering data from private companies; identifying some of the issues and considerations associated with doing so and suggests that the Police Service may need to rethink its approach if investigators are to maximise the potential of the data available.

The use of some forms of passive data is covered by legislation and this is reviewed by Giles Herdale from the NPIA. Finally, John Fox reflects on some of the wider issues around the use of passive data by the police and reviews some of the concerns that have been raised.

This collection of papers has been written exclusively by practitioners with first hand operational knowledge of the issues. We hope that they highlight the opportunities that passive data provides for SIOs as well as providing an insight into some of the legal, practical and policy issues that face the Police Service in this area.

Dr Peter Stelfox
Head of Investigative Professional Practice
NPIA

CCTV and Major Incident Investigation: Professionalising the Police Approach

DCC Graeme Gerrard, Cheshire Constabulary
Chair of the ACPO Video/CCTV Working Group

Abstract

Although we have been using CCTV evidence for many years, we have been slow in developing a professional approach to evidence recovery and analysis. This article compares our approach to conventional crime scene evidence such as fingerprints and DNA and argues that the increasing complexity of digitally recorded CCTV requires a fundamental change in the way we mange CCTV recovery operations.

Contents

All correspondence should be addressed to: DCC Graeme Gerrard
Cheshire Constabulary, Clemonds Hey, Oakmere Road, Winsford, CW7 2UA

1 Introduction

CCTV technology has been developed progressively since the first public television transmission in 1936. The video cassette recorder was introduced twenty years later and CCTV was first acquired by British retailers as early as 1967[1]. By 1975 London Underground had installed a CCTV network on the Northern and Victoria lines at Stockwell and four other stations due to staff assaults and theft[2] and in 1985, the UK's first public CCTV system was piloted in Bournemouth to counter vandalism on the sea front[3].

The United Kingdom is generally recognised as a leading user of CCTV for community safety and crime investigation purposes. The often quoted figure of 4.2 million cameras is an estimate based on the number of cameras found on Putney High Street, London in 2002 and then extrapolated to provide a figure for the United Kingdom as a whole[4]. I doubt that many areas of the UK have the same concentration of CCTV cameras as Putney High Street and so the 4.2 million figure should be treated with a great deal of caution. Nevertheless, we have more cameras than most comparable societies, particularly in public places such as streets, transport systems, hospitals and schools.

Despite the volume of cameras in the UK and the period of time that their surveillance product has been available to investigating officers, our processes and procedures for acquiring CCTV evidence are not well developed and lag far behind those associated with fingerprints, DNA and other forms of crime scene evidence.

This article examines why this is the case, identifies the pitfalls awaiting unsuspecting Senior Investigating Officers (SIOs) and outlines the actions that need to be taken if we are to maximise the effectiveness of CCTV evidence.

[1] Moran, J. (1998) 'A brief chronology of photographic and video surveillance' In Norris, C., Moran, J. and Armstrong, G. (Eds.) *Surveillance, Closed Circuit Television and Social Control*. Aldershot: Ashgate.
[2] Webb, B. and Laycock, G. (1992) Reducing Crime on the London Underground: An Evaluation of Three Pilot Projects. *Crime Prevention Unit Paper No 32*. London: Home Office
[3] Bannister, J., Fyfe, N.R and Kearns, A. (1998) 'Closed Circuit Television and the City'. In Norris, C., Moran, J., and Armstrong, G. (Eds.) *Surveillance, Closed Circuit Television and Social Control*. Aldershot, Ashgate.
[4] Cahill, M. and Norris, C. (2002) *On the Threshold to Urban Panopticon? Analysing the Employment of CCTV in European Cities and Assessing its Social and Political Impacts*. Urban Eye. RTD Project 2001-2004.

2 CCTV – The Early Days

There is little doubt that evidence captured by CCTV systems can contribute significantly to all forms of police investigation and numerous high profile cases have demonstrated the effectiveness of CCTV evidence in assisting criminal investigations. Most Senior Investigating Officers will be conscious of the need to recover CCTV evidence at the outset of an investigation and may have well developed policies and procedures that ensure the evidence is collected in an efficient manner. The Metropolitan Police, particularly their Counter Terrorist Command are probably world leaders in this field and have the capacity to recover and analyse large volumes of CCTV evidence. However, work undertaken when developing the National CCTV Strategy[5] has identified that many forces have still not developed their capacity to recover CCTV evidence and many SIOs are unsighted on some of the difficulties and issues that accompany the recovery of CCTV evidence. Indeed, it is true to say that the Police Service as a whole has yet to establish the most appropriate way of managing the recovery, analysis and storage of evidence recorded by CCTV.

The police response to CCTV is closely associated with the development of the technology. When CCTV was initially introduced into the UK, images were recorded onto VHS tapes and replayed using technology that was easy to use[6]. These early systems were relatively expensive and few shops and commercial premises could afford this new technology. Although the quality of the images often left a lot to be desired, police officers had little difficulty in obtaining the relevant VHS tape and viewing the evidence at the police station[7]. As CCTV systems became cheaper, more cameras were deployed in commercial premises and the technology used to record and play back the images started to appear in homes in the shape of the VHS Recorder. The very fact that we were familiar with the technology because we used it within our homes further assisted the police in the recovery of CCTV evidence. In essence, you recovered the VHS tape, put it in a VHS Recorder and pressed the play button. All very simple.

[5] Gerrard, G., Parkins, G., Cunningham, I., Jones, W., Hill, S., and Douglas, S. (Forthcoming) *National CCTV Strategy*. Home Office (to be published September 2007)

[6] Op.cit. 1

[7] Op.cit. 5

3 The CCTV Expansion Programme

In the early 1980s CCTV was beginning to be deployed in streets and other public places. The rapid expansion of town centre CCTV really started in 1994 when the government announced funding in the form of the CCTV Challenge Competition and made £38.5m available for 585 CCTV schemes nationwide. Between 1999 and 2003, a further £170m was made available by the Home Office as part of the Crime Reduction Programme and as a result, more than 680 CCTV schemes were installed in town centres and public spaces[8].

As a result of this huge investment, most public space CCTV is now owned, monitored and managed by local authorities, many of whom have procured different systems at different times and with a range of different specifications, leading to a mix of schemes across the country. In addition, the CCTV in commercial premises has also developed in a piecemeal fashion with little consistency in the type of equipment procured.

The government's CCTV expansion programme greatly increased the number of cameras in UK towns and cities. Placing thousands of cameras on the streets of the UK, each with the capacity to constantly monitor the local environment was bound to increase not only investigative opportunities but also the workload of the police. Unfortunately, whilst funding was made available for cameras, no additional funding was provided to the police to enable them to increase their capacity to recover and view CCTV images or respond to live incidents that were monitored by CCTV operators.

The expansion of CCTV during the 1990s also saw technological developments as systems were developed that allowed multiple cameras to be monitored on one screen. The technology, know as multiplexing, introduced a degree of complexity into the viewing process not hitherto experienced by police officers. The image was less easy to play back and specialist equipment in the form of de-multiplexers had to be purchased if you wanted to view the evidence captured by a single camera. In some forces, Technical Support Units (TSUs) were drawn into providing the technical expertise even though many units did not have sufficient capacity to undertake this work.

[8] Op.cit. 5

4 Image Retention and Recovery

4.1 VHS Recorded CCTV

Critical to any investigation is the length of time a CCTV image is retained before it is over recorded by the CCTV system. In the absence of any national standards, image retention periods differed significantly. In the *CCTV Codes of Practice* (2000) the Information Commissioner's Office recommended a 28 – 31 day period and although most town centre systems and those run by the large retail groups adopted this time period, the recommendation was never enforced and the amount of time the image was retained was left to the individual CCTV system owner.

Despite problems over tape retention periods, the quality of images and the technical complexities of multiplexing, the recovery of CCTV evidence was still relatively straight forward in that the image was recorded on a VHS tape and could be collected by a police officer without any technical expertise. The volume of available CCTV evidence could be a problem, especially in major crime and terrorist investigations but in the main, we still had a reasonable amount of time to gather it and the recovery was a straightforward process.

4.2 Digitally Recorded CCTV

As VHS recording equipment has been replaced with digital recording technology, the process of recovering CCTV images has become more complicated. The absence of standardisation in relation to down load formats has resulted in the development of hundreds of different systems, many requiring unique software to download the image into a viewable format. If an officer is fortunate enough to be handed the video evidence on CD or DVD, it is likely that they will not have the software to view the images. In addition, since many force computers have had their CD/DVD drives disabled by their Information Technology Departments (to prevent computer viruses being imported onto their networks) many officers cannot even find equipment to play the image and have resorted to playing the CD or DVD on their home computers in an attempt to view the evidence.

Most town centre systems and those used by the major retailers present their CCTV evidence in a viewable format and do not cause us difficulties. However, a large number of smaller systems, located in buses, shopping precincts, small shops, pubs, and other commercial premises can present a significant challenge for the officer sent to collect the evidence and recovery of some forms of digitally recorded CCTV has become a specialist function requiring specific technical skills. This not only increases the cost of CCTV recovery but can also result in crucial images not being recovered in time if the technical expertise in unavailable.

When the problems of recovering digitally recorded CCTV started to emerge, many forces started to use their TSU, High Tec Crime Unit or Computer Forensic Unit to recover the images. Whilst the staff involved may have had the technical expertise, they often did not have the capacity or equipment to go out and recover increasing quantities of CCTV evidence.

In order to combat the difficulties associated with play back of digitally recorded CCTV some forces have invested in equipment that contains the most commonly used play-back software and allows officers to easily view the images they have recovered. The Metropolitan Police and the Home Office Scientific Development Branch (HOSDB) have been examining commercially produced equipment and along with the ACPO Video/CCTV Working Group, are seeking to set a UK criminal justice standard that future providers of CCTV recording equipment would be invited to meet.

Digitally recorded CCTV uses large amounts of data that needs to be stored if the images are to be retained. The length of time an image can be retained will be dependant upon the quality of the image, the number of cameras on the system and the amount of hard disk storage in use. Digital images can be 'compressed' so that they take up less storage space. However, the compression process degrades the quality of the image and too much compression will result in pictures that are worthless to the SIO. If you tell a CCTV operator to keep their images for as long as possible and the CCTV system is digital, there is a danger that they may alter the compression and present you with pictures that are not fit for purpose.

The cost of storing digitally recorded CCTV images, particularly if the system has multiple cameras can be very high and many system managers have reduced the amount of time they will retain the images for. This can have serious implications for those with responsibility for investigating crime. The CCTV system that used to retain its evidence for 31 days may now only keep it for 7 days. If your force does not know the image retention periods of the CCTV systems in its area, it will be impossible for the SIO to prioritise the CCTV recovery operation.

In order to protect the footage in analogue recordings, VHS tapes are removed, stored and replaced by new tapes. In digital systems the material is exported from the system. Whilst most events can be exported to CD and DVD, those investigations that require the recovery of CCTV over several days or even weeks from multi camera systems, as is often the case in a homicide or terrorist investigation, will require long exports and large amounts of storage space. In some circumstances, the hard disks of the CCTV system will have to be removed in order to preserve the evidence and on occasions, complete systems have had to be

unplugged resulting in the entire system becoming disabled. Exporting 7 days of CCTV images from a town centre system could take several days depending on the complexity of the system and the number of cameras involved. If the system only records for 14 days and you don't get to it until day 10, the system will overwrite the last 3 days of images before they can be exported. The only option available to the individual with the responsibility for recovering the images is to remove the hard disk completely and replace it with a spare, assuming there is one available. Understandably, many CCTV managers are reluctant to allow this to happen, especially as it may affect the warranty of the entire CCTV system.

Recovering CCTV in these circumstances is clearly a job for specialist staff that have the right equipment and the appropriate level of training. It is not a job for the average police constable or detective and yet these are the people often sent to recover CCTV evidence.

5 National Image Retrieval Cadre

The experience of the Metropolitan Police following the terrorist incidents of July 2005 has resulted in the development of a cadre of image retrieval officers, drawn from most forces in England and Wales, who have been trained by the HOSDB to retrieve CCTV images from digitally recorded systems. In the event of any criminal investigation that requires large quantities of CCTV evidence to be recovered, Cadre members can be called out on a mutual aid basis to assist with the CCTV recovery operation. Getting sufficient suitably trained and equipped staff on the ground in the early days of an investigation will maximise the likelihood of evidence being recovered quickly and before it is overwritten. To date, 110 staff have been trained and officers from the cadre have been deployed to assist Suffolk with their investigation into the murder of 5 women and during the terrorist incidents at Glasgow Airport and London in July 2007.

Despite repeated notifications to forces of the existence of the Cadre, it is apparent that many SIOs are unaware of their existence. If the CCTV recovery operation relates to a terrorist incident, the 'call out' process for Cadre members is managed by SO15 of the Metropolitan Police. Contact should be made via your own Special Branch Office. If the CCTV recovery operation is not terrorist related, authority to instigate mutual aid arrangements should be sought from an officer of ACPO rank within your own force. Once authority is given, call out procedures are held within your force Control/Incident Room. It is recommended that you seek advice from your own imaging specialist or Cadre member prior to instigating the call out procedure.

6 CCTV Recovery Plans

An early task of any SIO is to determine, with their crime scene manager, the forensic recovery plan that will be implemented when investigating a homicide or other major investigation. We have recognised the specialist nature of crime scene examination and ensure that the SIO receives professional advice in relation to the recovery of conventional crime scene evidence. This advice includes the viability of examining crime scenes, the forensic techniques that will be deployed and the likely time and cost associated with the examination. In addition, if the crime has multiple scenes, we use a Crime Scene Coordinator to oversee the recovery of exhibits. However, when it comes to the recovery of CCTV, few SIOs benefit from similar advice and many have to develop their CCTV recovery plan based on their own limited knowledge. As the preceding paragraphs have suggested, recovering digitally recorded CCTV evidence is a complex process requiring a thorough understanding of the technology and the difficulties that may be encountered with multiple camera systems. Developing a professional capability to support SIOs is now becoming urgent and although some forces have recognised the need, many are still unaware of the issues and have failed to develop this capacity.

7 CCTV as Crime Scene Evidence

CCTV should be treated in a similar way to the conventional forms of crime scene evidence such as fingerprints, foot wear marks, fibres and DNA. The Police Service long ago accepted that these forms of evidence require specialist skills in terms of recovery and analysis. It has also accepted that this specialist discipline should be supported with professional training, accreditation, management structures and a performance measurement regime. We have data that provides us with the average number of scenes visited by each Crime Scene Investigator. We know how many samples of DNA are recovered and how many fingerprints are lifted. We know how many of these lead to identifications and how many of these result in detections. We can compare performance across forces and determine the cost effectiveness of this form of evidence. Furthermore, every force has invested heavily in both the recovery and analysis of conventional crime scene evidence and the discipline is recognised as an integral part of criminal investigation.

Compare this with our current approach to CCTV. Many forces still do not recognise it as a specialist discipline, training is ad hoc and not undertaken to any nationally accredited standard, there is no national performance regime and no data collected nationally or even locally that indicates the usefulness of CCTV. Furthermore, many forces have invested little in terms of staff and equipment in the recovery of CCTV evidence and in the main rely on the patrolling constable or detective to ‘go and get all the available CCTV’.

Yet it is probable that CCTV has the capacity to provide more evidence in support of criminal investigations than the conventional forms of crime scene evidence. National data indicates that for every 100 crime scenes visited, a Crime Scene Investigator recovers DNA from 17 scenes and fingerprints from 33. These recoveries produce 2.27 primary detections from DNA and 3.29 primary detections from recovered fingerprints. Since a Crime Scene Investigator visits, on average, 3.3 crime scenes per day, the 'average' CSI recovers evidence from a crime scene leading to a primary detection once every three days[9].

Although we don't have any national data relating to the detections that result from CCTV evidence, what information we do have tends to suggest that an officer engaged on the full time recovery of CCTV would produce evidence leading to a primary detection at least once every three days. If this is the case, there is an urgent need to review the relative contributions to crime investigation provided by CCTV and the conventional forms of crime scene evidence and determine whether we have allocated resources appropriately.

Since CCTV evidence can identify the actions of a suspect, it can be used to compliment other forms of crime scene evidence by providing information as to where the forensic recovery should concentrate. Knowing where the offender was standing, what he touched, where he discarded his cigarette will assist the CSI in the evidence recovery operation. For this reason, the collection of CCTV evidence should be co-ordinated with the forensic recovery operation. Early viewing of the CCTV will help to target the forensic recovery saving both time and money.

If we view CCTV as crime scene evidence it seems logical that the discipline should be seen as an extension of a Forensic Science Unit and be managed accordingly. We already have the supervisory structure in place and managing CCTV recovery from within this unit will ensure that the process is coordinated with conventional crime scene examination. Whether both roles can be undertaken by the same investigator has yet to be determined. Both require specialist skills but the nature of such skills is significantly different and it may be difficult to find individuals who can be trained up in both disciplines.

[9] IQUANTA Data. Home Office.

8 CCTV in Major Investigations

The recovery of large volumes of CCTV evidence will pose a challenge for any SIO and will require careful management. The ACPO Video/CCTV Working Group has been examining the lessons learnt from major investigations and has identified a number of key roles that will be required if large volumes of CCTV evidence are to be managed effectively.

CCTV Recovery Manager

The CCTV Recovery Manager acts in a similar way to the Forensic Crime Scene Manager in that he or she assists the SIO in preparing the CCTV recovery plan. Geographical areas will need to be identified, mapped and broken down into smaller areas for allocation to the CCTV Recovery Teams.

Knowing where the CCTV cameras are, what the image quality is like, what the field of view encompasses and how long the images are retained is important information for any CCTV Recovery Manager. Some forces have mapped this information onto GIS systems. This aids the recovery operation and assists in prioritising which CCTV needs to be collected first. In the absence of a mapping system, there is no alternative other than to visit all premises in the area in order to establish whether they have CCTV cameras.

CCTV Recovery Team Supervisor

The Recovery Team Supervisor is responsible for the day to day tasking of the Recovery Teams in response to the investigation parameters set by the SIO and the CCTV Recovery Manager. Since CCTV evidence will be lost if not recovered quickly, it is crucial that the Recovery Team Supervisor is aware of all investigative developments that may influence the CCTV recovery process. The tasking process will need to be dynamic in order to maximise the evidence gathering opportunities and recover CCTV images before they are over written.

CCTV Recovery Team Officer

The CCTV evidence will be recovered by the Recovery Team Officers. The number of officers required will be dependent on the size of the recovery operation and the amount of time available to recover the CCTV. Large recovery operations are likely to require assistance from surrounding forces and officers from the National CCTV Image Retrieval Cadre would provide a body of trained and experienced officers to assist in the recovery operation. Each Recovery Officer will need to be provided with a map of the area, pro-forma statements for continuity of exhibits and a detailed briefing of the information required in support of the

CCTV recovery. This will include the camera field of view, the earliest date of the recorded image, the screen time (checked against the speaking clock) and the full address on the CCTV location.

If the Recovery Team Officer does not have the technical expertise or equipment necessary to down load digitally recorded images, there will be a need to refer the CCTV systems to a staff member with these skills and equipment.

CCTV Viewing Room Supervisor

Recovered CCTV needs to be viewed as quickly as possible to establish whether it contains evidence relevant to the investigation. The viewing process can overwhelm an investigation if it is not managed effectively. Viewing facilities in the form of rooms and equipment need to be provided and the viewing operation needs to be managed by the Viewing Room Supervisor. The Supervisor is responsible for the day to day tasking of the CCTV viewing team and will prioritise the viewing operation in accordance with the investigative direction given by the SIO. It is likely that you will need technical support in the early days of an investigation in order to set up the viewing equipment.

CCTV Viewer/Analyst

The role of the CCTV viewer is to analyse the recovered CCTV and record any relevant sightings and evidence. Evidential logs should be completed and detailed records of camera positions noted.

CCTV Exhibits Officer

The CCTV Exhibits officer works to the lead exhibits officer on the enquiry and is responsible for the movement of CCTV product into the viewing team and the quality assurance of media exhibits submitted to the team.

Unless a force has already experienced a homicide or major investigation requiring the recovery of large volumes of CCTV evidence, it is unlikely that these roles will have been identified nor the officers briefed as to their responsibilities in the event of a major CCTV recovery operation. Contrast this approach to the way we manage conventional forensic recovery operations. We would not undertake a major investigation and develop our forensic recovery capability on the hoof so to speak. We would not wait for the event to happen and then start to identify and train the CSIs, the Crime Scene Manager and the Crime Scene Coordinator. We don't wait for the murder to occur before we start to buy the

equipment necessary to undertake a basic forensic examination. We don't wait for the big job to break before we determine how we are going to analyse the forensic evidence we collect. Yet this is the position that many forces are in with regards to CCTV and SIOs are being placed in particularly vulnerable positions because this capability has not been developed in their force area.

It is strongly recommended that all the roles outlined above are identified in advance of the need to deploy them. The Recovery Manager, Supervisor and Team Member will require specialist skills and knowledge and are likely to be drawn from the unit (if you have one) that has responsibility for CCTV recovery. The Viewing Room Supervisor, Viewer/Analyst and CCTV Exhibits Officer can be non-specialised officers who have been trained to undertake these specific roles. Some forces have incorporated these roles within their Major Incident Team.

9 Conclusion

There is a pressing need for the Police Service to recognise the risks and opportunities presented by CCTV evidence and start to develop the capacity to handle it in a more professional manner. Many of the issues raised within this article have been examined by the ACPO Video/CCTV Working Group and in September 2005 a report was submitted to the National Crime Reduction Delivery Board recommending that a National CCTV Strategy for the UK was required. The strategy has been developed and awaits publication by the Home Office. It is the culmination of 18 months of work undertaken by a small joint ACPO/Home Office project team, supported by a wide range of consultees. From a policing perspective, the strategy will support our use of CCTV and will help to resolve many of the external issues that currently cause us problems. However, we still need to put our own house in order by recognising the specialist nature of CCTV evidence, by providing the resources necessary to handle it effectively and by professionalising our approach in much the same way as we have for the conventional forms of crime scene evidence. Only then will we be able to maximise the benefit of a network of CCTV cameras that is currently the envy of investigating officers across the world.

Acknowledgements to:
CC Frank Whiteley (chair of ACPO, ANPR steering group),
ANPR Crime Investigations Working Group',
Det. Supt. Andy Brennan (W.Yorks),
DCI Colin Sutton (MPS),
A/Det. Supt. Steve Tolmie (TVP).

The following police forces for providing examples:
Bedfordshire Police,
Cumbria Constabulary,
Essex Police,
Gwent Police,
Hertfordshire Constabulary,
Kent Police,
Lancashire Constabulary,
Metropolitan Police Service,
Northumbria Police,
North Wales Police,
National Crime Squad,
South Wales Police,
Sussex Police,
West Midlands Police.

References

Bannister, J. et al (1998) 'Closed Circuit Television and the City'. In Norris, C, Moran, J., and Armstrong, G. (Eds.) *Surveillance, Closed Circuit Television and Social Control.* Aldershot, Ashgate.

Cahill, M. and Norris, C. (2002) *On the Threshold to Urban Panopticon? Analysing the Employment of CCTV in European Cities and Assessing its Social and Political Impacts.* Urban Eye. RTD Project 2001-2004.

Gerrard, G., et al. (forthcoming) *National CCTV Strategy*. Home Office (to be published September 2007).

ICO (2000) *CCTV: Code of Practice.* London: ICO. Available from http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/CCTV_code_of_practice.pdf

Moran, J. (1998) 'A brief chronology of photographic and video surveillance' In Norris, C., Moran, J. and Armstrong, G. (Eds.) *Surveillance, Closed Circuit Television and Social Control.* Aldershot: Ashgate.

Webb, B. and Laycock, G. (1992) Reducing Crime on the London Underground: An Evaluation of Three Pilot Projects. *Crime Prevention Unit Paper No 32.* London: Home Office.

Follow the Money: The Use of Financial Information in Major Crime Investigations

DS Kevin Smart
Investigative Practice Team, NPIA

Abstract

ACPO published *Practice Advice on Financial Investigation* in 2006, which was intended for use by all investigators.

This article outlines how the financial information recorded and held by financial institutions and other industries can provide opportunities in the investigation of major crime.

Contents

All correspondence should be addressed to: npia_investigations@npia.pnn.police.uk

1 Introduction

Over the last ten years there has been a significant shift towards the use of plastic cards and other cashless means of payment for goods and service. During 2005 spending on debit cards outstripped the use of cash for the first time. Anyone who holds some form of property, money or other asset is likely to use an electronic financial service such as a bank account. The computerised systems used by financial institutions and other merchant service providers provide a source of information about the lifestyle, movements and activities of those who use them. All of these can be used to inform productive lines of enquiry during a major investigation.

Financial records are detailed because the industry has a vested interest in collecting data to aid the smooth running of their business, increase profitability and to protect against fraud. Effective use of these rich sources of data by investigators is dependent on them knowing:

a) what information is available to them, and

b) how this information may be accessed.

While SIOs may be familiar with some aspects of financial information, this source of valuable information remains under used by many. The first section of this article presents the reader with the main sources of financial information. The second section explores the ways in which it can be incorporated into an investigative strategy.

2 Information Held by Financial Institutions and Other Bodies

There are numerous sources of data held by financial institutions and other bodies. Here are a few of the most useful and accessible organisations.

2.1 Merchant Service Providers

Merchant service providers, such as mobile phone companies, utility companies or firms that deal with merchants' claims for reimbursement for credit or debit card payments by customers, hold a variety of information of potential use to an investigation. This can include a person's location at a certain time or details of any electronic payments they may have made. Merchant service providers hold:

- Applications for services;
- Account information;
- Information from points of sale;
- Loyalty cards.

Sky TV records, for example, can be a reliable method of obtaining a person's address because of the popularity of the service they provide. Investigators can apply for production orders to obtain information from the financial institution that administers the chip and PIN or swipe systems (such as Link) for the merchant service provider, which can then be followed up.

2.2 Government Departments and Other Agencies

Various government agencies and departments hold financial information of use to a police investigation. Examples of these agencies are as follows:

- The Department for Work and Pensions (DWP);
- Her Majesty's Revenue and Customs;
- Local Authorities;
- The Land Registry;
- The United Kingdom Identity and Passport Service (IPS);
- Companies House.

Each department has its own protocol for access to data.

2.3 Credit Reference Data Bases

Credit reference agencies provide data access systems that can be used in criminal investigations allowing authorised officers to obtain information on an individual's financial relationships and status. Credit reference agencies in the UK include:

- Experian;
- Equifax;
- Call Credit (mostly based in the UK and primarily concerned with high street credit ratings).

Dunn and Bradstreet hold information on companies, company directors, multiple company directorships, a director's former earnings, company secretaries, trading addresses, company files, and names of disqualified directors. CIFAS, the UK's fraud prevention service, keeps information on multiple credit applications that are suspected of being fraudulent. They also maintain other fraud databases.

2.4 The ELMER Database (Suspicious Activity Reports)

All forces have access to a database called Elmer that is usually located in the FIU or FIB (or both). Elmer contains data from Suspicious Activity Reports or SARs. SARs can be a useful source of intelligence for investigators. They are produced by the regulated sector (the financial industry and other businesses that deal with large volumes of money), which is legally required to train all staff to recognise and report any suspicions that arise concerning money laundering or terrorist activity. SARs are sent to the Serious Organised Crime Agency (SOCA) which then disseminates them to forces via Elmer.

2.5 Access to Data

In order to access information held by other agencies and companies, an investigator must use a request for disclosure of personal data under the Data Protection Act 1998. The power to disclose information exists where disclosure is required for:

- the prevention or detection of crime;
- the apprehension or prosecution of offenders (section 29 (3)); or
- for reasons of national security (section 28) to the extent that non-disclosure of the requested information would be likely to prejudice one or more of those same purposes.

In cases where it may not be appropriate to claim the exemption, a special procedure order under section 9 and schedule 1 of PACE for the disclosure may be sought (although these production orders under PACE cannot be served on a government body).

In relation to requests for information from banks and other financial institutions information will usually be divulged to a financial investigator if one or more of the following criteria are met:

- where disclosure is under compulsion by law;
- where there is a duty to the public to disclose;

- where the interests of the bank require disclosure;
- where the disclosure is made by the express or implied consent of the customer.

These criteria came from the case **Tournier v National Provincial & Union Bank of England**[1] and although the information given is not for evidential purposes a special procedure order can then be sought to turn the intelligence into evidence.

There are various orders under the Proceeds of Crime Act 2002 which can be used to access financial information and to monitor accounts; however these orders can only be used in confiscation or money laundering investigations.

The legal provisions and working practices between the police and financial institutions in this area are complex and will generally be beyond the knowledge of an SIO. However, all forces have accredited financial investigators who will know exactly how to access the information. SIOs should ensure that they receive advice from them in all cases where they intend to use this sort of data.

3 Investigative Opportunities

As can be seen above there is a large amount of information available to the police but how can it be used in the investigation of major crime? Clearly, it will be more useful in some cases than others, but as a general rule, financial information can be used to provide material victims, offenders and witnesses.

These are common to all investigations, and SIOs will always seek to maximise the information they have about them. Financial information can be used to inform and generate lines of enquiry in a number of ways particularly around the following areas:

- possessions;
- lifestyle;
- networks;
- location;
- movements.

[1] [1924] 1 KB 461; [1923] All ER Rep 550; 130 LT 682

3.1 Possessions

The most common use of this aspect of financial data will be to link people with property. This will be either linking known articles to unknown people or linking known people to unknown articles. This can be done through financial and other service providers' databases. Linking people to possessions can also be used more creatively in some situations. For example, from the purchase of a suit, shirt and shoes by credit card in a large store chain, it is possible from the credit card information linked to the computerised store sales and stock management system to tell what size that person is, the sole pattern on their shoes and what material the suit was made of. It would therefore be possible to get an intelligence match for a footmark or fibres found at a scene in a covert manner without alerting a suspect or in cases where the original items had been destroyed or disposed of.

3.2 Lifestyle and Social or Business Networks

Knowing the lifestyle of victims and suspects can provide valuable opportunities to identify other sources of information about them. It is often the case that knowing how the victim lived their life gives some sort of clue as to why they died, and who may have killed them.

The information being gathered and stored on everyone automatically as they go about their daily business is immense. From a store loyalty card it is possible to tell a person's shopping habits and purchases, and therefore build up a lifestyle profile of that person.

It is possible to tell if there has been any significant change in purchasing which may have a bearing on something happening in an investigation.

From a financial profile it may also be possible to identify associates or activities of the victim or suspect which they may have kept secret and which are, therefore, unknown to partners or other members of a family. This will produce further productive lines of enquiry.

3.3 Movements

It is not only possible to chart a person's movements through their mobile phone. Their financial records can provide additional information. This can be used to:

- check accounts given in interview;
- set CCTV and search parameters;

- place a suspect in an area or with a victim or a witness;
- locate a suspect or witness.

It is also possible to link witnesses with a location or scene in this way.

3.4 Location

In addition to providing information about an individual's possessions, lifestyle and movements, financial data can also be used to provide information about locations. For example, when an incident occurs in an area where there are a number of financial outlets, such as a high street, it is possible to identify people who were in the area at the time of the incident who may be potential witnesses to the offence. A financial investigator will be able to identify financial outlets in the vicinity of the incident then get production orders to identify who used a credit or debit card through the switch system, or who had used a cash point around the time of the incident. It is therefore important for the financial investigator to visit the area where the incident has occurred. This is a fairly reliable way of identifying potential witnesses however with a caveat that a card maybe being used by someone other than the card holder. Care should also be taken in the setting of the parameters for such an activity as the amount of information gathered may be considerable.

4 Tasking and the Use of Financial Investigators in Major Crime

For the reasons already outlined above, it is always advisable to call a financial investigator into an investigation at an early stage. They need to start to gather information quickly if the information gathered is to be of use in generating other lines of inquiry. Some of the information may take at least seven days to obtain. The ideal situation would be to have a financial investigator dedicated to the investigation. Where this is not possible an ongoing liaison with a resource such as the force financial investigation unit could provide the same service. Financial investigators can advise the SIO in the following:

a) Writing of strategies for the gathering of financial intelligence including as part of strategies such as family liaison and search.

b) Tactical deployments to achieve those strategies.

c) The legal powers and policy that effect the gathering of this information.

d) The interpretation of the information gathered and its significance for the investigation.

e) Conversion of financial information into evidence.

When tasking a financial investigator it is sometimes more productive to give them parameters to work within and outline the desired outcomes. As stated previously, the problems that investigators have in relation to what can be achieved lie in not knowing what there is to access and where to find it.

Financial investigators should be included in briefings so they can identify areas in the investigation where they can further contribute; they also need to liaise with other key people in the enquiry such as:

- Family liaison officers;
- Exhibits officers;
- Search teams;
- Interview teams;
- Analysts;
- Surveillance teams.

The early deployment of a financial investigator in this way will ensure that financial information is effectively incorporated into the investigative strategy.

5 Conclusion

Financial information has the potential to provide SIOs with a rich source of material. Clearly, the exact contribution to the investigation will be determined by the circumstances surrounding the enquiry. While it may not be decisive in every case, it will present a massive intelligence opportunity in all but the rarest of investigations. Despite this, the full potential of this type of information is often overlooked. Therefore the SIO must explore the full potential presented by financial information at an early stage on the investigation.

The Legal Framework for Acquiring and Using Passive Data for Policing Purposes

Giles Herdale
Head of Professional Practice, NPIA

Abstract

Data is being gathered by organisations for a wide variety of purposes all the time. This covers such diverse issues as phone billing data, through banking or shopping transactions and use of the internet, to monitoring of locations through CCTV and ANPR. This so called passive data, distinct from information and intelligence specifically gathered by the police, has multiplied in recent years. This has prompted concern in certain quarters, including the Information Commissioner that we are sleepwalking into a surveillance society. However, it is undoubtedly the case that much passive data can be of significant benefit to the prevention and detection of crime. This article examines the legal basis for acquiring such information and highlights some of the challenges about using it successfully, focusing on the issue of human rights, data protection and RIPA.

Contents

All correspondence should be addressed to: NPIA Covert Advice Team, Specialist Operations Centre, Wyboston Lakes, Great North Road, Wyboston, Bedfordshire MK44 3BY
soc@npia.pnn.police.uk

1 What About Human Rights?

The Human Rights Act 1998 (HRA) has been blamed for everything from prisoners being able to access pornography to why terrorists cannot be removed from the UK. In fact the UK was bound by the European Convention on Human Rights (ECHR) before the introduction of the Human Rights Act. All the HRA has done in strict legal terms is to give jurisdiction to UK courts for considering breaches of ECHR. There has however undoubtedly been a more significant and fundamental cultural shift as a result of the HRA and the widely held belief that public authorities cannot act in a way incompatible with convention rights.

The implications for passive data centre on article 8, the right to respect for a private and family life. This right is not absolute however, it must be set against the other convention rights, including the right to life (article 2). The ECHR also recognises that there are circumstances where article 8 may be interfered with. The key principle here is that any interference must be lawful, in pursuit of a legitimate aim, necessary and proportionate.

Where passive data is concerned the legal focus here for whether article 8 is engaged is through the Data Protection Act 1998 (DPA) and Regulation of Investigatory Powers Act 2000 (RIPA).

2 What is Data Protection?

The DPA provides the legal framework for managing personal data (defined as information about a living individual processed electronically or on a defined filing system) in accordance with the ECHR. The DPA also defines a further category of sensitive personal data about such matters as a person's sexuality, involvement in any criminal matter or membership of a trade union etc. It should be acknowledged here that there is no direct read-across between personal data and article 8. Personal data is a much broader concept than 'private information' (not defined in DPA) which is 'significantly biographical' and engages article 8 issues around an individual's reasonable expectations of privacy.

Any organisation holding or processing personal data must be registered with the Information Commissioner and abide by the eight data protection principles set out in the DPA. This means that when dealing with an organisation that may have data that you need (defined in the Act as a data controller), you need to understand the implications of the DPA. It is important to bear in mind that the protections offered by the DPA are proportionate to the nature of the information in question. There will rightly be a higher

burden to share details of a person's sexuality for example than whether they were present at a particular public place at a certain time.

The DPA has had a bad press, with many commentators critical that data protection flies in the face of common sense. In fact most of the perverse outcomes blamed on data protection have come about not through the ruling of a court, but because a data controller has taken a restrictive and risk-averse interpretation of the requirements of the Act.

Contrary to much popular opinion the DPA does not prevent information being shared between data controllers and the police. There are examples of specific statutory gateways allowing data to be shared (such as section 115 Crime and Disorder Act 1998). In some cases this will be through some form of protocol, such as an information sharing agreement between agencies to exchange certain information. Many such agreements exist in the context of partnership arrangements such as Crime & Disorder Reduction Partnerships (CDRPs) or Multi-Agency Public Protection Arrangements (MAPPA).

An information sharing agreement does not, however, have to be in place to make information sharing legal. Moreover there is a specific exemption within the Act (section 29) to some of the DPA principles where those principles would be 'likely to prejudice' the prevention and detection of crime or the apprehension or prosecution of offenders. The key issue is that a clear policing purpose is advanced for why the information is necessary, and that the information in question is proportionate to the specific policing purpose being advanced.

It will often be the subsequent use or analysis of information, rather than the obtaining of it, that will give rise to privacy considerations, such as where information from a number of different sources is aggregated to build up a detailed picture of someone's lifestyle. Again the principles of necessity and proportionality apply.

More information about the relevance of DPA to policing is contained within the ACPO (2006) *Guidance on the Management of Police Information.*

3 What About the Regulation of Investigatory Powers Act 2000 (RIPA)?

The third statute that has become a whipping boy for law enforcement and politicians alike is the Regulation of Investigatory Powers Act 2000 (RIPA). Conceived at the same time as the HRA to provide an all-encompassing regulatory umbrella for a wide range of covert and to some extent unregulated activities it covers the interception of communications,

acquisition of communications data, directed and intrusive surveillance, conduct and use of covert human intelligence sources and encrypted data.

RIPA can provide specific lawful authority to intercept communications, acquire and disclose communications data, require disclosure of electronic data protected by encryption and to interfere with a person's Article 8 rights by means of covert surveillance and the use or conduct of a covert human intelligence source. RIPA is only relevant to passive data in limited circumstances. Covert surveillance, CHIS and the interception of live communications are concerned with the conscious gathering of information about individuals (without their knowledge).

Communications data (telephone subscribers, itemised billing etc) and electronically encrypted data (passwords, access codes etc) are examples of passive data which can be obtained with the appropriate RIPA authorisation. Communications data is defined in section 21 of RIPA "as any traffic data comprised in or attached to a communication". It is not the content of the communication itself but information about how and when it is delivered. As such communications data is gathered by communications service providers (CSP) for the purposes of charging, monitoring use of the network. This information is highly valuable for specific policing purposes as it can help identify who communicated with whom, when and where that communication took place, even though the content of the communication itself is not disclosed.

RIPA establishes a regime for using such material for a limited number of specified purposes, including the prevention and detection of crime, through specific channels set out in the Acquisition and Disclosure of Communications Data Code of Practice, including the appointment within each force or agency of an accredited Single Point of Contact (SPoC). The code is available at the following link: http://security.homeoffice.gov.uk/ripa/publication-search/ ripa-cop/acquisition-disclosure-cop.pdf. Once obtained, the use and processing of any communications data then becomes subject to the DPA.

Certain content of communications is stored by the telephone companies, for example a voicemail, and technically falls within the definition of passive data as it is data held by the company pending delivery or for the recipient to access whenever they wish to. This type of communication can be obtained from the company in a number of ways, including a PACE, schedule 1, production order. However if you have consent of the sender or the intended recipient of the voicemail then, along with a RIPA authorisation, the content can be lawfully obtained.

Directed surveillance, in which an individual is targeted with the aim of acquiring private information about them without their knowledge, is outside the scope of this article. By definition passive data, which is not covert, will fall outside the directed surveillance definition.

Any subsequent processing or analysis of such data (eg, linking images to biographical information about names and addresses, transactions or movements etc) may, however, enable a detailed picture to be painted of a person, their family or associates. Where this amounts to interference with that person's Article 8 rights, the DPA would provide an appropriate lawful authority.

4 Terrorism Act Passenger Data

The increased availability of data about international travel has obvious benefits for prevention and detection of crime, which is increasingly a cross-border phenomenon. Terrorism being an obvious but by no means the only example of cross-border criminality. Schedule 7 (paragraph 17) of the Terrorism Act 2000 provides a power for an examining officer to apply to the owners of specified ships or aircraft in writing for details of passengers, crew or cargo which must be supplied as soon as reasonably practicable.

5 Conclusion

Space precludes a more detailed consideration of the issues highlighted above, and it is important to remember that each case must be considered on its own merits. There is a dearth of case law on both DPA and RIPA, and so many of the views expressed above are just that, opinions, and have yet to be tested in case law. However there is a growing body of opinion that recognises that it is incumbent upon law enforcement to make the case that the acquisition and use of passive data can be justified as being entirely compatible with the framework of human rights provided by the ECHR.

Further advice and guidance on the issues raised is available from:

- ACPO (2006) *Manual of Guidance on Data Protection*
- ACPO (2006) *Guidance on the Management of Police Information*
- ACPO (forthcoming) *Guidance on the Lawful and Effective Use of Covert Techniques*

References

ACPO (2006) *Guidance on the Management of Police Information*. London: NPIA.

ACPO (2006) *Manual of Guidance on Data Protection*. London: NPIA.

ACPO (forthcoming) *Guidance on the Lawful and Effective Use of Covert Techniques*. London: NPIA.

Home Office (2005) *Acquisition and Disclosure of Communications Data Code of Practice* [internet]. London: TSO.
Available from: http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/acquisition-disclosure-cop.pdf.

Think Crime, Think Car, Think ANPR: The Use of ANPR in Major Crime Investigations

DCS Stuart Kirby, Lancashire Constabulary, and Det. Supt. George Turner, Thames Valley Police

Abstract

Many investigators will be aware of Automatic Number Plate Recognition. (ANPR) most notably through its use in identifying vehicles of interest allowing police to deploy intercept capability to take immediate action. This paper takes a wider view of ANPR technology, exploring its potential to identify suspects and witnesses, as well as more generally assisting the detection of major and complex crimes, in a more cost effective manner.

Contents

All correspondence should be addressed to:
John Dean, ACPO National ANPR Co-ordinator, Chair of ACPO National ANPR User Group
john.dean@npia.pnn.police.uk

1 Introduction

A statistician recently revealed that whereas in 1950, Britons travelled an average of five miles a day they now travelled 30 with the next generation being expected to travel 60 miles per day[1]. For those of us who continually battle with congested roads in our daily commute to work, those figures will feel all too familiar. However criminal psychologists explain to us that, as the general public travelling further, so do offenders who extend their reach to both target more lucrative victims and to protect their anonymity (Canter, 2003).

It is within this context that the government and ACPO have seen ANPR as a critical tool to 'target criminals through their use of the roads'. In recent years the benefits of the technology have been most apparent in police intercept teams who are able to check, within seconds, whether motor vehicles passing before them are flagged as being 'of interest' to the police. This has allowed police officers to stop the drivers of such vehicles and, if appropriate, arrest or report them for particular offences. The benefits of this intelligence based targeted approach increases the productivity of the police significantly. However, as this article will go on to show ANPR has much greater potential. Before some operational examples are used to illustrate this potential the reader will be reminded of how ANPR works.

2 A Quick Recap: How ANPR can be deployed and how it works

Each police force will have ANPR cameras which will be deployed at dedicated fixed sites (often in conjunction with CCTV), as well as through mobile units in dedicated vans or fitted in-car systems. Of course other agencies, such as the Highways Agency and other commercial organisations also use a network of these cameras to provide considerable coverage on commercial premises such as garage forecourts.

The capacity of the technology is extensive. Each ANPR camera is able to read approximately 3,600 vehicles per hour and, within 2 seconds, complete searches against databases which include PNC, local and foreign force databases, DVLA and MIDAS[2]. Although the technology that enables this is complex the operating process is straightforward. Initially the ANPR camera takes an image of the vehicle, which is digitised allowing a record to be stored of the number plate (known as the patch plate). The characters of the plate are then checked against local and national databases through a Back Office Facility (BOF), which stores the registration mark for further analysis. Work is

[1] 'The Guardian' as reported in 'The Week' 23/12/06.
[2] MIDAS checks insurance records and identifies those cars which are not insured.

ongoing to ensure that all forces who use ANPR have a BOF and that these are linked to the National ANPR Data Centre (NADC). This work should be completed in early 2008 enabling national searches of ANPR data in support of homicide investigations.

The process produces two types of data. First there is 'read data' which relates to all the number plates passing through the camera site. ACPO guidelines state that this data should be retained in a searchable system in the BOF for a period of two years, and in the NADC for five years. Guidelines also state that retention of ANPR data for intelligence purposes should be authorised by a Superintendent if the retention period exceeds 90 days. Secondly there is 'hit data'. This is when the ANPR gets a positive reading from the database that the registration number is of interest. This data is stored for seven years (albeit this period is currently being reviewed and could be reduced).

3 How ANPR Can Be Used To Assist Investigators

It should be highlighted at the outset there are specific limitations to ANPR. At rare times (for example due to a non regulatory number plate being displayed), the camera is unable to record the plate correctly; therefore the absence of a vehicle on ANPR does not totally exclude the possibility of its presence at a particular time and location. Secondly it must be remembered that ANPR provides information on vehicle movements and this should not be assumed to be the movements of a particular individual.

In general terms, however, ANPR provides considerable information which is consistent with the National Intelligence Model's emphasis on intelligence, enforcement and prevention. In terms of intelligence products, ANPR provides data to inform strategic and tactical assessments as well as being used in the development of subject and problem profiles. Further the data can be used for many facets of enforcement. The previously published ACPO (2006) *Investigators Guide to ANPR* and ACPO (2007) *Advice on the Use of ANPR* outline these benefits. In reactive investigations it encapsulates the ability to:

- Identify vehicles being used to commit crime;
- Research the movements of possible suspects;
- Research the movements of a victim's vehicle and assist with victimology;
- Identify witnesses;
- Research an alibi.

Whilst in pro-active investigations it can help by:

- Researching the movements of a target;
- Locate a vehicle and its movements for a future surveillance operation;
- Informing a trigger or arrest plan.

Finally to assist in prevention and disruption it can be used to:

- Assist with situational crime reduction measures i.e. increasing surveillance opportunities and deterring offenders;
- Intercept suspect vehicles before they commit a crime;
- Enforce road traffic offences, identified through ANPR, to disrupt criminal activity and to seize uninsured vehicles from prolific offenders.

4 Analytical Products and Examples of Their Use

As time goes on more and more police forces are becoming adept at utilising ANPR in innovative ways to investigate crime and detect offenders. During the research for this article operational examples were provided by fourteen police forces (see acknowledgements below) outlining their approach in this area. Unfortunately there is insufficient space to fully reflect the scope of this approach however all these examples fit within six generic analytical products which have been developed to assist in both pro-active and reactive investigations. These approaches are as follows:

4.1 Vehicle Pattern Analysis

This is used to provide information relating to a particular vehicle, or group of vehicles, to show pattern of movement. An example of this followed the investigation into the fatal shooting of Constable Beshenivsky during November 2005. After a witness highlighted a specific vehicle, ANPR was used to assist in the identification of the vehicle. As enquiries continued further suspects were identified and ANPR was again used to show the association between these vehicles as well as their use in Bradford at critical times before and after the incident (see ACPO (2006) *Investigator's Guide to ANPR*).

4.2 Geographical Profiling

This relates to where a vehicle's ANPR data is placed on a map to show trends or specific journeys which can be assessed against particular crimes. For example the movements of a suspect vehicle may be seen to correlate with the times and locations for a burglary hot-spot. An innovative example of this approach was an investigation into three linked armed robberies taking place on separate days at Maidstone, Ashford and Margate. Investigators from Kent Police compared data from the ANPR cameras in the vicinity of each of the robberies and discovered that of the 40,000 vehicles recorded overall only two were in the vicinity of all three robberies. One of these vehicles was later found to be directly involved in the crimes.

4.3 Location Time Analysis

This allows ANPR data to be analysed to establish cloned plates as well as identifying potential stolen vehicles. For example, a search for a vehicle of interest indicated that it passed ANPR cameras in Liverpool at 10am and in London at 10.30 am. In due course the NADC will automatically populate a hot list of potentially cloned vehicles.

4.4 Sequential Pattern Analysis

This can be used to identify behavioural patterns for a vehicle of interest, exploring any changes to expected patterns. For example a vehicle of interest may normally pass through three ANPR cameras between 8.15am and 8.30am every weekday. However on the day of the crime the vehicle does not travel through these cameras, a change of behaviour which passes critical information to the investigators. Such an approach was used recently on a category 'A' murder enquiry in the Thames Valley Police area. The ANPR hit led to images of the suspect on the day of the murder. The ANPR and CCTV evidence was an unchallenged but significant part of the evidence that secured a man's conviction for murder with a a sentence of 30 years.

4.5 Post Incident Analysis

The analysis of ANPR data from specific cameras at specific times to identify potential offenders and witnesses to crimes that have already taken place. An example of this was a serious assault at Heathrow Airport which followed what was alleged to have been a 'road rage' incident. Witness accounts at the scene pointed to a 'people carrier' type vehicle being used and analysis of the ANPR data close to the scene established the registration mark of such a vehicle following in close proximity to the victim's car. Within an hour

detectives had the name and address of a suspect and a quick arrest enabled the speedy retrieval of vital forensic evidence. Further use was then made of the ANPR data to identify vehicles at the scene within thirty seconds either side of the event. This targeted approach identified 128 other vehicles from which more witnesses to the actual assault were found as well as other information shedding light on how the incident may have started.

4.6 Convoy Analysis

This identifies vehicles of interest that are travelling together. An operational example is during the latter part of 2005 when six 'car key' burglaries occurred in Kent with no intelligence or information regarding potential offenders. Analysis of ANPR showed that three of the stolen vehicles left the county through the Dartford Crossing on the night they were stolen. ANPR back office searches then took place for five minutes either side of the stolen vehicles being identified to establish whether any vehicles were accompanying them. On each occasion a particular vehicle was seen to be travelling along the same or an adjacent lane within one minute of the stolen vehicles. Further searches showed that this vehicle had used the Dartford Crossing at the time of the other three burglaries. The analysts therefore suggested this vehicle as the one responsible for transporting the offenders to commit the burglaries. A short time later a further burglary was committed with a high value vehicle again being stolen. Equipped with the intelligence from the ANPR analysis, officers quickly deployed to the address of the owner of the target vehicle and established that the vehicle had been used recently. The owner was arrested and a further two stolen vehicles were found at his home.

5 The Media

As the examples above have shown ANPR is being discussed more and more in open court and the media have seized upon this as a further innovative method being used by the police to apprehend offenders. As such ANPR is being explained more and more in the media and this will no doubt continue as capacity increases and this technology is used more and more by commercial enterprises. As such SIOs should be comfortable in their disclosure to the media surrounding the use of ANPR in the apprehension of an offender. As with any technique however, care should be given not to dilute its effectiveness through educating offenders. In this regard investigators should be circumspect before revealing the exact location of an ANPR reader especially if the location is to be used in the future, or discussing how the data was analysed.

6 Conclusion

This short article has attempted to show that whereas ANPR might have initially been viewed as a high profile intercept tool for the Police Service, it has considerable potential beyond this remit. The large-scale investment and strategic deployment across the UK of ANPR technology provides far-reaching scope for its use in the investigation of major crime. Examples are being seen of investigators using ANPR in the way that CCTV and telephony are currently being used to build intelligence and evidence, as outlined in the 'passive data' section of the new ACPO (2006) *Murder Investigation Manual.* What this technology also does is to allow the investigator to target his or her resources, enabling a cost effective method of identifying suspects and witnesses, and of corroborating accounts. In the environment of ever tighter resource allocation this has to be welcomed.

Acknowledgements to:
CC Frank Whiteley (chair of ACPO, ANPR steering group),
ANPR Crime Investigations Working Group',
Det. Supt. Andy Brennan (W.Yorks),
DCI Colin Sutton (MPS),
A/Det. Supt. Steve Tolmie (TVP).

The following police forces for providing examples:
Bedfordshire Police,
Cumbria Constabulary,
Essex Police,
Gwent Police,
Hertfordshire Constabulary,
Kent Police,
Lancashire Constabulary,
Metropolitan Police Service,
Northumbria Police,
North Wales Police,
National Crime Squad,
South Wales Police,
Sussex Police,
West Midlands Police.

References

ACPO (2006) *Investigator's Guide to ANPR*.

ACPO (2006) *Murder Investigation Manual*. Wyboston, NPIA

ACPO (2007) *Advice on use of ANPR data*.

Bradford Telegraph & Argus 4.12.06

Canter, D.V. (2003) *Mapping Murder: The secrets of geographical profiling*. Virgin Books.

Stealing Time: The Use of Passive Data During Operation Nuthatch

DI Andy Tennet and Sergeant Hugh Dixon, Northamptonshire Constabulary

Abstract

Operation Nuthatch was the investigation into a triple fatal road traffic collision on the M1 motorway, which rapidly escalated into a long-term enquiry into a haulage company for offences of Corporate Manslaughter. This report details the course of the investigation; the obstacles the enquiry team overcame and the use of passive data that helped secure the first ever guilty pleas to Corporate Manslaughter.

The investigation would result in a change to the way in which Northamptonshire Police managed its investigations into such incidents and the training and configuration of its Road Policing Department

Contents

All correspondence should be addressed to: DI Andy Tennet,
ROSE Project, Ground Floor, Albion House, Victoria Promenade, Northampton NN1 1HH
andy.tennet@northants.police.uk

1 Introduction

Prosecutions of corporate manslaughter are still fairly rare and convictions even more so. As such the pool of knowledge available for reference is pretty small.

Operation Nuthatch started with a devastating collision and subsequent 'pile up' on the M1 motorway, just north of junction 15a, in the vicinity of Rothersthorpe, Northamptonshire. The vehicle at fault was a large goods vehicle and an early examination of the cab's tachograph chart suggested that for some time prior to the accident, the vehicle had allegedly been stationary – a statement which was obviously wrong. In addition the tachograph mechanism itself had been tampered with.

As the investigation continued so it became apparent that this was not a straightforward collision. The Road Policing Team working on the enquiry sought advice from the force Homicide and Major Crime Team which later led to the appointment of an SIO and the move onto HOLMES II. This was the first time Northamptonshire Police had run an investigation, which bought together the two disciplines of major crime and road policing.

Early advice and guidance from the Crown Prosecution Service proved vital to the direction of the enquiry, which ran from the 27th February 2002 to its conclusion at Northampton Crown Court on the 3rd December 2004. This case has particular significance in that it was the first guilty plea to Corporate Manslaughter.

This paper will try to share with other investigators the lessons learnt by the Op Nuthatch team in respect of joint working, case preparation for such an offence and the vital role that passive data played in the enquiry.

2 Background

Keymark Services was a haulage company based in Queensborough, Kent. The company had two directors, Melvyn Spree and his partner (in both business and life), Lorraine March. Apart from the drivers employed by the company, the only other employee was a secretary Claire Miller.

The company had a fleet of around 12 to 15 lorries, which in turn were maintained and serviced by Abbey Coachworks who operated from the same site and was owned by Melvyn Spree.

The company, its directors and a number of the drivers had existing convictions for breach of driver hour regulations and on one occasion had been caught breaching the legislation whilst already waiting to go to court for previous offences.

In all the company employed a dozen drivers full time, another three or more part time and Melvyn Spree himself drove when required.

One of the full time drivers who had worked for Melvyn Spree for some time was Stephen Law. At 10.30am on 25th February 2002 Stephen Law left Keymark Services in his LGV[1]. He was towing a refrigerated trailer and over the following two days Stephen Law worked almost continually and far in excess of the lawfully allowed driving hours.

[1] Large Goods Vehicle

At 15.16pm on Wednesday 27th February 2002, the lorry and trailer driven by Steven Law was involved in a road traffic collision on the M1 motorway near to the Rothersthorpe Services.

The lorry was travelling north and was on the nearside lane. Even at this time it would appear that Law was not heading back to Keymark Services but was en route to deliver another load in Leicestershire. Witnesses described how the lorry slowly drifted across all three lanes until the vehicle and its trailer collided with the central reservation, mounted the railing and crashed into the opposite carriageway, coming to rest on its side. A number of vehicles travelling south were unable to avoid the wreckage, either crashing into the lorry, each other, being struck by debris or ending up down the embankment. In total seven vehicles were involved.

Three drivers lost their lives. One was Stephen Law; the other two were Benjamin Kwapong and Neil Owen innocent members of the public, going about their daily business. The result of the accident closed the motorway for some 12 hours, bringing delays and misery to the whole region if not more.

3 The Investigation

An early examination of Stephen Law's tachograph revealed that not only had it been tampered with but also that immediately prior to the collision the vehicle was shown as being 'at rest'. It was apparent that the information recorded on the chart recovered from the vehicle was not a true representation of his activities for the period recorded and as such this data could not be relied upon.

Due to the evidence found at the scene, initial enquiries made into Keymark Services and

liaison with the Vehicle Inspectorate it soon became apparent that there might be corporate accountability. As such, on the 4th March 2002 a team of officers was sent down to Kent to execute a search warrant at the company offices and the home addresses of the company officers.

A vast quantity of documentation was seized along with computers and other related items. An early assessment of some of these items suggested that the company were heavily involved in illegal activity particularly in respect of drivers' hours and tachograph regulations. In addition to this, officers examined the tachograph units fitted to the other tractor units in the yard at the time and found that nearly all had been tampered with.

One type of document that was not to be found at any of the premises searched was the drivers' personal time sheets. These would have given a clear indication as to the working hours and practices of the company's employees and would be vital in the calculation of drivers' wages.

Initially the enquiry was staffed and managed by officers from the Road Policing Unit. As the investigation developed advice was sought from the force Homicide and Major Crime department who took responsibility for the direction of the investigation and on the 17th April 2002 an SIO was appointed.

The investigation was further supported by putting it onto HOLMES II, appointing a trained exhibit officer and looking for support from other forces in respect of liaising with the families of those killed.

A meeting with our local CPS was arranged and this led to the submission of a short advice file to the CPS head office in York. They advised that it was necessary to demonstrate to what extent the illegal practices were being used throughout the company.

They required that the tachographs for each driver employed by the company be examined for the four months prior to the accident. Including the owner of the company, Melvyn Spree, and his driver who died, this amounted to 15 drivers, working week in and week out.

This would be a monumental piece of work and expert advice was sought. However, the best company that was available were unable to sign up to such a huge commitment, in addition to which the financial implications would be immense.

As such it fell to the investigation team to complete this work. As it was apparent that we would never complete the work for all the drivers within the 6-month statutory time limit, it

was agreed that we would not prosecute the drivers for offences under the tachograph legislation but would look to prove offences of forgery.

Whilst this work was starting to develop, the enquiry was referred to the Casework Directorate in Birmingham who specialise in Corporate Manslaughter cases. Anamarie Coomansingh was appointed as the reviewing lawyer and point of contact.

It was agreed that we would prosecute each of the drivers for any offences committed in the four-month period prior to the accident. If it were found that such offences were endemic within the company and secured convictions against the majority of the drivers, the certificates of conviction would then form the bedrock of any prosecution against the company and its officers for Corporate Manslaughter.

Prior to the commencement of this work, it was imperative that we look to prove beyond reasonable doubt that the accident was caused by Stephen Law falling asleep at the wheel due to driver fatigue. As he had been alone in his cab, there were no witnesses to corroborate this. As such we needed to explore every other possible cause of the accident. These included:

- Tyre blow out – one of the tyres on the cab had blown but was this prior to or during the accident?
- Any mechanical defect with Stephen Law's vehicle?
- Had he been on his mobile phone?
- Were the weather conditions a contributory factor?
- Was there another vehicle involved which had caused the accident but not yet been traced?
- Did Stephen Law have any medical condition known or unknown to him, which might have caused the collision to occur?

All of the above possibilities were ruled out which left us with the only reasonable conclusion, that having driven for nearly two days, Stephen Law fell asleep at the wheel of his lorry.

Initially files of evidence were built up for just two of the drivers employed by the company. Amongst the documents seized from Keymark Services were almost all the tachographs for

each driver, for each day. In addition, we had all of the daily delivery schedules completed by Melvyn Spree. These were hand written by him and detailed all collections and deliveries for each day for each driver. By comparing the tachograph for any particular day with the delivery log for the same day we started to build up a true picture of each driver's activity on any given day.

This was further supported by a number of types of passive data generated by the companies who contracted Keymark Services and other sources. The majority of these contained more specific timed data, which is explained further in this report.

Officers were tasked with examining the enormous quantities of tachograph charts, invoices and other driver records and to separate out those that could be identified to individual drivers. It was agreed with the CPS that we would identify all the companies visited by Keymark Services during the period of 1st November 2001 to 28th February 2002 and to then ask for production of their security gate records or delivery receipts.

This resulted in a huge volume of actions for the enquiry teams who travelled the length and breadth of the country visiting companies and gathering evidence. The office manager would try to map out the companies to be visited to allow as many to be covered in each trip some of which took two or three days. The bulk of this aspect of the enquiry took almost four months to complete. Each visit generated new documents and data all of which had to be analysed and compared with the company records.

The tachographs themselves were photocopied, magnified and exhibited. These copies were then used as working copies, being used to mark up the timed activities obtained from the other passive data sources.

Slowly we built up chronological evidence packages for each driver. Each contained the working copy tachograph together with supporting evidence and copy documentation.

Once the initial evidence packages were prepared we started to contact the individual drivers and arrange for them to present themselves at pre-arranged police stations for interview. They were asked to provide details of their legal representative (if selected) and such was our confidence in the level of evidence we had against each driver, full and early disclosure was made either to them personally or to their solicitor some weeks before the interview date.

Without exception each driver fully admitted to all of the offences highlighted in their specific report. Each was charged with two specimen offences of forgery for each of the four months we had examined and had the rest of their offences taken into consideration.

We started to interview the first of the drivers whilst still compiling the evidence packages against their colleagues, the whole process taking sixteen months to complete. By the end of this process each driver had eight specimen charges and they had in excess of 400 offences taken into consideration.

Whilst most of the drivers were interviewed and charged in Kent, they were all bailed to Northampton Magistrates Court, where without exception, they all pleaded guilty to all of the charges on first appearance.

Once each had been dealt with at court they were approached with a view to providing a witness statement in respect of working practices at the company. The vast majority did so although the degree of detail they were prepared to go into varied.

4 Interview and Charge

4.1 Claire Miller

By the end of May 2003, the team were in a position to focus on Claire Miller.

Miller was the officer manager who had responsibility for checking tachograph charts and drivers' hours to ensure they complied with the legislation, along with maintaining the records relating to driver discipline issues.

By now it was clear that there were massive abuses of driver hours legislation by each and every driver and that there must have been knowledge of this within the company offices. Evidence was found amongst the documents seized from the company offices that Miller not only knew of this abuse but actively took steps to disguise what was happening from the relevant authorities.

Miller was invited in for interview on the 5th June 2003 and was arrested on suspicion of forgery and attempting to pervert the course of justice. Throughout the interview she denied any wrongdoing but admitted she was aware of some of the abuses. Miller claimed that anything she found she passed straight to Melvyn Spree or Lorraine March for them to deal with.

Miller was released on delay charge bail.

4.2 Melvyn Spree and Lorraine March

Full disclosure was made to both Spree and March almost a month prior to interviewing them. Due to the volume of evidence against them we had to arrange for personal delivery of the boxes of documents to them both. They presented themselves at Kettering Police Station in early July 2003 with their solicitor. A dedicated custody officer was assigned to the team and over the next five days both March and Spree were interviewed in respect of the mass of evidence we had uncovered.

The initial interviews concerned the activities and working practices of the company employees and concentrated on the falsified tachographs and records. This was time consuming and laborious and took four days to cover.

The final day of interviews focused on their individual roles and responsibilities within both Keymark Services and its sister company Abbey Works. The last journey of Stephen Law was also covered in some depth.

Throughout all the interviews Spree maintained his right to silence whilst March denied any knowledge of any wrongdoing blaming any such activity on other people within the company. Both were released on delay charge bail for a four-month period to allow the CPS to consider all the papers.

This process took much longer than anticipated and March, Miller and Spree finally answered their bail in November 2003 at which point they were further interviewed. Again, they were released on delay charge bail.

5 Sources of Passive Data

The vast majority of the evidence against Spree, March, Miller and the registered company of Keymark Services, came from passive data. The various types of data collected over the course of the investigation are described below.

5.1 Tachograph Records

The biggest of these had to be the tachograph records recovered from the company premises and from Stephen Law's vehicle. A tachograph is a precision instrument, which acts as a speedometer and at the same time records on a circular chart the speed of the vehicle, the distance travelled, driving and stationary time. The tachograph head is

mounted within the dashboard of all large goods vehicles. The head records information on a circular, cardboard chart the size of a CD. The data is recorded in the form of a number of thin line traces which can then be used to analyse the activities of the vehicle and hence the driver during the working day. A new chart should be recorded for every working day a driver completes and should also include details of the journey undertaken, the driver and the start/end odometer reading.

The ability to read a tachograph, interpret any information and identify issues of concern is a skill which requires specific training and plenty of experience. Whilst the examination of such documents is routine in the course of Road Policing, their use in this investigation went far beyond the normal boundaries in terms of the volume of charts included in the analysis.

The legislation that covers driver hours is normally dealt with summarily and as such has a six-month deadline on proceedings. Obviously with an investigation of this size and nature, six months was never going to be achievable and therefore we proceeded under Section 1 of the Forgery and Counterfeiting Act 1981, treating each of the tachograph charts as a forged instrument. This removed the need to analyse the tachographs within six months and required a more achievable level of proof than that required under driver hours' legislation. The CPS supported this decision.

In excess of a thousand charts had to be analysed. Each one was examined in detail and the date, times, location, driver name and vehicle recorded on each one was transferred to a spreadsheet setting out the alleged activity recorded on the tachograph.

5.2 Keymark Services Daily Traffic Sheets

Some of the first documents to compare against the tachographs were the records of projected deliveries and pick-ups maintained by the company and almost entirely by Melvyn Spree. These were in effect a "desk diary" into which details of all contracted work was entered on a daily basis, this included job reference number, driver and vehicle allocation, details of journey and re-numeration. This information gave us the basic daily work schedule for each driver and enabled the enquiry to identify and research timed data to overlay and compare with what was recorded on the tachograph charts.

This process was one of the most time consuming parts of the enquiry.

5.3 Company Security and Delivery Records

From the traffic sheets we identified dozens of companies to whom Keymark Services had been contracted. The majority were large national and international retailers or were in the process of supplying retailers.

As the majority of goods delivered by Keymark services were chilled foodstuffs, it was critical that the companies kept accurate records detailing exactly when and where goods were delivered or collected. In addition to this, the sheer volume of vehicles in and out of some of the depots meant that drivers had a specific time slot in which to arrive and leave. Drivers who fell outside of their allotted time period stood the risk of being turned away or having to wait for another slot.

As such each company had to visited individually, the relative records located, seized and evidenced. For some companies this was a monumental task, as we needed to go back through months and months of records, either held on computer or on a paper based system. In the majority of cases these records were hand written. The quantity and quality of the data varied greatly but usually recorded times in or off site, drivers name or company name and or registration number. Occasionally, only a load reference number would be quoted and some records were computer-generated printouts listing hundreds of daily traffic movements. These had to be examined manually to identify the relevant vehicles and information.

The team got into a system of identifying groups of companies, phoning them some days before hand to detail the investigation and what we required of them in terms of evidence. The enquiry teams would then be sent out, sometimes for days at a time, to tour round the companies recovering the data we required.

Again, this information was overlaid against the tachograph and delivery logs on the spreadsheets. As we did this an even clearer picture began to emerge in respect of the real journeys undertaken by the drivers.

5.4 DART Tags

Keymark Services were based in Kent and as such the company's lorries would travel across the Dartford bridge or through the Dartford tunnel on an almost daily basis. To allow them to proceed without having to stop and pay the toll fee, each vehicle was fitted with an individualised, serialised tag. This was a precredited electronic tag that when the vehicle approached either the bridge or tunnel the tag would be automatically read, recording the time and date of activation, the fee debited from the tag.

The company that managed the DART tags was approached and again were able to provide evidence from their data records with respect to the tags issued to Keymark Services. This took the form of a computer print out detailing each crossing made including the time, date and geographical direction of travel. Yet again, this data was overlaid against the evidence on the spreadsheets.

5.5 Fuel Cards

In much the same way as the DART tags, each driver was issued with a fuel card, allocated to a specific vehicle, with which to pay for fuel. Again, the company which operated this service was approached and was able to evidence when and where each vehicle was filled up with fuel. Yet again, this was added to the growing evidence being collated on the spreadsheets.

5.6 Telephone Records

It was soon apparent that the drivers employed by Keymark services were controlled and directed via their mobile phones. Obviously, no amount of phone analysis would prove or disprove where each driver was each time a call was made or received on any particular mobile phone.

It was however necessary, to ascertain if Stephen Law was on his mobile phone at or immediately before the accident occurred. Phone records were obtained for both incoming and outgoing calls and this showed that he was not on his mobile phone at the time of his accident.

5.7 Satellite Tracking

In the later stages of the investigation, it was discovered that a satellite tracking system had been purchased by Keymark Services and installed in all of their vehicles. This information came to light during one of the later drivers' interviews.

As a result of this a check was made of Stephen Law's vehicle, which was still in our possession, and a 'black box' was found fitted behind the dashboard area.

The company that had supplied the tracking device was contacted and confirmed that they had fitted the devices to all of the vehicles operated by Keymark Services. The data the system generated was automatically down loaded to and recorded on the hard drive fitted to Keymark services main office computer whenever the vehicle entered the yard at the operating base.

We had already seized and examined this computer but within the force, did not possess the necessary software to access or interrogate the tracking data and therefore it had not been recognised for what it was. A copy was made of the computer hard drive and this was supplied to the service provider, Minor Planet Ltd who was then able to produce extremely detailed information in respect of each vehicle's activity during any specified time period.

In fact we were faced with information overload in that the company could supply too much information amounting to thousands of pages of data. In effect they could tell us where each vehicle was at any minute in any day.

After some discussion we were supplied with data showing the location and time of each vehicle for every occasion that the ignition was turned on or off. The data supplied showed the exact location of each vehicle when the ignition was switched off for loading, unloading, fuelling, during breaks etc. This was sufficiently detailed to corroborate the data and the analysis completed to date.

6 Investigative Considerations for Passive Data

The use of passive data throughout the investigation raised a number of issues, which needed to be addressed.

6.1 Data Collection

The collection of such varied forms of data generated a vast quantity of information, only a relatively small proportion of which was valuable to the investigation. The difficulty in determining which information was likely to be of use to the investigation was further compounded by the fact that the data was collected, stored and retrieved in a way not necessarily suited to the requirements of a criminal investigation.

It rapidly became clear that we were at risk of being overwhelmed with information which may not be useful to the investigation. To avoid this we needed to first explore the full range of available information before setting clear objectives and parameters for each set of data

There were no data protection issues in accessing any of the data, as we were able to request information on specific vehicles.

Where information had been taken from a computer system we collected statements confirming the integrity of the system; that there had been no viruses and that the system

itself had not been interfered with. This prevented the defence from questioning the source of the data.

6.2 Interpreting the Data

Some of the data collected required individuals with specialist skills to interpret and comment upon it.

All the police officers employed to examine and analyse the tachograph charts and supporting documentation were experienced traffic officers who were previously trained to level 2 City and Guilds in tachograph analysis. In this investigation computer software and hardware was purchased to assist this process due to the volume of tachographs we dealt with.

As the investigation progressed the CPS recommended that we find someone qualified to comment on the running of Keymark Services as a haulage business. Both March and Spree held the Certificate of Professional Competence (CPC) which, in effect, qualified them as competent people to run a haulage company.

We explored this suggestion and found that to employ an expert in the field would be very expensive and as we needed advice on an almost daily basis, availability was an issue as well. As such three officers were nominated to attend a day release course at a local college to qualify them to CPC level thus qualifying them to actually take charge of and run a haulage company. This qualification enabled them (if challenged in court), to comment on the methods and procedures employed in Keymark Services.

In addition, whilst not applicable in every case, the training of officers to 'expert' level was a surprisingly inexpensive way to challenge or check evidence when compared with hiring in expert witnesses. The bonus for the force being that those officers are available for advice in this field for some time post investigation.

In addition to this, Council required that an independent expert be sought who would analyse and comment on the working practices employed by Keymark and Abbey Works and who could pass comment on the companies' failings when compared with what was regarded as best practice within the industry.

No such expert was known to the NPIA Specialist Operations Centre (then the National Crime and Operations Faculty) and as such the Transport Research Laboratory suggested the SIO contact Mr Alan Parker, who had previously been in charge of a number of national and international transport companies.

Mr Parker prepared an extremely detailed and damning report regarding the companies' working practices, especially with regards to Health and Safety issues.

Council also required that an expert in the field of driver's hours and tachograph chart analysis be found. In this respect the NPIA Specialist Operations Centre identified Mr Keith Lloyd of Burgoins Ltd.

He was employed to examine and comment on the investigative methods employed by the tachograph analysts, and also to verify the detailed analysis carried out by the police officer who examined the last three working days of Stephen Law. It is pleasing to note that not only did he support the findings but confirmed that the methodology employed throughout the investigation was beyond reproach.

Other specialists were employed during the course of this investigation to clarify certain evidential points in respect to passive data, including the interference with the tachograph unit in the lorry.

6.3 Disclosure

Due to the high volume of information collected from various sources, we made a full disclosure some weeks prior to each interview. This allowed the solicitor sufficient time to examine the material and advise their client appropriately.

6.4 Preparation and Presentation of Exhibits

In total there were in excess of 5500 exhibits to be presented at trial, the majority of which were comparatively technical in nature. In addition the significance of many of these exhibits was only apparent once placed into a wider context with a number of other exhibits. For example, the tachographs were only significant when coupled with the data collected from delivery records, satellite tracking data, DART tags, fuel cards and driver time sheets.

As a result, presenting the evidence from passive data sources in a clear, accessible and concise manner required much thought. The majority of exhibits actually put before the court were new exhibits created by the investigation team, which represented a culmination of a wider body of exhibited data. For example, Stephen Law's driving history over the previous six months was presented as a single spreadsheet. A large number of exhibits supporting this spreadsheet effectively sat underneath it, accessible to the defence if they chose to challenge the content of the spreadsheet itself.

7 Conclusion

This investigation proved to be extremely complex, time consuming and protracted. However following our experience, if we were faced with such an incident again it is likely that a similar investigation would be shorter as we would know what types of passive data are available and how to secure them.

Without doubt the thoroughness of the investigation and evidential package presented avoided the need for a lengthy and costly trial. Other forces have had 'not guilty' trials arising out of such collisions, which have lasted for up to four months.

The early guilty plea was a reflection of the hard work and diligence of all involved from start to finish, a period of some 32 months. The investigation had a direct impact on the manner in which our force investigates such incidents and the skills required by officers to conduct such enquiries.

The Road Policing Unit (RPU) now has trained Family Liaison Officers, Exhibit and Disclosure Officers as well as Vulnerable and Key Witness trained officers and Tier 2 interviewers (Tier 5 interviewers are to follow shortly). In addition, there is regular consultation between the RPU and the Homicide and Major Crime Team, and the RPU has its own dedicated and self sufficient Road Death Investigation Unit staffed by specially trained officers.

As a learning exercise, this investigation led to the use of a number of sources of passive data which was held by any number of companies and which had never been gathered or retained for the purpose of providing evidence but purely for the management of a business.

In effect, the investigation found that when you explore what passive data is available, the results can not only be quite surprising but when added to evidence gathered from the more traditional sources, can be a great source of independent corroborative information.

Do They Know More Than We Do? What Opportunities Are To Be Gained From Data Held by Other Organisations

Ray Green
Director, Focus Data Service Ltd

Abstract

Ray Green previously worked for what was then called Customs and Excise. He then moved to the private sector where he initially ran the investigation department of a telecommunications company and worked as the main liaison with the police during that time. He is now the Director of Focus, a forensic telecommunications company which manages telephone data for a number of forces.

Personal data is now routinely collected and stored by many companies, websites and other organisations. Does this data represent an opportunity to improve the efficiency of the investigative process? Four classes of data are explored in the article; restricted, company, commercial and open source. The potential and limitations of each are examined together with the issues surrounding obtaining timely, lawful and cost effective access.

Contents

All correspondence should be addressed to: Ray.Green@focusdata.uk.com

1 Introduction

An increasing amount of personal data is collected and stored every day by a whole variety of organisations. The purchase of goods over the internet, Paypal, loyalty cards such as Nectar, Friends Reunited, YouTube and even having to enter you car registration to buy a 40p car park ticket! It seems that everything you do creates a record. Edmond Locard, the father of forensic science said, "every contact leaves a trace". If he were alive to day he would probably say, "every transaction leaves a data trail". The question for resource challenged police forces is whether this data represents an opportunity to work smarter rather than harder. Can this data be used to assist the investigation of crime? If it can, then what knowledge and skills are required and how do forces gain access to it?

2 What Does the Industry Hold and Why?

Over the last few years the British government has privatised and deregulated industries causing a significant diversification in the provision of utilities. Previously, if you wanted to check on an address you would ask the incumbent gas, electricity or telephone company for details. There are now multiple virtual suppliers who might hold details. There are 17 potential suppliers of electricity for my home for example. Similarly, people change banks and credit cards much more frequently, all of which increases the complexity.

Another facet of this diversification has been the outsourcing by companies of functions such as servicing, distribution, customer care, call centres and marketing campaigns so that data is created and held by third parties. There is also the outsourcing of complete business operations in the form of branded services. For example, Tesco mobile phone is run entirely by O2. This can result in confusion as to the identity of the Data Controller authorised to release information to third parties. In larger organisations there is often a Data Protection Officer who can define this.

In broad terms let's categorise data sources in the following terms

1. Restricted Data – Closed data held by Public Authorities that is classified under restrictive markings.

2. Company Data – Closed data held by public or commercial organisations under Data Protection Act. The release of this data to Police would be at the discretion of the Data Controller under section 29 of the Data Protection Act.

3. Commercial Data – Open data held by commercial organisations that can be purchased such as subscription services like Equifax, or marketing lists etc.

4. Open data published freely and accessible via for example, the Internet.

Other than the social network sites such as Friends Reunited, the data that most commercial organisations collect is for a purpose and that is normally in order to:

1. Raise an invoice;
2. Obtain payment (credit card or Bank mandate);
3. Deliver goods or services;
4. Extend credit;
5. Market in future;
6. Manage loyalty schemes (Nectar etc).

And is normally restricted to:

1. Name;
2. Address;
3. Date of birth;
4. Gender;
5. Card number;
6. Bank account.

3 Accuracy and Currency

The value of any data largely depends on its accuracy and how up to date it is, or its currency. At one end of the scale there is open source data on the internet. It's quick and free but its accuracy and currency will be very variable.

Company data collected by organisations for their own purposes and kept confidentially is governed by the Data Protection Act (although the Act is barely enforced). The accuracy of that data will be governed by the purpose it is collected for and the ease of the "customer experience". We all want to log on, register and then do or use what we have just purchased.

Let's examine something that most will be familiar with; the subscriber details for prepay mobile phone. Mobile phone companies collect this as either a requirement of service (Orange) or by encouragement with the payment of bonus minutes. No validation is made of the details given and there are many "Mr Mickey Mouse, c/o Euro Disney, Paris". It would be impossible to validate the subscriber details unless they were checked against Equifax or Experian and that would only validate that a person of that name resided at the given address. It would not validate that the person registering or user was the named person. The mobile phone could be sold next day to a different user and the details would not be changed. Therefore the accuracy and the currency of the data are poor.

Let's examine the accuracy of that data, or what validation is made by a commercial organisation to ensure that data is accurate.

No	Reason	Validation
1	Raise an invoice	None
2	Obtain payment – credit card	Chip & PIN **or** address & AVS/CV2 algorithm. Given the high levels of fraud with "Card Not Present" transactions this is not very effective.
2a	Obtain payment – Bank Mandate	Rejection by bank or rejection by customer when transaction appears on statement.
3	Deliver goods or services	Successfully deliver but would not be alarmed if unsuccessful as there is no loss.
4	Extend credit	Equifax of Experian check
5	Marketing	None
6	Loyalty schemes	None

These can generally be described as the least line of resistance checks with the exception of Equifax and Experian checks that are pro-active and incur a cost. It may go through some data cleansing to tidy up postcodes etc but not a lot. Therefore, the quality of the data must be regarded as "face value". Or in other words, it's what someone chose to tell me. It's probably not a lot better than internet data.

The big difference is the Equifax and Experian data that is compared to previous records and names are linked to previous addresses.

4 What Use is the Data to the Police?

Once you have established the quality of the data is, the next step is to define the questions you want the answers to. In keeping with normal best practice it is helpful to define the objective before you start. It is very easy to start "roaming" through data sources with one step leading to another – all very interesting of course. But as each check can cost money, it is very easy to run up a significant bill for data that is very interesting but that does not actually get you anywhere. It is a pit fall that inexperienced or infrequent users can easy slip into.

It is probably helpful to corral the enquiries into standard "questions". This will help rank and file officers appreciate where open source data might help. For example:

- Where does John Smith live?
- Does John Smith live at this address?
- Who lives at this address?
- Does John Smith have a mobile phone/bank account/credit card?
- Who is the user of this pre pay mobile phone?
- What car does John Smith drive?

These and other questions can be answered but not in every instance, there is an element of luck. Exactly what assistance can be provided from these data sources can only be established if the resource is allocated to research the potential and then develop the role. However, what use the data might be depends on the above questions being answered. Several scenarios can be imagined. Does a major pizza chain have a central call centre for taking orders for home delivery pizza? If so do they keep the telephone number of the inward call which would allow you to correlate an unregistered pre-pay phone to the address the pizza was delivered to? Has anybody asked the pizza companies what data they hold?

5 Ease and Speed of Obtaining the Data

The logistics of obtaining the data is obviously a consideration if it is to increase the efficiency of the investigative process. Anything that is slow, cumbersome and labour intensive may not by of assistance.

It is quite simple to find out who holds what data, you can go and ask them; the difficulty is managing the release of that data. Organisations are often very willing to assist the police but may be concerned that this may be perceived as not preserving customer confidentiality, unaware that section 29 of the Data Protection Act allows them to do so. If the release of data is to be voluntary under the Data Protection Act then the Data Controller can also choose not to release it. As the data will probably have value as intelligence, not evidence then court orders may not be cost effective or timely.

Therefore, a long-term relationship will need to be built that encourages the release of data. That relationship needs to be built on trust that both sides will stick to agreements or Memorandums of Understanding (MoU). Over enthusiastic officers driving to get a result on a particular case could test such relationships. It is difficult for commercial organisations to understand the individual force structure of the police, and the levels of command within.

The key considerations in managing a relationship with an organisation that stores and retains any potentially useful data are:

1. The relationship needs to be "owned" by one force that acts as the liaison conduit. The Director of Intelligence of the force where the informant organisation's Head Office is located would seem a logical post. That force should take the lead in establishing what data is available, negotiating agreements on access protocols and the ongoing management of the relationship.

2. Agreements must then be adhered to.

3. The relationship must be cost neutral to the data holder. The cost of providing the data must be borne by the Police. While in the short term, the providing organisation may be prepared to bear the cost, long term it will become an issue. Therefore, address that issue within the MoU. There are a number of request management systems already in use between telecommunication companies and certain forces. These assist in retrieval and cost reduction of accessing such data (eg, Focus 112, PLOD).

6 Political Issues

This is a sensitive area. At the time of writing a Parliamentary Select Committee is examining the topic of a "Surveillance Society" after warnings from the Information Commissioner that we are drifting towards one. Whatever conclusions the Parliamentary Select Committee comes to, the concerns are apparent. If this data is of use in the investigation of crime I would suggest that Parliament is unlikely to consider statutory powers to require disclosure without substantial justification. That substantial justification will be difficult to accumulate if you don't know what data is available and you do not have the skills to use it.

There is an increasing ground swell in "Middle England", the bedrock of police support, that they are penalised for being legitimate, eg, registered, tax paying and easily traceable. In contrast the criminal underclass is seen to escape such scrutiny because it's not cost effective to take enforcement action against those who do not engage voluntarily with official systems. All policing requires the consent of the population and nowhere is this more pertinent than in the use of personal data. This will require careful and thoughtful management.

7 Managing the Technical Demands Presented by Passive Data

The speed with which industry is diversifying and changing is an issue both for the industry itself and the police. As a 49-year-old, my use of the internet and other digital resources is entirely different to that of my 17-year-old son. The use of digital resources varies greatly across different social groups. A 20-year-old male may not enter his car registration to buy a car park ticket because he can't afford to insure a car, but he will have an I-Tunes and a YouTube account, use instant messaging and chat rooms. The challenge is to understand which digital resources a particular group might use in order to know where to look for information. The speed of change is quite breath taking and the adoption of new technologies very fast in some groups.

This may have significant implications for police management. The mature and experienced detectives working in a major incident room may not have sufficient awareness of technological activities to recognise potential leads in this area. Nor may they be the best people to understand the intricacies and implications of the data collected.

If the opportunity to work smarter is to be realised it will not be from within the general detective population in a force but from a smaller cadre of officers who have the aptitude and are able to develop the technical expertise required to effectively access and interpret

such information.The initial training requirements for a team specialising in such a rapidly changing area will be low and ongoing training will be, to use the marketing expression, viral amongst peers. Such specialist officers would also be better able to understand the industry's perspectives and constraints, and as a consequence, foster a stronger working relationship.

Most of the data may be of limited evidential value and so it would likely form an intelligence function. Locating such expertise within the intelligence bureaux with a small cadre of analysts or researchers may have a number of advantages:

1. development and sharing of expertise;

2. linking of cases;

3. containment of costs for commercial data services.

An important feature will be the facility for officers to request searches and receive the answer swiftly. An intranet request and response system is therefore essential.

8 Conclusion

Undoubtedly the various non-police sources of data represent a potential asset that can add value to police work in tracing individuals or by placing them at particular locations at a given time. It is difficult to envisage in future that less data will be captured and processed. However, police access to that data is a politically sensitive issue that must be observed.

In order to gain the optimum benefit from this a force will need to dedicate a few people (probably intelligence researchers) to gain the skills and knowledge to know how to access the data that will produce an answer and how to interpret the results. This centralisation within a force will assist to contain costs and ensure the relationships are preserved.

Data suppliers will need to be identified and agreements negotiated at a strategic level in force. The use of request management systems will be essential to streamlining efficiency and providing transparency for audit purposes.

Are We Killing the Goose?

John Fox,
Consultant SIO trainer, NPIA

Abstract

The use of passive data, and in particular CCTV product, is considered by most SIOs to be a desirable, if not essential, line of enquiry in any major crime investigation.

This paper discusses the proliferation of passive data systems in the UK and warns how the media, some criminologists, and the Information Commissioner are highlighting a growing concern felt by society that these systems are growing at an alarming rate and that the product from them is not being protected to the degree which will help maintain public confidence that civil liberties are being sufficiently protected.

Ultimately, the fear is expressed that if steps are not taken to secure and maintain public confidence, politicians in the future may be forced to curb the usage currently being made or perhaps abandon some systems altogether.

All correspondence should be addressed to: SIO DP Administration,
NPIA Knowledge Centre, Wyboston Lakes, Great North Road, Wyboston, Bedford, MK44 3BY

Those who give up essential liberty to obtain safety,
deserve neither liberty nor safety.
Benjamin Franklin 17th February 1775

The trawling of passive data systems, such as closed circuit television camera installations, has become an early investigative strategy for police officers engaged in many different kinds of criminal enquiry. It is so commonly carried out that it is hard to remember a world when this source of intelligence or evidence was not available to be harvested. Whilst it is difficult to imagine future politicians being forced to restrict its use, it may be timely for law enforcers to reflect on the public disquiet emerging as a result of the proliferation of passive data systems, and perhaps to note a growing perception that the product is being misused by the guardians of the data generated. If the police and other agencies are to be allowed the continued use of this powerful and useful investigative tool, the deal should surely be that society must be given the confidence that strict rules of engagement are being observed, there is no continual creep or gradual lowering of standards, and that the product from the surveillance is carefully guarded to ensure it is not used for any purpose other than strictly that for which it was intended.

On the 23rd March 2007, the British newspaper, the Daily Mail, ran a story entitled, *"We'll be watching you, MPs warn Big Brother firms"*. According to the newspaper, an inquiry would be held by Members of Parliament into the personal information databases of information held by local councils, supermarkets, and government departments. The theme of this story, that of exposing a creep towards an oppressive, surveillance orientated society, was repeated a week later when the same paper published, in advance of its release, details of a report by the Information Commissioner, Richard Thomas, which, according to the Mail, would contain a warning of "creeping encroachment" on civil liberties by the government and official bodies.

An editorial linked to the latter story contained the following powerful rhetoric.

"Some surveillance is obviously useful, particularly when it helps to curb crime or stop terrorism. But that isn't where the line has been drawn. Just about everyone is spied on. In the streets, on the roads, when we use the bank. In Britain there are more CCTV cameras per head than any other country. The state has 266 powers to enter your home. Your emails and letters may be legally intercepted. Under this government, which boasts of enshrining human rights in law, we have lost more civil liberties than at any other time in history."
(Daily Mail, 29/4/07)

The fundamental problem at the root of the newspaper reports is how to control crime and disorder on the streets most effectively and with the minimum resources yet at the same time maintain the basic liberties of people in society. Clearly the editor of the Daily Mail is convinced that the Franklinesque warning has not been heeded and the balance has swung too far in favour of safety at the expense of liberty.

"Please be aware this town is covered by 43 CCTV cameras" proudly announces a sign attached to a lamppost near Guildford Railway Station. In fact similar signs can be found on lots of lampposts around Guildford, and probably lots of lampposts in lots of different cities and towns all over the United Kingdom.

In this paper I will examine what is meant by the term "surveillance society" and explore the benefits and drawbacks in using advanced technology as a means of social control. Britain would normally be included within the list of so called "developed countries" but it is pertinent to say that on a global level, the proliferation of the use of technology for information gathering, surveillance and commerce varies dramatically, further exacerbating the gap between the rich and poor nations. Whether or not living in a nation with a high level of technical advancement is altogether an advantage, is something I shall explore. One prominent criminologist, David Lyon, warns,

> *"Surveillance technologies and practices are proliferating, bred and cloned by electronic technologies. Security cameras, barcodes, personal identification numbers and passwords exist as an unremarkable part of the fabric of daily life."*
>
> Lyon, 2001

Whilst I will primarily focus on the common and relatively overt form of surveillance, known as Closed Circuit Television (CCTV), in many ways this is one of the more benign methods of social control. A far more insidious technique for example, is the apparent routine eavesdropping by the American National Security Agency on all telecommunications traffic passing through the UK, and the associated filtering of our conversations for key words and phrases (Campbell, 1999). When considering whether or not in the UK we already live in a "surveillance society" one must take into account not only CCTV schemes, but also the existence of a wide range of social control methods including such diverse developments as the National DNA database, the National Health Service patient records system (Connecting for Health), the Police National Computer, the Driver and Vehicle Licensing Authority, as well as hundreds of private companies, from insurance brokers to credit checking agencies like Experion and Equifax. David Lyon (2001) provides a useful definition of surveillance as being *"any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data has been garnered"*.

Britain has in fact already been dubbed a "surveillance society" in a report published by the Information Commissioner in September 2006 (ICO, 2006). This revealed that there are an estimated 4.3 million CCTV cameras in public areas of the UK, and that the average Briton is observed by such a camera several hundred times a day. These cameras are installed and operated by various bodies including the police, local councils (such as the Guildford example), or private companies such as Tesco, British Petroleum etc. Some devices are permanently monitored by a human being, some record in real time or by time lapse onto tape or digital media while others constantly feed separate information databases such as the Driver and Vehicle Licensing Authority computer which contains details of all car owners in the UK.

Sociologists will be familiar with the concept of panopticism as described by Michel Foucault in his book Discipline and Punish (1975). In fact, the panopticon was the name given to a type of prison which would allow a single warder, working from a central tower to observe and control the activities of all the inmates in cells arranged in a huge outer circle. By a clever positioning of screens in the control tower, the inmates would not know if, and when, they were being observed, but they would be obliged to assume that at all times they were. The idea that a whole society could be controlled in a similar way, by a small number of officials, was taken on by Foucault when he described how disciplinary power should be.

> *"Visible and unverifiable. Visible: the inmate will constantly have before his eyes the tall outline of the central control tower from which he is spied upon. Unverifiable: the inmate must never know whether he is being observed at any particular moment."*
>
> Foucault, 1975

In 1975, the idea that there may soon be 4.3 million cameras watching the activities of people in Britain (and perhaps a similar number in Foucault's native France) was unlikely to have entered into the imagination of the author of *Discipline and Punish*, yet what better example of the general idea of panopticism could one find than the explosion of public place CCTV? A handful of operators can create the impression to millions of people that their activities are probably being observed, so that they will not dare engage in deviant behaviour. Or so the installers of the expensive equipment would hope.

Most of the local authority or police installations are not only overt, in other words the camera is not hidden, but they also have signs positively announcing their presence. An essential aspect of the panoptic metaphor is that potential deviants think that someone is probably watching their activity. A few months ago, whilst carrying out research into a book called *Code of the Street* by Elijah Anderson, I visited Philadelphia. Anderson's book is the story of a road called Germantown Avenue which runs from the wealthy suburbs to what he

described as the "hyperghetto" in the city centre. I drove down Germantown Avenue to understand the context, but one of the most interesting things I saw concerned CCTV emplacement. Entering the inner city area as darkness fell, I often had to stop at the traffic lights at intersections, and invariably I was approached by one or two drug dealers who I assumed would be armed with knives or guns. It was an intimidating experience. There was one major intersection however which seemed a little safer and there were no dealers evident. The difference, I noted, was the presence of four CCTV cameras prominently jutting out from the corners of nearby buildings. They were made particularly prominent by each having a flashing blue light on the top and POLICE in large letters on an attached sign. Having felt quite intimidated and anxious throughout most of my journey down Germantown Avenue, I can say that the presence of these very overt police cameras gave me a feeling of security and wellbeing. Of course, I have no idea if they were being monitored, or even if they were connected to anything, but that's the point of panopticism – neither does the deviant. I can say for sure therefore, that at least in terms of providing a level of public reassurance, CCTV installations can work. Whether or not they have any serious effect on levels of criminality however, is less certain.

The Middlesbrough Borough Council sells the idea of their state of the art surveillance system to the tax-payers by claiming,

> *"CCTV is an important tool in the fight against crime. It can record evidence of crimes being committed which can then be used in court. It also acts as a deterrent to criminals and helps reduce the fear of crime. It is well documented that people often feel safer after CCTV has been installed."*
>
> (http://www.middlesbrough.gov.uk/ccm/content/policing-and-public-safety/crime-and-law-enforcement/cctv.en).

This sounds very convincing but other sources suggest the evidence for these claims may be a bit thin. An interesting Home Office Research Paper *Assessing the Impact of CCTV* (Gill and Spriggs, 2005) paints a picture that many town centre CCTV installations have been set up without any data which suggest they will be particularly effective. Ben Brown (1995) also conducted research based on three UK town centre CCTV systems and his overall conclusion was that CCTV had little impact on reducing crime but did have some impact on displacing it. It is right to point out that Brown's research was carried out when town centre CCTV was in its infancy, but his conclusions were pretty well replicated seven years later in another Home Office research paper, *Crime Prevention Effects of Closed Circuit Television: A Systematic Review* (Welsh and Farringdon, 2002) who, rather unenthusiastically, tell us, *"overall, it might be concluded that CCTV reduces crime to a small degree".*

Even if the evidence that CCTV has a beneficial impact on crime reduction is less than convincing, few would argue that it can be a fantastic tool in the detection of serious crime. A "passive data trawl" is nearly always on the fast track action list of any senior investigating officer, and whereas there appears to be no hard research telling us how often crimes are cleared using the product, there is ample anecdotal evidence that many are solved in this way. It is crucial for SIOs therefore, that nothing is done to disturb the fragile pact between police and society in which people are prepared to accept a loss of some degree of privacy in order to better protect their overall quality of life.

I will now turn to consider whether any law abiding person has any reason to be concerned about living in a "surveillance society". Certainly, when I arrived back at Heathrow's Terminal Four recently and waited for 25 minutes in the immigration queue, I became extremely envious of those citizens who had previously allowed their retinal characteristics to be recorded. They were smugly gliding through their simple entry procedure which involved no human immigration officer and no waiting. Lyon (2001) points out how we benefit from the extra speed in commercial transactions which are possible because companies already hold personal information about us, but he also argues that surveillance *"is seen by many as a cause of risk, of potential unwarranted government intrusion into private life or of commercial control of personal consumption".* Whether or not these fears are grounded in reality, perceptions matter, and if people worry about surveillance it must, to some degree, be detrimental to their wellbeing. The importance of a system of trust between society and government was highlighted in a follow up report about the 2006 International Conference of Data Protection and Privacy Commissioners (Ball et al, 2007). This paper used powerful language to illustrate the point that;

> *"a society which relies on surveillance for governance may be committing slow social suicide. This is because a reliance on surveillance in any setting sends messages to the people within that setting that they cannot be trusted, which has knock-on effects for the way in which social relations and privacy are constituted."*

In the report published by the Information Commissioner (2006), the authors warn that;

> *"surveillance is two-sided, and its benefits must be acknowledged. Yet at the same time risks and dangers are always present in large-scale systems and of course power does corrupt or at least skews the vision of those who wield it."*

The report also highlights the possibility of the accidental or inadvertent misuse of private information.

"Large-scale technological infrastructures are peculiarly prone to large-scale problems. And especially where computer systems are concerned, one inadvertent or ill-advised keystroke can easily cause havoc. Think of the release for 'research' purposes, of twenty million online search queries made to AOL by ordinary people in August 2006. Supposedly shorn of identifiers, it took only moments to start connecting search records with names."

(ICO, 2006)

I will now briefly explore how the law protects, or perhaps fails to protect the private lives of citizens. Until 2001 the legislation governing the use of CCTV systems in the UK was rather ambiguous. In that year however, an amendment to the Data Protection Act 1998, required that all new installations had to be set up on an explicit legal basis. Article 8 of the European Convention of Human Rights (ECHR) was incorporated into UK law in 1998 and this requires that any interference by a governmental body with a person's private or family life could only be conducted if specific legislation allowed it. This is why, in 2000, the Regulation of Investigatory Powers Act (RIPA) was enacted to enable the Police and Security Services to carry out their surveillance lawfully. The latter Act brought in strict controls about the use of surveillance, such as a requirement to show that the use of the technique in question is proportionate to the crime being investigated and that any collateral intrusion into other people's private lives is a justifiable necessity because of the seriousness of the case. The law enforcement agencies have to demonstrate to their authorising officer that no other less intrusive technique is likely to work and the greater the level of intrusion the higher the level of authority required. This authority level culminates with a requirement that in cases where extreme intrusion into someone's private life is likely, an independent high court judge, known as the Surveillance Commissioner, must approve the operation.

During 1998 I sat as a member of the Home Office Covert Policing Steering Group. At that time, the Police Service was hoping to cope with the problem caused by the introduction into UK law of Article 8 by agreeing to adhere to Codes of Practice on surveillance. I was described as "pusillanimous" when I suggested to the Group that my interpretation of the Human Rights Act meant nothing less than primary legislation would be required to allow the police to carry out even the most basic surveillance activities. At great expense, Codes of Practice were drawn up, implemented… and quickly found to be ineffective in protecting the police from legal challenges under the Human Rights Act, hence the hasty introduction of the primary legislation now known as the Regulation of Investigatory Powers Act. The relevance of this anecdote to the paper is that whereas the public may feel the police have virtually unlimited powers of surveillance, in fact police covert activity is tightly controlled, and officers would argue that they have been restricted to a far greater degree than they would have liked. The effect of RIPA means, for example, that if an officer wants to carry

out relatively innocuous surveillance by simply using a pair of binoculars to improve eyesight in observing a suspect in a public place, he or she must first fill in several forms and get approval from a senior officer independent of the investigation. The police can, when necessary, carry out very intrusive surveillance, but the legal safeguard for the suspect and law abiding public is considerable.

Contrast that with the apparent uncontrolled explosion of public place CCTV schemes during the 1990s. Until they were brought under the umbrella of the Data Protection Act in 2001, there appears to have been no legislation restricting the installation, scope or use of CCTV cameras by local authorities or private companies. At the same time that the official law enforcement bodies were desperately trying to salvage their legal right to carry out *any* forms of surveillance in the wake of the introduction of the Human Rights Act, law abiding members of society, going about their daily business, were beginning to be routinely subjected to the greatest ever intrusion into their private lives. The fact that parliament sought to so closely control the surveillance activities of the official law enforcement bodies must mean that during the committee stages of the RIPA legislative process, a great deal of evidence was produced by civil libertarians about the detrimental effect uncontrolled surveillance activity would have on non-deviants. It is astonishing to me therefore, that until the Data Protection Act created greater regulation in 2001, an apparently cavalier approach by many local councils and some private businesses was allowed in respect of installing visual monitoring systems which are capable of observing the intimate private activities of millions of law abiding people.

Even now the legislation appears to allow unregulated surveillance of general groups of people in a public area, and only when a particular individual is targeted, does the Data Protection Act offer some protection from intrusion. The website of the Information Commissioner for England offers the following guidance on how the Data Protection Act works.

> *"The highly sophisticated 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 identify criminal activity. These types of images are covered by the Act, but if a general scene is recorded without an incident occurring, the pictures are not covered."*
>
> http://www.ico.gov.uk

It would appear then that the millions of non-deviants randomly observed by CCTV systems every day, are offered no protection if their privacy is intruded upon. Yet these are the very people who would be considered potential victims of "collateral intrusion" when an application is made by a law enforcement body to conduct an operation under the RIPA

legislation, and in those circumstances, the law demands that a high level of consideration be given to their right to a private life.

Writing his rather depressing account of social control systems, Stanley Cohen (1985) describes how the *"people processing professions have received a collective license for gathering information"*. Like Foucault before him, Cohen wrote this book before anyone, apart perhaps from George Orwell (1948), had envisaged the current use of surveillance technology. By coincidence it was in the year Cohen's *Visions of Social Control* was published that the first open street CCTV surveillance system was erected in the seaside town of Bournemouth (McCahill and Norris, 2002). Cohen (1985) acknowledges the concerns and anxieties of the many commentators raising the possibilities of misuse of the massive amount of data collected on individuals in society. He accepts the concern that what he describes as an *"information prison"* is a form of social control. However, Cohen reassuringly points out that the detrimental effect of information gathering is weakened by *"the natural inefficiency of bureaucracy in dealing with all this information"*. In other words, he is saying that despite the fact a huge amount of personal and private information is gathered we need not be overly concerned because the inefficient systems will just be overwhelmed and unable to do anything with it. In visual surveillance terms therefore, the hundreds of hours of footage recorded by a publicly sited CCTV camera in a year would be benign because no-one could possibly have the time to examine it all. In 1985 that may well have been the case, but I suspect Cohen would re-evaluate this proposition in the light of the massive increase in cheap computing power which has emerged from Silicon Valley in the last 22 years. As David Lyon (2001) points out *"it is the massive growth in computer application areas and technical enhancement that makes communication and information technologies central to surveillance"*.

Automatic number plate recognition cameras for example, can instantly send digital images of car number plates from police motorway and town centre cameras to a central computer. According to the Information Commissioners report (ICO, 2006) this computer has an operational capacity to process 35 million ANPR reads every day, increasing to 50 million by 2008, and the data will be stored for two years. Instantly, law enforcement officials can be alerted if a suspect vehicle, or simply a vehicle with no road tax, passes within "eyeshot" of the ANPR camera. It is highly likely that hundreds of times a day people are being sent letters asking them to account for their presence on a particular stretch of road at a particular time when an incident occurred. They must hope that if they are unfortunate enough to have a suspicious partner who has a habit of opening official looking letters, then the reason for their presence on that road was a legitimate one.

Finally, I will take a glimpse into the future of CCTV surveillance as a means of social

control. I was interested in two news stories on the BBC Website. In the first (news.bbc.co.uk/1/hi/england/merseyside/6477831.stm) Merseyside Police heralded the use of flying surveillance drones to assist with crime and public order control. On the same day the Deputy Chief Constable of Hampshire, Ian Readhead, was quoted as saying in an interview,

> *"I'm really concerned about what happens to the product of these cameras, and what comes next. Are we really moving towards an Orwellian situation where cameras are at every street corner? I really don't think that's the kind of country that I want to live in."*
>
> news.bbc.co.uk/2/hi/uk_news/6673579.stm

I agree with DCC Readhead. The idea that in order to patrol the streets of Liverpool, police will be using the same aerial drone technology that the CIA are apparently using to track Osama Bin Laden, is something many people may find quite unacceptable. The area that will be observed by the camera from say, 5000 feet will obviously be far greater than a ground level camera, thereby markedly increasing the likelihood of collateral intrusion into private lives. Whereas the police currently reassure the community that the drones will only be used for specific events such as football matches, it seems somehow inevitable that before long they will be used for routine patrol work. The residents of Liverpool who enjoy sunbathing naked in their back garden may soon need to invest in camouflage netting. Undoubtedly this cheap form of aerial surveillance will, within a few years, be taken up by most police forces, and our skies will be filled with constantly vigilant video cameras sending back images of our "back garden activities" to a police or local authority control room where, no doubt, the staff will be kept highly amused by the sight of our bare, flabby bodies. When one considers that some local authorities and police forces supply town centre footage, or patrol car and airborne surveillance video footage of car chases to TV companies for entertainment programmes such as *"Police, Camera Action"*, together with a regular trickle of news stories reporting how camera operators engage in voyeurism, what chance is there that they can be trusted with routine patrol footage from unmanned drones?

Some observers have noted that the next development in CCTV may be covert "listening cameras" placed in public locations where wrongdoers gather. What better, one may think, than to hear the crimes actually being planned in the first place? The law enforcement benefits of secret cameras placed in public places would undoubtedly be enhanced if they could capture an audio as well as a visual record of the targeted incident or person. The potential for a massive increase in collateral intrusion into people's lives however cannot be overstated and according to a BBC news report many people (including the Information Commissioner, Richard Thomas) see this as a step too far. The Commissioner is reported as saying,

"We would be hostile to the suggestion of any sort of microphones in relation to cameras. We think that would be unacceptable."
http://news.bbc.co.uk/1/hi/uk_politics/6610139.stm

With so many "lines in the sand" already crossed, and with technology around surveillance methods getting more and more sophisticated, I see Richard Thomas as a modern day King Canute, trying to hold back the relentlessly rising tide of intrusion. The authors of his report (ICO, 2006) even accept the fact that *"as people increasingly move round the world – whether for business or leisure travel, or for immigration and asylum-seeking purposes, or to commit acts of terrorism – surveillance activities gain a heightened international, cross-border dimension that surpasses that of the past."*

I believe it is now futile to argue for expensive CCTV installations to be dismantled but I think that to prevent a huge backlash in public attitudes, far more stringent controls are needed in respect of the *product*. If the police and local authorities are to be allowed this unprecedented intrusion into our private lives, it is crucial that law abiding people have confidence that the authorities will rigorously guard the material obtained. Strong sanctions, perhaps even specific criminal sanctions, should be imposed when operators deliberately use their equipment to engage in deviant voyeurism, and strict controls should be imposed on the police and others when providing TV companies with their surveillance footage – whether or not a criminal offence is being depicted. A clear distinction should be made between the release of pictures to identify suspects, and the use of images for entertainment and achieving higher TV ratings.

As someone who spent several years as an Authorising Officer (AO), I know there is a danger that law enforcement RIPA authorisations can become "routine", and currently most AOs have received no specific training for that important task. Confidential guidance produced by the National Policing Improvement Agency recommends training for AOs but that aspiration is yet to become a reality. Ensuring all AOs receive advanced training, and perhaps a system of accreditation are ideas that could be pursued by the Police Service in order to enhance public confidence.

However, the official law enforcement agencies are not really the main problem because as I have already pointed out, the controls imposed on them are fairly robust. I suggest that a great deal more attention needs to be paid to the virtually uncontrolled use of surveillance techniques by local authorities and private companies.

The spectre of global Islamic fundamentalist terrorism which fills our newspapers and television news bulletins every day has allowed governments to introduce social control

legislation which would have been unthinkable a few years ago. The Patriot Act in the United States, and the plethora of anti terrorist legislation enacted in the UK in 2000, 2001, 2005 and 2006, all create extra dimensions of social control, and possibilities for governmental interference with our private lives. The statistical chances of any individual actually becoming a victim of a terrorist act are remarkably low, yet virtually everyone in the western industrialized societies is, in some way, adversely affected by the measures put in place to "protect" society from terrorists. Politicians sometimes brand those who express concern about this surveillance creep as "unpatriotic or even "subversive". Perhaps some politicians think society needs to accept a "new normality" where the right to privacy no longer exists. Perhaps they think we should accept that those who gather data about us are not a threat, but are in fact our benefactor's, merely protecting us from non-conformist's and deviants.

I conclude that whilst we do indeed live in a "surveillance society" and will continue to do so, I am not yet conditioned enough to accept this vision of a new normality. Perhaps Benjamin Franklin was right and those privileged to be able to use the data produced by social control systems, should take care not to contribute to greater public discontent. Senior investigators really need the product from passive data systems, but if we are not careful… well, something about dead geese and golden eggs springs to mind.

References

Brown, B. (1995). *CCTV in Town Centres: Three Case Studies*. Crime Detection and Prevention Series Paper 68. London: Home Office.

Campbell, D. (1999) *Development of Surveillance Technology and Risk of Abuse of Economic Information (An appraisal of technologies of political control) Volume 2/5: Interception Capabilities 2000.* Luxembourg: European Parliament, Directorate General for Research, Directorate.

Cohen, S (1985) *Visions of Social Control*. Cambridge: Polity Press.

Ditton, J. and Short, E. (1999) 'Yes, It Works, No, It Doesn't: Comparing the Effects of Open-Street CCTV in Two Adjacent Scottish Town Centres', in N. Tilley and K. Painter, (eds.) *Surveillance of Public Space: CCTV, Street Lighting and Crime Prevention*. Monsey, NY: Criminal Justice Press.

Foucault, M (1975) *Discipline and Punish*. London: Penguin Books.

Fyfe, N. R. and Banister, J. (1994) *The Eyes on the Street, CCTV Surveillance in Public Places.* Presented at the Association of American Geographers Conference, Chicago March 1994.

Gill, M. and Spriggs, A. (2005) *Assessing The Impact of CCTV*. London: Home Office.

Murakami Wood, D., ed. (2006) *A Report on the Surveillance Society* Online Support [Internet]. Available from http://www.ico.gov.uk [Accessed 12 September 2007].

Ball, K., Murakami Wood, D. and Raab, C. (2007) Part E: *Postscript following the Conference of Privacy Commissioners* [Internet]. Available from http://www.ico.gov.uk [Accessed 12 September 2007].

Lyon, D. (2001) *Surveillance Society*. Buckingham: Open University Press.

McCahill, M. and Norris, C. A. (2002) *CCTV in Britain*. Working Paper No3. Urban Eye.

Orwell, G. (1949) *Nineteen Eighty Four*. London: Secker and Warburg.

Welsh, B. and Farrington, D. (2002) *Effects of Closed Circuit Television: A Systematic Review*. London: Home Office.

IT'S YOUR JOURNAL
YOUR CONTRIBUTION MATTERS

You don't have to be an experienced writer…
We can offer you editorial support.

Be a part of *The Journal of Homicide and Major Incident Investigation.*

Contact the editorial team by email at npia_investigations@npia.pnn.police.uk or telephone 01480 334 615

Relevant and Informative…

Launched in 2005 and published twice yearly, *The Journal of Homicide and Major Incident Investigation* contains ACPO guidance on investigating particular types and elements of homicide, good practice and case studies, together with academic research and legal discussion.

Useful…

So far, *The Journal of Homicide and Major Incident Investigation* has included articles on:

- Guidance on the Use of Serving Prisoners as Witnesses;
- Investigation of Deaths Following Police Contact and Investigating Drug Related Deaths;
- The Use of Interpreters During Operation Lund;
- Managing and Preventing Critical Incidents;
- Honour Related Violence: Context, culture and consequences.

We need you to contribute…

We are looking for articles that we can publish in forthcoming issues.

- Have you worked on a case which may be of interest to other SIOs?
- Have you used a particular technique (forensic/passive data/surveillance) in an innovative and unusual way?
- Do you have specialist knowledge, of a type or aspect, of homicide investigations?
- Has good practice been identified in your force which would be of value to other forces?

THE JOURNAL OF
HOMICIDE AND MAJOR INCIDENT INVESTIGATION

Volume 3, Issue 2 – Autumn 2007