

## CCTV Industry News Digest



Issue #20: July 06

**Welcome to redcare's regular industry digest for public sector CCTV professionals. The briefing contains a round up of the issues that affect CCTV managers – from funding to transmission.**

---

If you would like to unsubscribe to this briefing or recommend a colleague please email [redcare@bt.com](mailto:redcare@bt.com) with unsubscribe in the subject header or recommend and your colleague's email address in the cc. box.

---

### In this issue:

**FUNDING:** Home Office unlikely to provide a new dedicated fund for CCTV; many CCTV schemes in funding crisis as 'first generation' equipment nears the end of its life-cycle  
*- To read more - go to page 2*

---

**DATA PROTECTION:** Information Commissioner plans major investigation of the UK's 'surveillance society'; it will include consideration of the use of CCTV  
*- To read more - go to page 3*

**PERFORMANCE:** Control room ergonomics seen as vital factor in improving CCTV system efficiency  
*- To read more - go to page 6*

---

**ANPR:** Police plan to extend the new national ANPR camera network to cover private-sector sites including car parks, shopping centres and petrol stations  
*- To read more - go to page 9*

## **FUNDING: Home Office unlikely to provide a new dedicated fund for CCTV; many CCTV schemes in funding crisis as ‘first generation’ equipment nears the end of its life-cycle**

The current wide ranging Home Office review of CCTV – the Home Office National CCTV Project – is unlikely to recommend a new round of dedicated CCTV funding. Instead, any future government funding for CCTV is likely to be provided only for projects where CCTV is just one element within an integrated Crime and Disorder Reduction Partnership (CDRP) strategy.

Any future central funding for CCTV in this way is also only likely to be forthcoming if it is matched by funds from local government.

Gary Parkins is Head of the Crime Strategy Unit at the Home Office, and is currently involved in the Home Office National CCTV Strategy Project. He believes that before any new Home Office funding for CCTV can be considered it is vital to understand what it would be for: “We need to develop the [national CCTV] strategy before we consider resourcing. The strategy must drive the funding, and not the other way around.

“My own view is that I would like to see a combination of Home Office funding and local government funding,” says Parkins. “I don’t believe that there will be another dedicated funding programme for CCTV. There is a significant amount of money within the Safer & Stronger Communities Fund - something in excess of £220million, and it will grow year-on-year,” he adds.

However, Parkins acknowledges that CCTV operators are under significant funding pressure just to keep the current CCTV infrastructure operational. “Who pays for the country’s public space surveillance CCTV systems, and keeps them going is a huge issue – it is a huge cost,” he says. “However, we need a

*The current far-reaching Home Office review of UK CCTV is unlikely to result in a further round of dedicated central funding for CCTV. Future funding is likely to be given to crime and disorder reduction schemes integrating a variety of solutions. Meanwhile, many town centre public space surveillance schemes are reaching crisis point as their now-aging CCTV infrastructure begins to fail. Some local authorities have either closed systems or reduced camera coverage as funding pressures deepen*

strategy first – then we need to put a price tag on it, and then, only after that, we will need to consider how we find that.

“With the initial Home Office funding for CCTV in the late 1990s we bought £150million of CCTV kit, but we didn’t buy a single operator or a single maintenance contract,” he acknowledges. “The installed technology is now very old and we are very quickly going to get to a stage where we are going to have to replace it,” Parkins concludes.

Many public space CCTV operators believe that the situation is reaching crisis point, as the existing CCTV infrastructure reaches the end of its life-span with no obvious route for replacement.

“We are all being forced to diversify and take on other roles just to keep the systems going,” says Mike Withers, Salisbury District Council.

“What is the life of a CCTV system?” questions Peter Fry, Director, CCTV User Group. “Seventy per cent of the UK’s public space surveillance systems originate from 1995 and 1996.”

“A lot of local authorities are questioning how they can continue to fund their CCTV systems – let alone how they can find the money to replace them altogether, since they are fast becoming obsolete,” says Fry. “I think we have problems. The very first scheme – on Bournemouth seafront,

involving 74 cameras – recently also became the very first to remove its CCTV public space surveillance system.”

Norman Rice is CCTV manager at Bournemouth Borough Council. Speaking recently to the CCTV User Group magazine, CCTV Image, he says there are other local authorities like his own that are either failing to upgrade their CCTV systems or reducing camera coverage because of funding pressures. “With no central government funding it is becoming extremely difficult for local authority schemes,” Rice says.

Perhaps rather revealingly, Bournemouth seafront experienced an increase in criminality once the cameras were switched off, and 36 of the cameras have now been made operational again. Says Rice, “Vandalism had started to creep up again after the cameras were taken down. It’s been surprising how much of a deterrent the seafront cameras were to crime.”

The last Home Office Crime Reduction funding scheme for CCTV ended in 2002. At present, CCTV must compete with other crime reduction measures for a share of the funding available to Crime & Disorder Reduction Partnerships under the police Basic Command Unit (BCU) Fund and the Safer Stronger Communities Fund. To win money from these schemes it is necessary to demonstrate that CCTV is an integral part of the local CDRP strategy. Bids should also include clear methodologies for performance measurement.

Some of the other current sources that can provide funding for CCTV initiatives include those for regeneration funding, the New Deal For Communities Fund and the European Social Fund.

## **DATA PROTECTION: Information Commissioner plans major investigation of the UK's 'surveillance society'; it will include consideration of the use of CCTV with allied technologies such as ANPR**

The Information Commissioners Office (ICO) is planning a major report on what it describes as the UK's 'surveillance society'. The report will cover technology initiatives including both CCTV and Automatic Numberplate Recognition systems (ANPR).

The Information Commissioners Office (ICO) now views addressing the data protection issues raised by these types of systems as a priority. "We have the infrastructure of the surveillance society being assembled before us – CCTV, ID cards, ANPR," says Jonathan Bamford, Assistant Information Commissioner. "We need to make sure that any intrusion [in people's lives] that occurs, happens [only] for the reason it was intended."

The ICO plans to commission a major report on the 'surveillance society' later this year. And as part of that work, the ICO will for the first time consider the data protection issues associated with ANPR.

"ANPR and other ways of recording vehicle movements – with the plan for data to be kept for up to five years for innocent people – engage these concerns," says Bamford.

"Technology has moved on into ways that profile people's activities. Increasingly we are seeing allied computer technologies being put with CCTV."

"We are looking at ANPR, and its development particularly within the police service," says Bamford. As part of this work the ICO is conducting a piece of research, in the form of a questionnaire sent to each of the police forces, aimed at trying to identify the increasing uses of ANPR and of the ANPR data.

*The Information Commissioners Office plans a major investigation of what it dubs our 'surveillance society', expected for publication before the year-end. The work will look particularly at the data protection implications of CCTV and the way allied technologies such as ANPR are now being added to enhance the core CCTV functionality. In a related development, ACPO has outlined its plans for the storage and retention of ANPR data within the police system for different types of CCTV equipment*

"We shall be looking at the use of ANPR with cameras that have been set up for other purposes, such as traffic monitoring. And we shall also be looking at the use by the police of ANPR data collected for other purposes – for example for congestion charging, by the DVLA or traffic flow monitoring data."

The potential concerns with ANPR that the ICO has so far identified include:

- Pro-actively monitor the activities of increasing and different uses of ANPR
- the increase in the number of cameras, both fixed and mobile
- the possibility of national data centres
- system reliance on multiple databases
- the use of ANPR data collected by third-parties, for example by TfL with the London congestion charging
- access to ANPR data by third-parties
- accuracy of ANPR data and ANPR target data lists
- public awareness and support for ANPR
- proposed data retention periods.

As far as a third-party access to ANPR data, Bamford gives the example of a person whose car is damaged in a public car park by another driver who drives off. In the event that the police won't pursue it, who should have access to the ANPR data on the offender's car – nobody, the local authority, the insurers?

The Information Commissioners Office work on ANPR is being driven, in part, by the unveiling by the police and the Home Office earlier this year of a National ANPR Strategy plan which includes the provision, including funding, for a national network of ANPR cameras, allied to a National ANPR Data Centre (NADC).

“By mid-August the National ANPR Data Centre will be capable of analysing and storing up to 50million numberplate ‘reads’ per day,” says John Dean, National ANPR Coordinator. “Data will be retained on the system for up to five years.”

Under the national ANPR strategy, the intention is that ANPR data will be retained as follows:

**0-90 days.** All ANPR numberplate ‘reads’ will be retained for 90 days – including those for which there is no ‘match’ – available for general access by authorised personnel.

**91days to 2 years.** After 90 days all ‘reads’ will still be kept, but will only be able to be accessed by those involved in major crime investigations. Data will be stored in a live searchable system accessible locally, probably, via superintendent’s authority.

**2 years to 5 years.** The National ANPR Data Centre will retain all reads for five years. They will be stored in a live searchable system with access, probably, only on Chief Officer’s authority.

The following types of data will be held at the NADC:

- plate patch (the captured image of the numberplate)
- the ‘read’ (the ANPR computer’s data interpretation of the numberplate in the plate patch)
- the time, date and location where the vehicle was photographed.

Where there is a data match of a ‘read’ against a target numberplate held on the national ANPR database then the data relating to this ‘hit’ will be kept for as long as there is a requirement, up to the seven years civil litigation limit.

Police interest in ANPR is being led by a strong correlation that is being observed between those people who are guilty of various types of vehicle crime, and those who engage in other forms of criminality. ANPR is proving itself as a powerful policing tool, which can be used not just for identifying suspects, but also witnesses. It can also be valuable to help exclude suspects from investigations. By March this year ANPR systems were responsible for over 400 arrests per week and over 700 vehicle seizures a week.

## **PERFORMANCE: Control room ergonomics seen as vital factor in improving CCTV system efficiency**

CCTV control room design and ergonomics is now seen as a vital factor in determining a CCTV system's effectiveness, yet surprisingly little work has been conducted to establish best practice.

Perpetuity Research's Malcolm Brown, who has been involved in the design for over 100 CCTV schemes across the country, believes that ergonomics and control room design are the key to successful CCTV operation. "All too often CCTV is just moving wallpaper," he says.

Mike Withers, Salisbury District Council and Chairman of the CCTV User Group Standards Board, agrees, "The human element must be the essential element in all of our CCTV systems."

Yet, despite this, until very recently little, if any, research work had been carried out to assess CCTV technology with control room end users.

Now, to some extent that gap has begun to be filled, following a recent study of CCTV control room operations, carried out by Hina Keval, a human-factors ergonomist at the University College London Human Centred Systems.

The research, undertaken with the support of the Home Office Scientific Development Branch (HOSDB), took what Keval describes as a 'user-centric approach' to assessing the effectiveness of CCTV at a number of operational control room environments.

The main conclusion found from the work was that the technology in CCTV control rooms is often poorly designed to support the operator. "The technology is poorly linked to the tasks," says Keval. "There is a need for the system design to be focused around the operators and how they work, rather than around the technology."

*CCTV control room design and human-factors ergonomics are now believed to be critical factors influencing both CCTV operator performance and overall CCTV system performance. New research conducted by University College London with Home Office support highlights a number of typical CCTV system shortcomings*

Keval's colleague and head of University College London's Human Centred Systems department, Professor Angela Sasse, observes, "If only one per cent of the [CCTV control room] hardware budget was to be spent on requirements analysis and designing for usability, you could probably get twice as much performance out of the system."

"A common feedback was that the technology is now ten years old, and no longer performing well," says Keval. "At the same time, local authorities are adding more cameras to their control rooms, without adding to the number of operators," she adds.

Keval's research identified a number of specific barriers to efficient CCTV control room operation:

**Can't See.** Poorly sited cameras, signal loss (microwave or radio transmission), PTZ controls didn't work. These issues caused 'embarrassment' when sharing data with police.

**Information Overload.** Too much going on, too many communication systems, too much noise and surrounding activity, confusion when various alarms ring, affecting task flow. Audio input should be managed based on priority.

**Poor Work Patterns.** 'Too busy for lunch breaks', fatigue driven by poor social and work set-up. Regular breaks needed, standard hours of work. Better planning and historical understanding of workflow could lead to better matching of operator resources and work.

**Poor Technology Integration.** Linkage between the different technologies in

operation – screens, communication systems – was often weak.

**Mapping.** There were no maps linked to the cameras in any of the control rooms visited in the study – either on-screen or on paper. As a result staff often drew their own. Paper maps can go astray and are difficult to keep up to date.

**Camera Locations.** Operators had to memorise camera locations, numbers and screens. Some form of on-screen mapping system linked to a database of camera locations would improve performance.

**Device Usage.** Too many input devices created confusion. Both touch screen and mouse input not uncommon.

**Too Many Screens.** Operators were commonly being required to simultaneously view images from too many screens.

**Room Set-up.** Sometimes, because of room layout, supervisors were not able to see operators.

**Local Knowledge.** Operators lacked local knowledge. The majority of CCTV operators did not live in the area that they survey.

The study looked at the activity at five public area CCTV control rooms, and involved detailed interviews with some 26 CCTV operators. The work focused on work patterns, working hours, tasks and activities and problems encountered with technology or the environment.

The Home Office support for the University College London research follows the publication in spring 2005 of the Scarman Centre Home Office CCTV Effectiveness Evaluation. One element of this wide-ranging work considered the effectiveness of CCTV control room operation. Although the research concentrated on stakeholder relationships and communications, parts of the work considered control room management, control room operation, control room design and operator working practices.

The work, entitled ‘Control Room Operation: Findings From Control Room Observations’, conducted by Professor Martin Gill and his team at Leicester

University, demonstrated that control room operation is a vital factor in the overall effectiveness of any CCTV scheme.

The Gill research concluded:

- The design of the control room, the number of cameras, monitors and operators - and the organisation of operators – were all found to have noticeable impacts on the effectiveness of control room operation
- The probability of detecting an incident is substantially reduced if there is a high camera-operator ratio. With high ratios of cameras to operator cameras were left unobserved for long periods of time, and the system tended to become used as a reactive rather than proactive tool
- Most control rooms were left without effective hands-on control. Six of the 13 control rooms employed a full-time dedicated control room manager, but only four of these were involved in day-to-day operations
- To be successful, operators require the following:
  - technical and operating skills to track targets effectively, obtain quality images and pass on intelligence
  - geographical knowledge of target area and camera locations
  - knowledge of previous crime-related activity in the area
  - knowledge of relevant legislation so they can operate legally (eg, data protection, RIPA, human rights)to do any of the following:
- Operators showed varying levels of skill in obtaining evidential quality recordings of incidents that they spotted. Often they were not aware of the need to meet the police requirements for evidential quality images
- It proved helpful to supply operators with a list or map showing which cameras and camera numbers cover which areas – but this was not always the case
- There was substantial variation in operator attitudes towards their jobs, towards management and towards external agencies

- Operator boredom is a major issue and keeping operators interested in their work is therefore a key success factor
- Operators were generally poorly paid – ranging from £5.00 to £8.12 per hour. Low levels of pay resulted in high staff turnover and high levels of overtime being worked to supplement their wages. Where operators worked extended shifts it tended to reduce concentration and levels of monitoring activity

The complete Home Office report, RDS OLR 14/05 - Control Room Operation: Findings From Control Room Observations (24.2.05), can be downloaded in pdf form from the Home Office RDS website as follows:

[www.homeoffice.gov.uk/rds/pdfs05/rdsolr1405.pdf](http://www.homeoffice.gov.uk/rds/pdfs05/rdsolr1405.pdf)

There is also an established international standard – ISO 11064 – for the principles of design of control centre / control suite type environments - though it is not specifically designed for CCTV control room set-ups. ISO 11064 does however set out some of the general basic ergonomic and environmental requirements for control room operations as well as some basic principles for the evaluation of control centres.

## **ANPR: Police plan to extend the new national ANPR camera network to cover private-sector sites including car parks, shopping centres and petrol stations**

The national ANPR Coordinator has revealed a plan to extend the present joint police/Home Office National Automatic Numberplate Recognition (ANPR) strategy to include camera sites in the private sector.

The plan – called Operation Columbus – would see the current national network of public surveillance ANPR camera supplemented by cameras within private car parks, shopping centres and petrol stations.

“Under Project Columbus we will be able to begin taking [ANPR] data collected from cameras at petrol forecourts, shopping centres and car parks,” says John Dean, National ANPR Coordinator. “We will have developed the operational requirement and the necessary standards by the first half of 2007.”

Under the plan, live data collected from privately-owned and operated ANPR cameras will be able to be fed directly into the computer database at the newly established police National ANPR Data Centre (NADC), and matched in real-time against target lists of ‘wanted’ vehicles.

Not only will Project Columbus have the potential to greatly increase the police’s national ‘footprint’ of strategic ANPR coverage, but it will also mean, for the first time, that private sector companies will, effectively, be able to have their customers’ vehicles ‘checked’ against the police national ANPR computer.

Evidence of the effectiveness of ANPR as a policing tool shows a strong correlation between those people that are guilty of various types of vehicle crime and those people who engage in other types of

***ACPO has revealed radical plans to extend its national automatic numberplate recognition system camera network to include privately owned and operated cameras. The move could see real-time feeds of customer vehicle numberplate data from shopping centres, petrol stations and car parks being stored and analysed by the ACPO/Home Office project’s new National ANPR Data Centre computer as early as mid-2007***

criminality. Because of this, the big retailers, car park owners and petroleum companies – fighting to combat shoplifting, vandalism and theft – are likely to welcome the opportunity to add their cameras to the police network. Already, with police support, private ANPR systems are quite widely deployed at petrol stations at high-traffic sites such as motorway service stations, to try to deter ‘drive-offs’ – drivers who drive off without paying for the petrol.

The main obstacle at present to adding such third-party camera data feeds to the NADC is the issue of data compatibility. Project Columbus will establish clear technology requirements for third-party ANPR cameras and systems (a development of the current national ACPO ANPR standards (NAAS) work), as well as minimum operating performance and the necessary data standards and conformity with system security policy required for central data management compatibility with the national ANPR database BOF II.

Before any non-governmental organisation will be accepted to add their ANPR data feed to NADC is it likely that their system will need to undergo some form of accreditation – possibly by PITO the Police Information Technology Organisation – to ensure system compliance with the core ANPR data model.

Project Columbus is a newly revealed element of the joint ACPO/Home Office National ANPR Strategy. The overall strategy plan, first unveiled in Spring

2005, sets out how the police service will deploy and develop ANPR from now until 2008 to meet its goal of 'denying criminals use of the roads'.

The main elements of the plan are:

- Development of a national infrastructure of ANPR-enabled cameras and readers to cover 'strategic' sites
- Developing a National ANPR Data Centre to analyse intelligence from this network of ANPR readers;
- Every police force in England and Wales to have at least one ANPR intercept team by October 2005 with more teams to be added subsequently;
- Further ANPR development to be funded from hypothecated income from Fixed Penalty Notices generated from ANPR activity; and
- For the use of ANPR equipment and ANPR-generated data as a tool integrated within police force intelligence gathering and investigation activities.

As well as ACPO and the wider police service, the ANPR plan is supported by the Home Office Police Standards Unit and the Association of Police Authorities (APA). In addition, it has been designed to sit alongside a wider national ANPR strategy currently being developed with other partners including the Department for Transport (DfT), the Highways Agency and the DVLA.

The use of ANPR to 'engage criminality on the road' is viewed by the Government and the police as being aligned with a number of the key objectives for the police service, including the National Policing Plan, the Strategic Plan for Criminal Justice 2004-8, the police service's Criminal Intelligence Model and the ACPO Road Policing Strategy.

ANPR is a now well-established technology that allows vehicle registration marks (VRMs) to be identified from CCTV image data. Pattern recognition software analyses the video images and is able to automatically 'read' vehicle registration numbers seen on camera .